



### *Audit e l'impronta sul futuro*

*di Donatella Rosa*

Dopo aver ampiamente commentato, nel numero scorso, il Convegno Nazionale AIEA, tenuto a Firenze lo scorso mese di maggio, eccoci qui a pensare al prossimo Convegno. Sarà il XX e, come al solito, ci vedrà tutti impegnati (noi del Consiglio Direttivo, e voi soci) a prepararlo al meglio.

La conclusione di ogni nostro Convegno, infatti, non è un punto di arrivo, ma è il punto di partenza per nuovi impegni e nuove sfide.

Il convegno è l'occasione di confronto di idee ed esperienze e questo comporta suggerimenti e spunti per nuove iniziative o nuove strade da percorrere che, magari, saranno i temi con i quali confrontarci nei successivi incontri o nel Convegno successivo.

Quello che mi piace immaginare, in questo circolo così simile a quello del miglioramento continuo, è il "miglioramento" della figura dell'Auditor.

Siamo passati dagli eroici inizi di controlli su tabulati cartacei, tra la diffidenza ed il sospetto dei nostri "auditati", al riconoscimento sempre più palese del nostro ruolo.

Quando siamo entrati nell'era e-, alle nostre attività, si sono aggiunti nuovi fattori di complessità.

Le applicazioni tradizionali e quelle per il Web sono, infatti, profondamente diverse: le transazioni su Web sono attivate da una clientela ignota e instabile, il traffico è imprevedibile, asimmetrico, le azioni di altri soggetti sono essenziali per il perfezionamento delle transazioni, la tecnologia è immatura, la sicurezza e la riservatezza sono spesso molto scarse, la giu-

*(Continua a pagina 2)*

### **LINK**

*Strategie di ISACA ->pag.3    Agenda->pag. 9  
Incidenti informatici ->pag.13    BS7799->pag. 17*

### *In questo numero*

*La condivisione delle esperienze ci da consapevolezza della nostra professionalità e rilevanza nel contesto economico-aziendale. Ma è soprattutto uno sguardo al futuro che ci permette di capire dove è orientata la prua e di prepararci a cogliere nuove sfide e nuovi successi. Guardiamo avanti con l'editoriale della Vicepresidente Rosa e con le strategie di ISACA, presentate alla Global Leadership Conference e commentate dal Vicepresidente Narduzzo. Ci aiutano ancora a capire la strada percorsa e le prospettive Marios Damianides ed Everett Johnson, rispettivamente Past Internal President e International President di ISACA. Nuove sfide per motivarci.*

*La gestione degli incidenti ha un ruolo sempre più rilevante, anche per l'IS Auditor, ce ne parla Dario Forte.*

*Completiamo la pubblicazione dell'articolo che presenta l'esperienza di IC-CREA Banca nell'utilizzo dello standard BS7799 per la valutazione del Sistema di Gestione della Sicurezza.*

*Share your knowledge. (O.N.)*



### Sommario: numero 2 del 2005

Audit e l'impronta sul futuro <i>di D. Rosa</i>	1
K-NET <i>di M. Ballerini</i>	2
Global Leadership Conference: le strategie di ISACA e di ITGI, IT Governance, protezione della IP di ISACA e ITGI <i>di O. Narduzzo</i>	3
Calendario attività	9
Bookstore	9
Il messaggio dei Presidenti di ISACA: M. Damianides E.C.Johnson	10
L'IS Auditor e gli incidenti informatici <i>di D. Forte</i>	13
Corsi COBIT	16
BS7799 e la valutazione del SGS presso ICCREA Banca <i>di G. Teti e A. Gaglione</i>	17
Sessioni di Studio	22

Nel prossimo numero:  
Privacy, CISM,  
ISO17799, ...



## *Audit e l'impronta sul futuro* di D. Rosa

(Continua da pagina 1)

risdizione é incerta, le esperienze sono limitate, l'affidabilità e le prestazioni sono poco prevedibili, il rischio è alto.

Inoltre, nell'e-business, poiché non è mai festa e, soprattutto, non tramonta mai il sole, occorre assicurare il funzionamento dei sistemi h24, per tutti i giorni dell'anno.

Anche l'utente ha cambiato natura: si documenta, è informato, fa confronti, è deciso.

Nelle attività di e-business il concorrente di una azienda è lontano solo un "click" e, se il servizio non funziona adeguatamente, il rischio è di perdere business e fatturato.

L'esperienza di mera verifica e successiva correzione dei guasti informatici si è progressivamente tradotta in analisi del rischio, con l'evidenza della complessità del sistema economico, industriale e sociale.

In tutti i casi, comunque, il management "pretende" risultati tangibili e misurabili, in termini di continuità operativa, di livelli di Servizio per l'utente e di riduzione dei costi di gestione.

Ecco che, per rispettare i Livelli di Servizio ed assicurare la continuità e qualità dei servizi, occorre un **controllo** adeguato ed un monitoraggio costante delle prestazioni erogate. Occorre tenere sotto osservazione gli indicatori di criticità, verificare i processi organizzativi.

L'ambito di intervento è fortemente mutato.

I tempi "eroici" delle prime attività di Audit, appartengono alla nostra storia, al nostro passato.

Nell'organigramma aziendale, l'Audit sta diventando, ma spesso lo è già, una funzione "veramente" riconosciuta.

E' in questo contesto che, ora, stiamo lavorando o meglio, stiamo mettendo la nostra **impronta**.

Sono convinta, per chiudere e ritornare al circolo del miglioramento continuo, che stiamo mettendo la nostra **"impronta sul futuro"**.



Security provisioning: come affrontare la problematica in ambienti molto complessi

<http://www.isaca.org/TemplateRedirect.cfm?template=/MembersOnly.cfm&ContentID=13851>

Un'approfondita audit check list per gli ambienti SAP R3

<http://www.isaca.org/TemplateRedirect.cfm?template=/MembersOnly.cfm&ContentID=13848>

Strategie e difese per contrastare in maniera efficace il cybercrime

<http://www.banktech.com/story/news/showArticle.jhtml?articleID=17501355>

(a cura di M. Ballerini)

## *Global Leadership Conference: le strategie di ISACA e di ITGI*

*di Orillo Narduzzo*

La globalizzazione doveva appiattire le differenze e creare un unico mercato. Invece le nazioni stanno viaggiando a velocità diverse riaccutizzando le differenze, sia dal punto di vista economico sia infrastrutturale. La tecnologia propone ancora fattori abilitanti per il business ma non vengono tradotti concretamente in opportunità con la stessa pervasività e immediatezza. Le comunicazioni hanno annullato "alcune" distanze, hanno ridotto "alcuni" costi, ma hanno creato contraddizioni e il mercato ha reagito con un certo nervosismo.

E' una fase di riflessione per imparare dalle esperienze fatte e individuare i fattori di successo per la prossima tappa. In questo scenario bisogna ripartire dall'analisi dei fondamentali, approfondire il ruolo dei diversi attori e focalizzarsi sulle leve gestionali più semplici e più efficaci. Le migliori risposte consentiranno di formulare strategie vincenti. In particolare, dopo aver sentito che l'IT non è fondamentale (*It doesn't matter*) e che dall'Auditor ci si aspetta di più, due sono i ruoli da analizzare: il CIO e l'IS Auditor.

ISACA (vedi riquadro a lato) è da diversi decenni attenta allo sviluppo professionale degli auditor di sistemi informativi e in questi ultimi anni ha ampliato la sfera di influenza offrendo spunti di riflessione e contributi professionali a tutti gli informatici e non più solo agli auditor. All'inizio del terzo millennio ISACA ha discusso le proposte elaborate dal Comitato per le Strategie nella Global Leadership Conference, tenutasi a Las Vegas alla fine dell'aprile 2000 dove ha raccolto i rappresentanti di tutti i 170 capitoli distribuiti in tutto il mondo.

La conclusione alla quale è pervenuta ISACA è che l'attore chiave di questa fase è il CIO (Chief Information Officer). Da lui dipende il successo delle aziende, perché è lui che può ottenere quei risultati che oggi appaiono indispensabili: allineamento tra strategia aziendale e investimenti in IT, processi di business con l'IT integrata e coerente – dal punto di vista economico, delle funzionalità, della sicurezza – con il modello di business aziendale.

