



# InfoAIEA

**AIEA**  
**Capitolo ISACA**  
**di Milano**

Dicembre 2004

## Venticinque e non li dimostra

di *Silvano Ongetta*

Per un'Associazione professionale come la nostra 25 anni potrebbero rappresentare un lasso di tempo sufficiente per non riuscire più a nascondere gli acciacchi e/o i segni di stanchezza. Credo in tutta coscienza che ciò non ci possa riguardare e che gli eventi/attività che siamo riusciti a organizzare quest'anno siano la miglior riprova – la nostra cartina di Tornasole.

### Eventi/attività:

**Associazioni** – continua la collaborazione con il CLUSIT (fa piacere vedere che ben 7 soci AIEA siano presenti nell'attuale direttivo) - proseguono i contatti con l'Associazione Italiana Internal Auditor ed abbiamo avviato contatti con l'ANSSAIF (Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria) e con SINCERT con cui abbiamo organizzato un convegno durante il mese di marzo.

**Bancaforte** - numerosi associati hanno usufruito della possibilità di abbonarsi gratuitamente alla rivista edita dall'ABI

**CISA - CISM** - abbiamo proceduto alla traduzione del manuale CISA, come è ormai da anni prassi con-

*(Continua a pagina 2)*

## In questo numero



Continuiamo anche in questo numero le celebrazioni per i 25 anni di AIEA con l'editoriale del Presidente: AIEA è nata il 20 dicembre 1979 e il "Silver Jubilee" ricorre proprio in questo mese. Grande evoluzione anche per COBIT®: in questo mese viene rilasciata la versione 3.2 di COBIT Online: nuove funzionalità e nuovi contenuti, per auditor e per manager.

Concludiamo il tema dell'IT Governance con la traduzione di Pederiva dell'articolo su IT Governance e Outsourcing dal Control Journal. Le analogie tra il controllo e la qualità sono trattate dall'articolo di Rosa che descrive l'evoluzione dei sistemi per la qualità.

Le nostre certificazioni, CISA® e CISM®, si stanno affermando a livello mondiale, l'articolo di Macartney ci illustra le loro caratteristiche e la ragione di questo successo.

### Sommario:

Volume 2 numero 4

Dicembre 2004

Venticinque e non li dimostra <i>di S. Ongetta</i>	1
COBIT® Online 3.2	1
Il Governo dell'Outsourcing IT <i>di A. Pederiva</i>	4
Il Governo dell'Outsourcing IT <i>di H. Parkers</i>	5
CISA® and CISM®: Internationally Recognized for Future Success <i>di Leslie Macartney</i>	13
Qualità dei servizi, qualità dei sistemi e controlli <i>di Donatella Rosa</i>	16
Sessioni di studio	19

## COBIT® Online Release 3.2

Sul sito [ww.isaca.org](http://ww.isaca.org) è stata rilasciata la *release* 3.2 di COBIT ON LINE, nuove funzionalità a disposizione degli associati ISACA e dei sottoscrittori del servizio. La nuova *release* comprende i benefici e le funzioni della precedente versione e aggiunge parecchie nuove possibilità.

*(Continua a pagina 3)*





## *Venticinque e non li dimostra*

*di Silvano Ongetta*

*(Continua da pagina 1)*

solidata ed è stato anche quest'anno inserito nel Bookstore ISACA e proceduto anche alla traduzione (non ufficiale) del manuale CISM in tal modo i colleghi che hanno affrontato le sessioni di esame 2004 hanno avuto un adeguato supporto di studio.

**COBIT** - abbiamo completato la traduzione del COBIT v.3 (Management Guidelines, Executive Summary, Framework and Control Objectives), che si è proceduto a mettere a disposizione di tutti i soci e stiamo attualmente completando la traduzione dell'ultimo volume: l'Implementation Toolset. Anche quest'ultimo sarà incluso, soddisfatte le pratiche amministrative, nel Bookstore di ISACA.

**Convegni** - abbiamo partecipato ad alcuni Convegni organizzati da altre organizzazioni:

febbraio	Convegno Jekpot - Milano
marzo	Convegno organizzato con il nostro contributo da Sincert (Sistema Nazionale per l'Accreditamento degli Organismi di Certificazione e Ispezione) - Milano
maggio	Stati Generali delle Associazioni - Roma
ottobre	3° Global Security Conference di IBM - Milano
novembre	4° Italian Cyberspace Law Conference - Bologna
dicembre	Sicurezza Digitale c/o la Unindustria - Treviso

**Gruppi di Ricerca** - il Gruppo di Ricerca ISMS ha concluso brillantemente i suoi lavori così anche quello relativo alle Leggi Informatiche, mentre gli altri tre Gruppi (Outsourcing IT: Best practice e Auditing - Il valore dei penetration test dal punto di vista dell'Auditor - L'auditing dei sistemi OpenSource) dovrebbero produrre il loro output entro la prossima primavera.

**GRA** - Governmental and Regulatory Agencies Board – James Cheyne partecipa alla task force per il progetto relativo al "Chapter Government Liason" per il coordinamento delle attività di contatto con gli enti governativi.

**Newsletter** - ad InfoAIEA si è affiancata la Newsletter avente cadenza mensile che raccoglie informazioni da KNET - il bollettino del Garante della Privacy quello del CNIPA e la newsletter del CLUSIT.

**Numero associati** - il numero degli associati ha superato di slancio quota 400 – ora siamo in 433 .....non ci poniamo limiti.

**CPE hours Continuing Education** (Ore per le qualifiche) - sono state messe a disposizione dei soci per il mantenimento delle loro qualifiche più di 80 ore di Continuing education.

**Patrocinio** – AIEA ha patrocinato la Survey sull'IT Governance svolta dalla PWC.

**Regolamento Esecutivo** – abbiamo finalizzato la redazione del documento che regola la vita del Consiglio Direttivo e del Comitato dei Proviviri.

**Riconoscimenti** – con rischio di inorgoglierci troppo abbiamo ricevuto da ISACA tre prestigiosi attestati: il "K. Wayne Snipes Award for the best Large Charter for Europa/Africa", il "Best Newsletter Award worldwide" in the Large Chapter category per InfoAIEA e per non farci mancare proprio nulla il "Silver award" per il sito web.

*(Continua a pagina 3)*

## *Venticinque e non li dimostra*

*di Silvano Ongetta*

(Continua da pagina 2)

L'ho già detto e lo ribadisco il miglior attestato per l'Associazione è il vostro apprezzamento.

**Scuola AIEA** - il corso per la preparazione all'esame CISA è stato tenuto sia a Roma sia a Milano per complessive 20 giornate di docenza mentre per il corso CISM il corso ha avuto uno svolgimento di un numero minore di giorni. Oltre ai sopra citati corsi si è svolto a Milano il corso COBIT base e quello Avanzato; il tutto sarà riproposto ovviamente a Roma in febbraio-marzo 2005.

**Sessioni di Studio** - si sono svolte 14 Sessioni di Studio: 6 a Milano e altrettante