Le criticità sono evidenti. Thornton A. May, conclamato guru dei CIO, ritiene che solo circa il 39% dei CIO abbia performance accettabili. Vari osservatori  
(Continua a pagina 4)

**ISACA®**



*ISACA® - Information Systems Audit and Control Association® - è leader mondiale nell'IT Governance, nel controllo, nella sicurezza e nell'assurance. La missione di ISACA è quella di aiutare i professionisti nel conseguire alti livelli di prestazioni aziendali e di conformità attraverso l'applicazione di appropriate pratiche di sicurezza, di assurance e di management in ambito IT.*

*L'associazione è fortemente impegnata nel fornire quanto serve nelle emergenti discipline professionali: ricerche originali, formazione concreta, certificazioni, standard di mercato e best practice, una rete di rapporti con i colleghi, fonti professionali e pubblicazioni tecniche e manageriali. ISACA gestisce due certificazioni riconosciute a livello mondiale: Certified Information Systems Auditor (CISA®) e Certified Information Security Manager (CISM®). L'associazione organizza conferenze internazionali e corsi, e pubblica una importante rivista tecnica, l'Information Systems Control Journal.*

*ISACA è consapevole che deve fornire prodotti, servizi e valore aggiunto ad una ampia platea di professionisti dell'IT che lavorano per assicurare informazioni e sistemi affidabili. Fra gli associati ci sono: auditor informatici, responsabili della sicurezza informatica, professori universitari, consulenti, internal auditor, manager dell'IT, external auditor, Direttori Generali.*



## *GLC: le strategie di ISACA e ITGI*

*(Continua da pagina 3)*

stimano in 20-30% la quota di budget persa in progetti che non portano valore alle aziende. Un'analisi dell'ITGI sulle aziende del gruppo Fortune 500 ha rilevato che solo il 30% di queste ha una strategia per l'IT approvata o ha un Comitato dedicato alla strategia IT. Una poltrona che scotta quella del CIO.

Fin dal 2000 ISACA propone, attraverso l'ITGI (vedi riquadro in questa pagina), un insieme di modelli e suggerimenti per supportare il CIO nel governo dell'ICT. E questo sarà uno degli ambiti più importanti della strategia di ISACA: fornire soluzioni che facilitino l'allineamento ICT-Business e l'IT Governance, avvicinare l'IS Auditor al CIO sviluppando ulteriormente il ruolo consulenziale dell'IS Auditor.

In quali contesti l'ITGI può dare un aiuto ai CIO per il governo dell'IT può essere illustrato prendendo spunto dalla pubblicazione: "IT Governance Executive Summary". Essi sono innanzitutto la definizione di una strategia per l'IT, dalla quale avere le linee guida per generare valore concretizzando il vantaggio competitivo, dalla quale avere le linee guida per mantenere il valore degli asset ed evitare le perdite, in sintesi per riuscire a risolvere i problemi facilitando il miglioramento continuo. I domini dell'IT Governance individuati sono: allineamento strategico col business, creazione di valore attraverso le risorse IT, gestione del rischio informatico, gestione delle risorse informatiche, misura delle performance.

ITGI è già un interlocutore riconosciuto di fornitori mondiali e di aziende innovative, ai quali ha indicato la strada da percorrere. Il livello indirizzato è il Top Management o il Consiglio di Amministrazione, per il futuro ITGI coniugherà le sue intuizioni e svilupperà delle ricerche a vantaggio dei collaboratori del CIO per aiutare questi ultimi a concretizzare quei processi che permetteranno di governare l'IT e di comunicare con il vertice aziendale.

Marios Damianides, International President, ha completato la presentazione delle strategie di ISACA citando i recenti accordi con le associazioni più rappresentative del mondo della sicurezza (ASIS International e Information Systems Security Association—ISSA) e riepilogando i punti di forza che verranno ulteriormente sviluppati: COBIT, K-NET, CISA e CISM.

*(Continua a pagina 5)*

**ITGI®**



*ITGI® - IT Governance Institute® - è stato fondato nel 1998 per sviluppare il pensiero e gli standard per la direzione ed il controllo dell'IT. ITGI aiuta i leader, i dirigenti e gli amministratori delle aziende nel far fronte alle loro responsabilità riguardanti l'IT Governance.*

*Per fornire una linea guida alle organizzazioni di qualunque dimensione e settore in tutto il mondo, ITGI ha sviluppato COBIT®, il modello internazionalmente accettato per il controllo dell'IT, delle informazioni e dei loro rischi. Inoltre ITGI ha svolto delle ricerche e pubblicato: COBIT Security Baseline, Board Briefing on IT Governance, Information Security Governance, IT Control Objectives fro Sarbanes-Oxley, IT Governance Implementation Guide.*

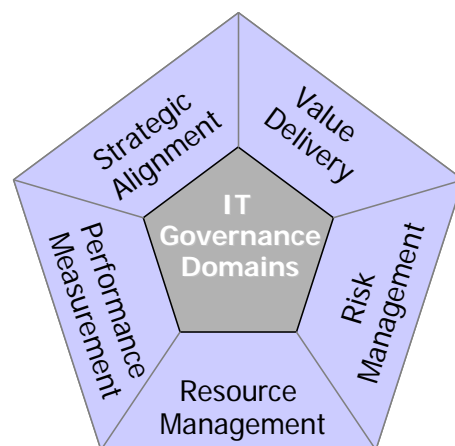
*ITGI ha realizzato una indagine sullo stato dell'IT Governance: il 91% delle aziende riconosce che l'IT è vitale per le loro attività ma i loro Direttori Generali non hanno competenza sufficiente per esercitare un controllo sull'IT. ITGI aiuta dirigenti e amministratori a perseguire proprio quegli obiettivi indicati dai CEO nell'indagine: misurare le performance dell'IT, gestire meglio i rischi e le risorse IT, creare valore con l'IT, allineare l'IT alle strategie aziendali.*

## *GLC: le strategie di ISACA e ITGI*

*di O. Narduzzo*

“Anche COBIT verrà rivisto” – è prossima la pubblicazione della quarta versione –, ha detto Erik Guldentops, “per avvicinarlo ancora di più al business”. Il Framework fornirà un link più esplicito per collegare i processi aziendali agli IT Goals, mentre i Control Objectives saranno semplificati e correlati più strettamente alle attività aziendali. Sarà inoltre perseguita una armonizzazione con gli altri standard riconosciuti: ISO17799, ITIL, CMM, PMBOK.

In questo contesto l'Auditor dovrà quindi considerare non solo il rischio ma anche come i processi generano valore e individuare il livello di rischio accettabile commisurato appunto al valore generato, per suggerire le azioni sostenibili nella specifica situazione aziendale. In questa attività l'auditor sarà aiutato dal modello di maturità di COBIT che consente di esplicitare il posizionamento rispetto all'eccellenza favorendo la consapevolezza del CIO sulle opportunità e sulle criticità esistenti al fine di selezionare le azioni più opportune. Il modello di maturità, le control practices, le motivazioni dei controlli - che si possono trovare in COBIT 3.2 – costituiscono un “paniere” dal quale scegliere gli interventi che consentiranno di ridurre i costi, mitigare i rischi, conseguire efficienza e performance migliori.



ITGI e ISACA saranno attive nell'Assurance, nella Sicurezza, nell'IT Governance e avranno come destinatari la Business community, le aziende, i professionisti, cercando di andare oltre l'IT Control. E' la scommessa di chi crede che l'IT Matters, non per se stessa ma per il valore che genera nelle aziende.

*O. Narduzzo, Vicepresidente AIEA*

### **Il nuovo Consiglio Direttivo di ISACA.**

International President	Everett Johnson, CPA	USA
Vice President	Bill Boni, CISM	USA
Vice President	Abdul Hamid Bin Abdullah, CISA, CPA	Singapore
Vice President	Jean-Louis Leignel	France
Vice President	Lucio Molina Focazzio, CISA	Colombia
Vice President	Howard Nicholson, CISA	Australia
Vice President	Bent Poulsen, CISA , CISM	Denmark
Vice President	Frank Yam, CISA, FHKCS, CIA, CFE, CCP, CFSA, FFA	Hong Kong
Past International President	Marios Damianides, CISM, CISA, CA, CPA	USA
Past International President	Robert S. Roussey, CPA	USA
Advisor to the Board	Erik Guldentops, CISM, CISA	Belgium
Secretary and CEO	Susan M. Caldwell	USA



## *Global Leadership Conference: la missione di ITGI*

La definizione di "IT Governance" formulata da ITGI, e in particolare il suo modello *Control Objectives for Information and related Technology* (COBIT®), costituiscono la base per tutti gli altri standard e modelli dell'IT nell'indirizzare le problematiche che le imprese debbono affrontare quando si concentrano sul governo dell'IT, passo sollecitato anche dalle normative (SOX, Privacy, Basilea II, ecc.).

Per capitalizzare questo primato ITGI deve considerare le imprese come stakeholder che richiedono una attenzione specifica, in particolare per ricercare e proporre tecniche e strumenti manageriali per promuovere la formazione, la implementazione e la consulenza nell'ambito del governo dell'IT. Concretamente questo significa sviluppare tecniche e supporti per i concetti dell'ITGI e per il modello COBIT, strumenti che possono aiutare coloro che hanno nelle aziende la responsabilità del governo dell'IT.

Attualmente ITGI – leader nell'IT Governance - finanzia e coordina ricerche in quest'ambito per l'individuazione di nuovi concetti, sviluppo degli approcci selezionati, creazione di strumenti pratici per le aziende. ITGI traduce quindi queste ricerche in pubblicazioni e supporti per la formazione, sia webcast sia corsi (in-house, online, documenti) e con carattere divulgativo organizza un simposio con cadenza annuale. Esempi di queste ricerche comprendono: COBIT, *Board Briefing on IT Governance, 2nd Edition*, *IT Control Objectives for Sarbanes-Oxley* and *The CEO's Guide to IT Value @ Risk*.

ISACA è un canale di diffusione di questi risultati, ISACA infatti inserisce i concetti di IT Governance nei domini di conoscenza delle certificazioni CISA e CISM, e ne sviluppa le conseguenze per quanto riguarda la sicurezza (vedi ad esempio il documento *Security Harmonisation*).

La missione di ISACA è di aiutare i professionisti dell'audit, del controllo e della sicurezza informatici. Quella di ITGI è invece diretta verso le aziende e quindi gli interlocutori sono il top management, in particolare la Direzione Generale, i Responsabili dell'IT (CIO- Chief Information Officer) e i manager delle funzioni IT. L'ITGI non può perseguire da solo questi obiettivi, ma deve farlo in collaborazione con gli altri enti ed associazioni che hanno gli stessi destinatari.

L'ITGI è costituito da tre categorie di aderenti. Il Comitato degli Esperti che seleziona gli ambiti da approfondire e valuta i trend del mercato per individuare le opportunità per il governo dell'IT. Gli associati - organizzazioni nazionali o regionali senza scopo di lucro - che desiderano pubblicamente favorire lo sviluppo di questa disciplina, esistono già, ad esempio, gli ITGI di Giappone e Francia; anche i capitoli di ISACA appartengono a questa categoria. Infine gli Sponsor che sono organizzazioni commerciali che partecipano finanziariamente alle ricerche di ITGI per favorire lo sviluppo delle attività e la divulgazione dei risultati.

Anche se le attività di ISACA sono svolte da associati non retribuiti, vi è co-

(Continua a pagina 7)

## *Il Governo dell'IT: le pratiche e le competenze*



Nel 2004, l'IT Governance Institute, assieme a Lighthouse Global, ha svolto una approfondita indagine sul dominio della conoscenza relativo al governo dell'IT, sono stati intervistati oltre 200 professionisti dell'IT appartenenti a 14 paesi dell'America, Asia ed Europa. Il risultato di questa analisi è stato riepilogato in cinque briefing direzionali, i primi quattro sono disponibili sui siti di ISACA e di ITGI ([www.iaca.org](http://www.iaca.org) e [www.itgi.org](http://www.itgi.org)).

### ***Optimising Value Creation From IT Investments***

Tratta una problematica che è frequente nelle aziende: la sfida di ottenere adeguati ritorni dagli investimenti in risorse informatiche.

### ***Information Risks: Whose Business Are They?***

Inquadra la gestione del rischio informatico, uno dei concetti chiave del governo dell'IT e una problematica di competenza del top management.

### ***Governance of Outsourcing***

Esamina le best practice per il governo dell'outsourcing delle attività IT, una pratica divenuta comune in tutto il mondo nella ricerca di servizi IT più efficienti ed efficaci.

### ***Measuring and Demonstrating the Value of IT***

Tratta le problematiche della misura delle performance, comprese le best practice per la gestione delle performance nell'IT e la loro rilevanza nel governo dell'IT.

### ***IT Alignment—IT Strategy Committees***

Esamina l'efficacia di un comitato per le strategie IT nell'aiutare a perseguire l'allineamento tra gli obiettivi IT e quelli aziendali più generali.

(a cura di O. N.)

Per maggiori informazioni su ITGI e le sue pubblicazioni visitate :

[www.itgi.org](http://www.itgi.org)

(Continua da pagina 6)

munque la necessità di una struttura di coordinamento, analogamente per l'ITGI. L'elemento chiave della struttura dell'IT Governance Institute è il Comitato. Fra l'altro l'ITGI Committee ha il compito di selezionare i progetti e definirne gli ambiti e le priorità.

Le linee guida per il Comitato sono individuate dal Comitato degli Esperti. I mezzi finanziari per le attività dell'ITGI sono reperiti attraverso ISACA che diffonde i risultati dell'ITGI e attraverso contributi ricevuti direttamente.

(A cura di O. Narduzzo)



## *Global Leadership Conference: la tutela delle proprietà intellettuali di ISACA e di ITGI*

ISACA e ITGI hanno recentemente sottolineato l'importanza di proteggere le proprietà intellettuali possedute dall'associazione e di regolarne l'utilizzo. L'argomento è stato discusso nell'ambito della Global Leadership Conference. Riteniamo utile riprendere queste linee guida anche su queste pagine.

Tra i marchi depositati di ISACA ci sono:

- \* Certified Information Security Manager<sup>®</sup> (CISM<sup>®</sup>)
- \* Certified Information Systems Auditor<sup>™</sup> (CISA<sup>®</sup>)
- \* COBIT<sup>®</sup>, COBIT<sup>®</sup> 3<sup>rd</sup> Edition<sup>®</sup>, COBIT Quickstart<sup>™</sup> e COBIT Online<sup>™</sup>
- \* *Global Communiqué*<sup>®</sup> e *Information Systems Control Journal*<sup>®</sup>
- \* Information Systems Audit and Control Association<sup>®</sup> (ISACA<sup>®</sup>) e IT Governance Institute<sup>®</sup>
- \* Information Systems Control Association<sup>®</sup> (ISCA<sup>®</sup>)
- \* K-NET<sup>®</sup>

Alcune delle regole alle quali attenersi:

- \* Solo ISACA International può autorizzare ad usare i lavori di ISACA e di ITGI.
- \* Parti di lavori di ISACA e di ITGI possono essere usati per fini interni o accademici, ma non commerciali, da parte dei capitoli e degli associati; è solo richiesta la citazione esplicita degli autori e della fonte (ISACA o ITGI).
- \* Per uso commerciale o per la diffusione di lavori di ISACA/ITGI è necessaria una autorizzazione scritta.
- \* E' opportuno evitare di usare i *logo* citati in eventi o lavori di terze parti, soprattutto se con tale comunicazione si accredita una approvazione di ISACA che non c'è.
- \* I professionisti, certificati CISM e CISA, possono usare tali acronimi nei propri biglietti da visita e possono omettere il simbolo di marchio registrato (®).
- \* I *logo* sopra citati non possono essere usati assieme ai *logo* aziendali al fine di evitare di comunicare qualsiasi accreditamento o accordo.

AIEA, come capitolo di ISACA, può usare i logo di ISACA/ITGI nelle proprie pubblicazioni e nel proprio web per comunicare la propria affiliazione ad ISACA e per promuovere quanto fornito da ISACA (esempio gli esami per le certificazioni CISA e CISM).

AIEA ha versato ad ISACA le *royalties* richieste ed è stata autorizzata per iscritto da ISACA ad effettuare le traduzioni di COBIT ed a distribuire gratuitamente la versione italiana.

(a cura di O. Narduzzo)

## Nella ... TUA AGENDA



<u>INIZIATIVA</u>	<u>SEDE</u>	<u>DATA 2° SEMESTRE 2005</u>
Sessione di Studio	Siena	9 luglio
Sessione di Studio	Torino	22 settembre
Sessione di Studio	Roma	28 settembre
Sessione di Studio	Milano	7 ottobre
Corso COBIT Base	Milano	18-19 ottobre
Corso COBIT Avanzato	Milano	25-26 ottobre
Sessione di Studio	Roma	3 novembre
Sessione di Studio	Milano	11 novembre
Sessione di Studio	Verona	25 novembre
Sessione di Studio	Torino	28 novembre
Corso: da COSO a COBIT	Milano	1 dicembre
Sessione di Studio	Roma	13 dicembre
Sessione di Studio	Milano	16 dicembre
Corso Audit Base	Milano	da definire
Esame CISA	da definire	10 dicembre 2005
Esame CISM	da definire	10 dicembre 2005
ISACA Training week	Praga	3-7 ottobre 2005
ISACA Training Week	Chicago	7-11 novembre 2005
ISACA Training Week	Scottsdale	5-9 dicembre 2005

## Bookstore

Nel Bookstore di ISACA ([www.isaca.org](http://www.isaca.org)) sono state inserite le seguenti pubblicazioni:

*Core Concepts of Accounting Information Systems*

*Hardening Windows Systems*

*Linux: Security, Audit and Control Features*

*Hardening Network Security*

*Gray Hat Hacking: The Ethical Hacker's Handbook*

*Disaster Recovery Yellow Pages*

*Essential Project Investment Governance and Reporting*

*Security Awareness: Best Practices to Secure Your Enterprise*

*The Visible Ops: Starting ITIL in 4 Practical Steps*



## I MESSAGGI DEI PRESIDENTI DI ISACA



*I messaggi del presidente internazionale che chiude il suo mandato —Marios Damianides—e del nuovo presidente internazionale che apre il suo impegno —Everett C. Johnson— sono una ottima opportunità per capire il cammino percorso e dove stiamo andando.*

*Questi due messaggi sono stati pubblicati su Global Communiqué di luglio e agosto 2005.*



Marios  
Damianides

This is my last message to you in my position as international president of ISACA and ITGI. During my two years in office, I have had several occasions to ponder the ancient Chinese proverb, "May you live in interesting times." I am sure that all of you who read this would wholeheartedly agree that this has been one of the most "interesting" years our profession has faced. We have emerged from these challenging times stronger and ready for the next challenge, both as a profession and as ISACA and ITGI. In fact, I would apply another old saying to our current situation: "It is not how you start, but how you finish." Although we have finished another very successful year, we are highly cognizant of the fact that often the riskiest time for organizations is when they are most successful. Therefore, we choose not to rest on our laurels, but instead approach our future with cautious confidence and bold plans.

We had much to celebrate in 2004. In a year that marked the 35th anniversary of ISACA, we also certified our 35,000th Certified Information Systems Auditor™ (CISA®). In addition to membership and CISA growth in 2004, we saw the new Certified Information Security Manager® (CISM®) certification expand and begin to stake out its niche in the marketplace, research projects come to fruition, and COBIT receive increased recognition and adoption. New standards, guidelines and procedures were issued, education programs and conferences reached a widening audience, and work continued on the business strategy and supporting balanced scorecard.

Speaking of COBIT's continued worldwide recognition and adoption, this was recently underscored by the announcement that COBIT has been selected by the Commission of the European Communities (EC) as one of the three internationally accepted standards to be used to provide information security and control over its agricultural paying agencies.

The regulation, adopted on 22 March 2005, is aimed at tightening information systems security across the European Union's 25 member states. Paying agencies associated with the European Agricultural Guidance and Guarantee Fund (EAGGF) are now required to select COBIT, ISO Standard 17799 or the *IT Baseline Protection Manual* [British Standards Institution (BSI)] as the basis for their information systems security.

The EU regulation directs that one of the three standards must be used retroactively from 16 October 2004. From financial year 2008, starting 16 October 2007, auditors must provide a statement on the security measures in place based on the chosen standard.

*(Continua da pagina 10)*

During the period 2004-2007, the annual auditors' reports are required to include a score for each domain of the chosen standard based on a maturity model developed directly from COBIT's generic process maturity model. Even if a member state chooses one of the other two standards, the auditor still must use the COBIT-based maturity model as part of the reporting mechanism.

Clearly, this is a significant honor for COBIT, and I am proud to have had the opportunity to play a part in the organizations whose efforts have brought COBIT into practice. In fact, it has been my privilege to be part of the entire ISACA/ITGI team for the past several years, and I look forward to a continuing role in the years to come. I am especially pleased at the worldwide outreach exhibited by the Board of Directors this year; from meetings in Australia to speaking engagements in virtually every area covered by ISACA, the board members have tangibly displayed their commitment to ISACA's global nature.

Thanks to the efforts of the leadership network—both volunteer and staff—ISACA and ITGI can look back at 2004 and ahead to the remainder of 2005 with equal enthusiasm.

As I have maintained throughout my tenure as international president, "Excellence is not an act but a habit. Success is not a destination but a journey." I am deeply grateful to the vast network of volunteers that has made the organizations what they are today. I look forward to continuing on this journey with each of you.

Marios Damianides, CISA, CISM, CA, CPA  
2004-2005 ISACA International President

---

This is my first message to you, so I want to begin by thanking you for the honor and privilege of serving as ISACA's international president. One only has to look at ISACA's growth and expanded presence over the past years to know that this is an association with a rich heritage and an equally promising future. It is an opportunity and a challenge to be at its helm.

Of course, it is not a job anyone can accomplish alone. I am grateful to the other members of the international Board of Directors and all the supporting key board and committee chairs and members, chapter leaders, volunteers and our very capable International Headquarters staff for their help in making the association what it is today—and what it shows the promise to be in the coming years.

I recently attended our International Conference in Oslo, Norway, and—aside from enjoying the fabulous hospitality of the Norway Chapter—I had the opportunity to look around and marvel at the incredible reach and diversity of our membership. Our 47,000-plus members live and work in 140-plus countries and hold virtually every IT control-related title, including IS auditor, consultant, educator, IS security manager, regulator, chief information officer, external auditor and internal auditor. We also have a few CEOs. Some are new to the field, others are at middle management levels, and still others are in the most senior ranks.

They work in nearly all industry sectors, including financial and banking, public accounting, government and the public sector, utilities, retail and manufacturing.



Everett C.  
Johnson

*(Continua a pagina 12)*



## ***I MESSAGGI DEI PRESIDENTI DI ISACA***

*(Continua da pagina 11)*

Our Board of Directors is a microcosm of the ISACA diversity. Look at this roster:

- Everett Johnson, retired from Deloitte & Touche, USA
- Abdul Hamid Bin Abdullah, deputy director of the Auditor General's Office, Singapore
- Bent Poulsen, chief IS auditor at VP Securities Services, Denmark
- Frank Yam, chief executive officer of Focus Strategic Group Inc. and Handshake Networking Ltd., Hong Kong
- Howard Nicholson, business analyst for the City of Salisbury, Australia
- Jean-Louis Leignel, partner at MAGE Conseil, France
- Lucio Augusto Molina Focazzio, external IS auditing and security consultant, Colombia
- William Boni, vice president and chief information security officer of Motorola Information Protection Services, USA

That is quite a diverse crew—a truly varied mix of job titles, industries, years of experience, backgrounds and locations. This phenomenon is mirrored—and multiplied—in the ISACA membership. I am convinced this wide-ranging diversity is good for the association and its members. It opens members' eyes to the challenges and opportunities faced by colleagues in other countries, positions and industries. It enables the association to draw on a vast pool of talent to accomplish its goals. It is, quite simply, one of ISACA's strengths.

Of course, our diverse member base presents challenges as well. It is not always easy to determine what the association should be offering to meet the varied needs of its constituents. However, we have now finalized our strategy and my number one goal will be to oversee its implementation.

An important part of the strategy is meeting your needs, and we continually strive to determine, through surveys and informal discussion, what issues are important to a good cross-section of members, and then devise an appropriate product or service to meet the need. Now that we have our balanced scorecard in place, we will be doing even more reaching out for information, so if you are on the receiving end of a survey or phone call, please take time to let us know what is on your mind.

Thank you again for the honor of holding this position. I look forward to working with you in the year ahead to continue the association's tradition of success.

Everett C. Johnson, CPA  
2005-2006 ISACA International President

## *Il ruolo dell'IS Auditor nella gestione degli incidenti informatici*

*di Dario Forte*



*In tutte le strutture ove sia presente la gestione degli incidenti informatici, anche l'IS auditor ha un ruolo sempre più importante nell'incident management.*

### **Principi di Incident Management: le fasi e l'operatività.**

Con il termine "incidente informatico", la letteratura attuale definisce qualsiasi violazione, volontaria o non, alle politiche di sicurezza aziendale, con particolare riferimento a quelle relative all'ICT. Nell'ultimo triennio stiamo assistendo ad un'escalation di questa categoria di problematiche, che hanno un impatto anche serio sull'intero ciclo biologico IT.

Secondo le best practices di letteratura (molte delle quali contenute anche nell'ultima versione dell'ISO 17799), le fasi di gestione di un incidente informatico sono le seguenti:

- Pre incident
- Notifica dell'incidente
- Attuazione di una strategia di risposta
- PostMortem e ripristino (incluse le Lessons Learned)
- Reporting.

All'interno della fase di Postmortem, inoltre, sono contenute le attività di Digital Forensic, che vengono di norma effettuate sia in caso di attacco subito sia nel caso in cui un utente abbia utilizzato un computer per portare avanti una qualsiasi condotta criminosa. All'interno della Digital Forensic, inoltre, vi sono anche le attività di Log Analysis, sempre più importanti in questo particolare momento storico.

L'output di un processo di incident management può essere duplice: interno ed esterno. E' interno quando tutta la documentazione, la ricostruzione dell'accaduto e le analisi vengono portate a conoscenza solo del management dell'azienda; esterno quando si porta a conoscenza anche l'Autorità Giudiziaria. Esiste, poi, un'ultima eventualità: un ente esterno all'azienda, comunque autorizzato per legge ad effettuare dei rilievi (per esempio l'Autorità Giudiziaria), può richiedere all'azienda stessa l'esibizione di log files, caselle di posta, files etc. Atteso che sono davvero pochi i casi in cui, teoricamente, le aziende sono tenute a conservare dette informazioni, appare comunque necessario dotarsi di un'interfaccia che gestisca i rapporti con l'Autorità Giudiziaria, non solo dal punto di vista formale (di solito ci pensa l'Ufficio Legale) ma da quello sostanziale, cioè un supporto alla fase operativo/investigativa.

*(Continua a pagina 14)*



## *L'IS Auditor e gli incidenti informatici*

*di D. Forte*

*(Continua da pagina 13)*

### **Il ruolo dell'IS auditor**

Di solito l'IS auditor viene chiamato nelle circostanze che seguono:

- Preparazione agli incidenti: A prescindere dal ruolo ovvio di ownership ricoperto, nella fase di esercizio e in quella operativa, dalla funzione sicurezza (inclusa quella informatica), l'Audit viene di solito chiamato a discutere l'incidenza delle politiche e delle procedure di gestione dell'incidente nei confronti del Top Management e della Polizia/autorità Giudiziaria. Può, in alcuni casi estremi, avere potere di veto ( succede soprattutto nell'ambiente finance) ed è un anello infungibile nella catena di gestione.
- Notifica: a seconda delle procedure che sono state stabilite nella fase di cui al punto precedente, l'Audit riceve (anche in cc) una comunicazione dell'avvenuto incidente. Con notifica, in questo caso, alcuni intendono anche l'avvenuta notifica, da parte dell'Autorità Giudiziaria, di un qualsivoglia Decreto, per l'acquisizione di eventuali log e/o ulteriori informazioni eventualmente disponibili.
- PostMortem/Digital Forensic. Come più volte chiarito in letteratura, la produzione di potenziali fonti di prova deve seguire determinati criteri tecnico/legali. Per esperienza personale mi capita sempre più spesso di assistere all'intervento diretto degli IS auditor in attività di Digital Investigation correlate a violazioni di tipo interno (per esempio causate da impiegati infedeli). Alcuni IS auditor (esperienza diretta su cliente inglese operante in Italia), inoltre, operano congiuntamente all'IT security al fine di reperire eventuali falle replicate sui sistemi e porvi rimedio.
- Reportistica e Lessons Learned. L'audit, per definizione, ha una linea diretta con il Top Management. E' quindi evidente come, in molti casi, sia questa categoria di operatori a dover stilare il rapporto finale relativo all'incidente, ferma restando l'infungibile attività dell'IT security.

### **I problemi di tutti i giorni**

Per la sua connotazione quasi "poliziesca", l'IS auditor deve, per forza di cose, giostrarsi tra varie realtà aziendali, sia interne sia esterne. Per esempio deve interagire con la massima efficacia con IT security e ufficio legale, in quanto, per definizione, gli incidenti informatici hanno una componente molto alta gestita dai due players sopra citati. Per questo motivo (e qui parlo, come sempre, per esperienza diretta) lo skill specifico richiesto agli IS auditor in questo settore è sempre più alto. Da un lato, infatti, dovrà avere connotazioni di trasversalità (nozioni di tipo legale sono essenziali) mentre, dall'altro, dovrà essere in grado di garantire una technicality di primo livello, specie nell'attività correlata all'analisi forense. Queste caratteristiche professionali, unite ad un' interazione infungibile con le altre funzioni tecnologiche ed un adeguato supporto esterno, sono gli ingredienti del successo, sempre avendo un occhio a quello che sta arrivando.

*(Continua a pagina 15)*

(Continua da pagina 14)

### Le soluzioni e le sfide del futuro

Mentre, in questo momento storico, stanno partendo i primi progetti strutturati di incident management e digital investigation, le sfide dell'incident management aumentano in maniera esponenziale. Argomenti come Remote Incident Response sono ormai all'ordine del giorno, e le implicazioni forensi di questa disciplina sono valutate attentamente anche dalla comunità scientifica. Esistono progetti in corso (soprattutto negli Usa, ma anche nell'est Europeo e in Russia) che vedono banche e grosse aziende investire nell'investigazione remota, sia dal punto di vista procedurale sia di quello tecnologico.

In un momento storico in cui la convergenza tra sicurezza logica, fisica, protezione delle informazioni e controllo sono ormai un dato di fatto, è una sfida alla quale la professione non può sottrarsi.

### L'autore

Dario Forte, CISM, CFE, si occupa di sicurezza dal 1992. Dopo un lungo trascorso nelle Forze di Polizia (dove si è occupato di crimine organizzato e abusi tecnologici) ha fondato DFLabs, ([www.dflabs.com](http://www.dflabs.com)) un'azienda specializzata in prevenzione e gestione degli Incidenti e Information Security Risk Management. Docente di Gestione degli Incidenti Informatici all'Università di Milano, vanta collaborazioni con NASA ed Esercito statunitense. E' stato intervistato da numerosi media internazionali, tra cui Newsweek e Washington Times. E' socio AIEA.

***WWW.AIEA.IT***

Il nostro sito è stato premiato da ISACA con la medaglia d'oro.

Complimenti al nostro webmaster ed a tutti coloro che hanno collaborato.

***Webcast***

I *webcast* realizzati da ISACA sono stati archiviati e sono disponibili sul sito ([www.isaca.org/webcasts](http://www.isaca.org/webcasts)):

- Introduction to Information Security Architecture
- How to Carry Out a Strategic COBIT-based IT Risk Assessment
- An Overview of Threat and Vulnerability Analysis
- IT Risk Management: A Case of E-commerce Availability
- The IT Balanced Scorecard
- The Road Ahead: Living With Sarbanes-Oxley...Forever

L'aggiornamento conseguito attraverso un *webcast* consente di guadagnare un'ora di credito per la CPE delle certificazioni CISA e CISM.



***Corsi COBIT (nuova edizione)***  
***BASE a Milano il 18 e 19 ottobre 2005***  
***AVANZATO a Milano il 25 e 26 ottobre 2005***

**Obiettivi.** Il corso permette di acquisire una adeguata conoscenza su COBIT, finalizzata allo svolgimento di verifiche basate su questo framework. Il corso ha un carattere prevalentemente pratico: brevi sessioni informative saranno alternate ad esercitazioni.

I partecipanti, alla fine delle due giornate del corso BASE, saranno in grado di:

- \* individuare gli obiettivi di controllo pertinenti alla verifica di un processo, garantendo la completezza della verifica; divulgare all'interno della propria organizzazione l'utilizzo di COBIT quale supporto al perseguimento di un migliore sistema di controllo;
- \* inserire nei propri programmi di lavoro gli opportuni riferimenti a COBIT;
- \* e avranno chiari anche i limiti (di contenuto e di applicabilità) di COBIT;

alla fine delle due giornate del corso AVANZATO, saranno in grado di:

- preparare un programma di lavoro dettagliato per effettuare la verifica di un processo IT;
- misurare il livello di maturità di un processo IT;
- formulare dei suggerimenti per migliorare un processo IT, sulla base dei rischi individuati e del modello di maturità.

**Contenuto.** Il contenuto del corso Base riguarda: Implementation Toolset, Executive Summary, Framework, Control Objectives; il corso AVANZATO riguarda invece: Audit Guidelines e Management Guidelines.

**Destinatari:** IS auditor, Internal Auditor, Information Security Officer, Addetti alla sicurezza logica, Sistemisti, Analisti e Manager IT interessati ad acquisire una conoscenza approfondita di COBIT, il modello di governo dell'IT.

**Docenza:** Narduzzo Orillo, CISA, CISM, Vicepresidente AIEA, SEC SERVIZI, Pederiva Andrea, CISA, DELOITTE.

**Sede:** AIEA, Via Valla, 16, MILANO. Orario: 9-17.15.

**Durata:** corso BASE **18-19 ottobre 2005**, corso AVANZATO **25-26 ottobre 2005**.

La partecipazione a ciascun corso consente di guadagnare fino a 16 ore di credito nell'ambito del CISA/CISM Continuing Education.

Per informazioni: visita il sito [www.aiea.it](http://www.aiea.it), telefona alla segreteria AIEA (dalle ore 9 alle ore 12) al numero **02 84742.365** o invia un messaggio ad [aiea@aiea.it](mailto:aiea@aiea.it).

# *L'utilizzo del BS7799 nella valutazione del Sistema di Gestione della Sicurezza: il caso CRG di ICCREA Banca*

di Giuseppe Teti e Antonio Gaglione

*La prima parte è stata pubblicata sul precedente numero di InfoAIEA, il n.1 del 2005. Nel riquadro un breve riepilogo*

## **Abstract**

L'articolo illustra il metodo seguito presso il Gruppo Iccrea ed il movimento del Credito Cooperativo per eseguire le verifiche di conformità a requisiti normativi interni, derivati dallo standard internazionale per la gestione della sicurezza informatica BS7799, e relativi alle principali aree di gestione della sicurezza.

Il metodo ha introdotto il concetto di Modello di Maturità, legando la valutazione del Livello di Maturità delle aree di indagine al grado di conformità di Iccrea Banca e delle Strutture Tecniche (gestori informatici per conto delle Banche di Credito Cooperativo, di seguito BCC).

## **4. I risultati**

### **4.1 Modalità di esecuzione**

L'attività si è articolata nelle seguenti fasi:

- \* la rilevazione, mediante analisi documentale e mediante interviste con i referenti individuati per ciascuna area di indagine, dei principali presidi organizzativi e tecnici che soddisfacevano gli Obiettivi di Controllo di Alto Livello del Regolamento ed utilizzando le Specifiche di Dettaglio come "linee guida", eventualmente integrate o tradotte nel contesto aziendale;
- \* eventuale verifica a campione dell'effettiva esistenza dei presidi appena citati;
- \* elaborazione delle osservazioni e delle evidenze raccolte, aggregandole al livello di Obiettivi di Controllo di Alto Livello.

(Continua a pagina 18)

Un esempio di utilizzo dello standard BS7799 effettuato da ICCREA.

Prima parte: InfoAIEA n.1 del 2005

Seconda parte: InfoAIEA n.2 del 2005.

#### Riepilogo della prima parte.

Nella prima parte è stato illustrato il Sistema di Regolamento Contabile per il mondo delle BCC, per il quale ICCREA Banca ha definito il Regolamento Tecnico Operativo, basato su principi e raccomandazioni del BS7799. Sulla base delle 10 aree di questo standard sono state definiti gli Obiettivi di Controllo di Alto Livello ai quali è stato applicato il concetto di Maturity Model e concordando un livello target pari a 3 come rappresentativo di una buona conformità ai requisiti.

Le categorie di valutazione del livello di maturità sono le seguenti:

- \* regolamento del processo
- \* presenza ed efficacia della prassi
- \* presenza di controllo di conformità
- \* tecniche di supporto e livelli di automazione
- \* ambito di applicazione.



## **ICCREA Banca: BS7799 e valutazione dell'ISMS**

(Continua da pagina 17)

### **4.2 Modalità di esposizione**

I risultati sono stati esposti con due livelli di aggregazione, uno di sintesi ed uno di dettaglio. Nel livello di sintesi, per ciascun Obiettivo di Controllo di Alto Livello sono stati riportati, in una tabella di riepilogo:

- \* il livello di maturità osservato, inteso come grado di conformità ai requisiti: esso è stato calcolato, secondo la regola precedentemente esposta, in base alla valutazione quantitativa di ciascun ambito dell'Obiettivo di Controllo di Alto Livello;
- \* le principali osservazioni relative ai cinque ambiti d'analisi: la colorazione attribuita a ciascuna osservazione ne indica una preliminare valutazione qualitativa, ottenuta sulla base degli elementi riportati nei paragrafi successivi.

La tabella ha assunto l'aspetto della tabella n.3 (sono stati omessi i dettagli descrittivi ed è stata modificata, per motivi di riservatezza, la colorazione delle celle – indicativa della valutazione).

(Continua a pagina 19)

<b>OBIETTIVO</b>	<b>LIVELLO DI MATURITÀ RILEVATO</b>	<b>REGOLAMENTO PROCESSO</b>	<b>PRESENZA ED EFFICACIA DELLA PRASSI</b>	<b>PRESENZA DI CONTROLLO DI CONFORMITÀ</b>	<b>TECNICHE E AUTOMAZIONE</b>	<b>AMBITO DI APPLICAZIONE</b>
<i>Documentazione delle Procedure</i>	Valore numerico rilevato	Descrizione sintetica				
<i>Procedure per la gestione degli incidenti</i>						
<i>Separazione delle</i>						
<i>Separazione tra le funzioni di sviluppo e produzione</i>						
<i>Gestione delle strut-</i>						
<i>Protezione contro</i>						
<i>Gestione della rete</i>						
<i>Gestione dei supporti di memorizzazione</i>						
<i>Controllo degli ac-</i>						
<i>Autenticazione dei</i>						
<i>Procedura di controllo delle modifiche</i>						
<i>Housekeeping</i>						
<i>Gestione della conti-</i>						

**Tabella n.3—Quadro sinottico delle osservazioni**

***L'utilizzo del BS7799 nella valutazione del Sistema di Gestione della Sicurezza:  
il caso CRG di ICCREA Banca.***

(Continua da pagina 18)

**Legenda**

	Insufficiente		Da migliorare		Valore finale
--	---------------	--	---------------	--	---------------

L'opportuna colorazione delle celle, secondo la legenda riportata, ha consentito una immediata rappresentazione grafica del livello di maturità di ciascun Obiettivo di Controllo per ogni specifico ambito.

L'esposizione di dettaglio ha fornito, per ciascun Obiettivo di Controllo di Alto Livello:

1. il livello di maturità osservato;
2. la valutazione sintetica a fronte delle analisi svolte;
3. la valutazione per ciascuno dei cinque ambiti di analisi (sviluppo dimensionale del Modello di Maturità);
4. per ciascun ambito, gli elementi di rilevazione che supportano la valutazione data;
5. le aree di miglioramento.

Lo schema utilizzato per l'esposizione di dettaglio viene riportato nella tabella n.4.

## 5. Conclusioni

La Convenzione di Regolamento Giornaliero rappresenta il Sistema di Regolamento Contabile per il mondo delle BCC. Per la partecipazione a tale Sistema, Iccrea Banca e le BCC aderenti si sono impegnate ad applicare e rispettare criteri e raccomandazioni definite in un Allegato Tecnico che riprende il BS7799 Parte 1.

Per la verifica, da parte di Iccrea, della corretta applicazione delle prescrizioni è stato necessario introdurre un metodo comune e condiviso dalle parti, applicabile con facilità su realtà tecnicamente e dimensionalmente differenti, basato sui principi del Controllo Interno ma anche focalizzato sulla capacità di garantire un corretto funzionamento del Sistema.

Il metodo ha avuto un elevato grado di accettazione presso le strutture interessate, grazie alla facilità di applicazione ed alla strutturazione nella rilevazione dei dati e nell'esposizione dei risultati.

Pur nella consapevolezza di alcuni limiti intrinseci, derivanti dall'obiettivo dichiarato di attuare delle verifiche di conformità e non di introdurre un modello di ISMS conforme a quello proposto dal BS7799, l'attività ha contribuito alla diffusione del concetto di Sistema di Governo della Sicurezza dell'Informazione inteso come complesso di procedure attuato e mantenuto dall'organizzazione per garantire nel tempo il soddisfacimento dei requisiti di sicurezza concordati.

*Giuseppe Teti, CISA, IS Auditor in ICCREA Holding SpA*

*Antonio Gaglione, responsabile Ufficio Segreteria Tecnica di ICCREA Banca SpA*



***L'utilizzo del BS7799 nella valutazione del Sistema di Gestione della Sicurezza:  
il caso CRG di ICCREA Banca.***

**Tabella n.4 - Controllo Accessi**

**Tabella n.4.1 - Controllo Accessi: obiettivo di controllo**

**Obiettivo di controllo:** l'accesso alle informazioni e ai processi aziendali dovrebbe essere controllato sulla base dei requisiti di sicurezza e aziendali. Questa valutazione dovrebbe tenere conto delle politiche di diffusione delle informazioni e di autorizzazione.

Dovrebbero essere definite procedure formali per controllare l'utilizzo dei diritti di accesso ai sistemi informativi e ai servizi. Le procedure dovrebbero coprire tutti i passi del ciclo di vita di un accesso utente, dalla registrazione iniziale dei nuovi utenti alla cancellazione finale degli utenti che non richiedono più l'accesso ai sistemi informativi e ai servizi. Un'attenzione speciale dovrebbe essere dedicata al controllo dell'utilizzo dei diritti di accesso privilegiati che permettono, agli aventi tali diritti, di superare i controlli del sistema

**Tabella n.4.2 - Controllo Accessi: valutazione sintetica**

<b>Livello di maturità rilevato</b>	<b>Valutazione sintetica</b>
<i>Valore numerico del livello di maturità rilevato</i>	<i>Giudizio sinottico della situazione aziendale relativa all'Obiettivo di controllo analizzato</i>

**Tabella n.4.3 - Controllo Accessi: osservazioni**

<b>REGOLAMENTO PRO-CESSO</b>	<b>PRESENZA ED EFFICACIA DELLA PRASSI</b>	<b>PRESENZA DI CONTROLLO DI CONFORMI-</b>	<b>TECNICHE E AUTOMAZIONE</b>	<b>AMBITO DI APPLICAZIONE</b>
0				
1				
2	<i>Sintesi delle risultanze per l'ambito, coerenti con il valore indicato.</i>		<i>Sintesi delle risultanze per l'ambito, coerenti con il valore indicato.</i>	
3	<i>Sintesi delle risultanze per l'ambito, coerenti con il valore indicato.</i>			
4	<i>Sintesi delle risultanze per l'ambito, coerenti con il valore indicato.</i>		<i>Sintesi delle risultanze per l'ambito, coerenti con il valore indicato.</i>	
5				

## ICCREA Banca: BS7799 e valutazione dell'ISMS

(continua da pagina 20)

### Tabella n.4.4 - Controllo Accessi: dettaglio dell'analisi per ambito di applicazione

#### Regolamento processo

Viene riportato il dettaglio dell'analisi.

Vengono indicate le aree di miglioramento rilevate, ai fini di innalzare il livello di maturità dell'ambito.

Viene riportato il valore del livello di maturità.

#### Presenza ed efficacia della prassi

Viene riportato il dettaglio dell'analisi.

Vengono indicate le aree di miglioramento rilevate, ai fini di innalzare il livello di maturità dell'ambito.

Viene riportato il valore del livello di maturità.

#### Presenza di controllo di conformità

Viene riportato il dettaglio dell'analisi.

Vengono indicate le aree di miglioramento rilevate, ai fini di innalzare il livello di maturità dell'ambito.

Viene riportato il valore del livello di maturità.

#### Tecniche di supporto e livelli di automazione

Viene riportato il dettaglio dell'analisi.

Vengono indicate le aree di miglioramento rilevate, ai fini di innalzare il livello di maturità dell'ambito.

Viene riportato il valore del livello di maturità.

#### Ambito di applicazione

Viene riportato il dettaglio dell'analisi.

Vengono indicate le aree di miglioramento rilevate, ai fini di innalzare il livello di maturità dell'ambito.

#### Nota. La determinazione del livello.

Un punteggio complessivo per l'Obiettivo di Controllo di Alto Livello, interpretabile come indicatore sintetico della conformità dell'azienda all'Obiettivo di Controllo, è stato ottenuto mediante una media pesata dei punteggi assegnati a ciascun ambito. Il peso indica l'importanza dell'ambito ai fini della valutazione dell'Obiettivo di Controllo.

In termini matematici, la media ponderata è stata ottenuta come

$$M_p = \frac{\sum_{i=1}^n v_i P_i}{\sum_{i=1}^n P_i}$$

in cui  $M_p$  rappresenta il valore finale della media ponderata,

$n$  è il numero di ambiti considerati nella media (eventualmente inferiore a 5 nel caso di ambiti non applicabili),  $v_i$  è il punteggio assegnato all' $i$ -esimo ambito,  $p_i$  è il peso dell' $i$ -esimo ambito.



## Sessioni di studio

Roma - 26 gennaio 2005

Monte Dei Paschi di Siena  
Sala Convegni di Via Minghetti 30A

### PROGRAMMA

- 14.15 Introduzione dei lavori da parte del Chairman (Donatella Rosa Vicepresidente AIEA)
- 14.30 **Giancarlo Turati (Fasternet)**  
*Le nuove frontiere della sicurezza: la telefonia IP, intercettazioni, configurazioni, contromisure*
- 15.20 **Corrado Degani (Monte dei Paschi di Siena)**  
*Il Disaster Recovery nel Consorzio Operativo Gruppo MPS*
- 16.10 Pausa caffè
- 16.25 **Michele Bianco (BULL)**  
*L'An ISMS Framework for Enterprise Organizations*
- 17.15 Dibattito con i relatori
- 17.45 Conclusione dell'incontro a cura del Chairman
- 17.50 Termine dei lavori



## Sessioni di studio

Milano - 28 gennaio 2005

Unicredit Servizi Informativi  
Via Livio Cambi, 1

### PROGRAMMA

- 14.15 Introduzione dei lavori da parte del Chairman
- 14.30 **Luigi Brusamolino (Symantech)**  
*I nuovi fenomeni di Cybercrime: fraud & phishing*
- 15.20 **Corrado Degani (Monte dei Paschi di Siena)**  
*Il Disaster Recovery nel Consorzio Operativo Gruppo MPS*
- 16.10 Pausa caffè
- 16.25 **Edoardo Chiesa (Sacitel)**  
*Applicazione di CobiT in attività di analisi dei rischi aziendali*
- 17.15 Dibattito con i relatori
- 18.15 Conclusione dell'incontro a cura del Chairman
- 18.20 Termine dei lavori



## Sessioni di studio

Torino - 8 marzo 2005

R.S.I. Sistemi  
Corso Stati Uniti, 29

### PROGRAMMA

- 9.15 Introduzione dei lavori da parte del Chairman
- 9.30 **Siro Tasca (Protiviti)**  
*Adeguamento al Sarbanes-Oxley Act: requisiti normativi ed impatti per le imprese italiane*
- 10.20 **Daniela Werling (Gruppo Telecom)**  
*L'esperienza Telecom*
- 11.10 Pausa caffè
- 11.30 **Stefano Arduini (KPMG)**  
*Disegno ed efficacia dei controlli IT sul Financial Reporting: le attività di audit*
- 12.30 Pausa pranzo
- 14.00 **Ada Di Sario (FIAT REVI)**  
*Sarbanes-Oxley Compliance per i sistemi informativi: l'esperienza del Gruppo Fiat*
- 15.00 **Franco Rasello (Integra)**  
*Aspetti operativi dell'analisi e dell'adeguamento SOX per i sistemi informativi*
- 16.00 Dibattito con gli oratori e conclusione dell'incontro a cura del Chairman
- 16.30 Termine dei lavori



## Sessioni di studio

Roma - 9 marzo 2005

Monte Dei Paschi di Siena  
Sala Convegni di Via Minghetti 30A

### PROGRAMMA

- 14.15 Introduzione dei lavori da parte del Chairman (Donatella Rosa Vicepresidente AIEA)
- 14.30 **Roberto Mircoli (Cisco System)**  
*Network Security: Situazione e Prospettive*
- 15.20 **Gianpiero Giacobino (Telecom Italia Learning Services)**  
*E-learning e Sicurezza*
- 16.10 Pausa caffè e consegna PIN
- 16.25 **MRaffaella D'Alessandro (Ernst & Young)**  
*Privacy e Sicurezza nei servizi in outsourcing*
- 17.15 Dibattito con i relatori
- 18.15 Conclusione dell'incontro a cura del Chairman
- 18.20 Termine dei lavori





## Sessioni di studio

Milano - 18 marzo 2005

Unicredit Servizi Informativi  
Via Livio Cambi, 1

### PROGRAMMA

14.30 Introduzione dei lavori da parte del Chairman

14.45 **Luigi Neirotti (Ernst & Young)**

*Leggi e norme aggiornate alla base dello sviluppo del Paese:  
i certificati digitali uno strumento strategico*

15.45 Domande e dibattito con i relatori

16.00 Pausa caffè

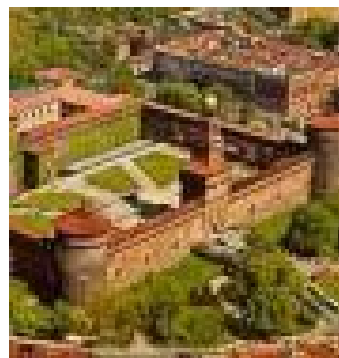
16.15 **Massimo Chiusi (Gruppo Unicredit)**

*La firma digitale: applicazioni in ambito bancario*

17.15 Domande e dibattito finale con i relatori

17.45 Conclusione dell'incontro a cura del Chairman

17.50 Termine dei lavori



## Sessioni di studio

Firenze - 6 aprile 2005

Monte dei Paschi di Siena  
via dei Pecori, 6/8

### PROGRAMMA

14.15 Introduzione dei lavori da parte del Chairman (Francesco Santiloni—Consigliere AIEA)

14.30 **Marco Gori (Presidente dell'associazione AI\*IA)**

*Introduzione all'Intelligenza Artificiale: cenni storici e principali paradigmi*

15.20 **Piero Poccianti (Consorzio Operativo Gruppo MPS)**

*Applicazioni dell'Intelligenza Artificiale: esperienze e strumenti utilizzabili*

16.10 Pausa caffè

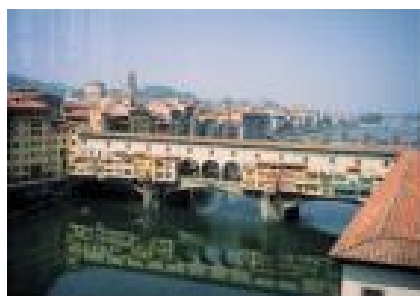
16.25 **Fabio Massacci (Università di Trento)**

*Enterprise Privacy Policies: gestire politiche organizzative di privacy con il supporto di  
tecniche di ragionamento automatico*

17.15 Dibattito con i relatori

18.15 Conclusione dell'incontro a cura del Chairman

18.20 Termine dei lavori



## Sessioni di studio

Milano - 15 aprile 2005

Auditorium SIA—ACTALIS  
Via Taramelli 26

### PROGRAMMA

- 14.15 Introduzione dei lavori da parte del Chairman
- 14.30 **Roberto Mircoli (Cisco System)**  
*Network Security: Situazione e Prospettive*
- 15.20 **Adalgisa Di Sario, CISA (Fiat Revi)**  
*Sarbanes-Oxley Compliance per i sistemi informativi: l'esperienza del Gruppo Fiat*
- 16.10 Pausa caffè
- 16.25 **Francesco Faenzi, CISA (Lutech)**  
*Risk Analysis "for dummies": chi coinvolgere, cosa chiedere, come documentare i risultati, dove si va a finire?*
- 17.30 Dibattito con i relatori
- 18.15 Conclusione dell'incontro a cura del Chairman
- 18.20 Termine dei lavori



## Sessioni di studio

Roma - 20 aprile 2005

Monte Dei Paschi di Siena  
Sala Convegni di Via Minghetti 30A

### PROGRAMMA

- 14.15 Introduzione dei lavori da parte del Chairman (Donatella Rosa Vicepresidente AIEA)
- 14.30 **Luigi Vedani**  
*Sarbanes Oxley Act, ovvero sistemi di controllo interno sui "financial statements"*
- 15.20 **Fabrizio Matta (Business-e)**  
*Monitoraggio della sicurezza: criteri per la classificazione degli allarmi e la gestione degli incidenti*
- 16.10 Pausa caffè
- 16.30 **Marco Recchia (Banca Antonveneta)**  
*L'auditing dei BCP: problematiche*
- 17.00 **Anthony C. Wright (BNL e Presidente ANSSAIF)**  
*Business Continuity: ... e se parlassimo di "best practice"?*
- 17.30 **Mario Sestito (ICCREA Banca)**  
*L'Il recente rapporto CNIPA sul rischio informatico: spunti di interesse; quali contributi ai progetti di Business Continuity*
- 18.00 Dibattito con i relatori
- 18.30 Termine dei lavori





**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**

2005, Volume 3 n.2  
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  
Hanno collaborato: Antonio Gaglione,  
Orillo Narduzzo, Donatella Rosa,  
Giuseppe Teti.

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, .....

**SCRIVETEICI!!**

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 Nazionale 2004-2006**

Presidente: Silvano Ongetta  
Vice presidenti: Donatella Rosa,  
Orillo Narduzzo  
Segretario: Enzo Toffanin  
Tesoriere: Aureliana Radaelli

**Consiglieri:**

Emanuele Boati, Daniela Cellino,  
Francesco Galli, Angelo Rodaro,  
Francesco Santiloni

**Probiviri:**

Francesco Blanco, Daniela Landini,  
Enrico Schiocchet



**ISACA**

Information Systems Audit and Control Association

**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.*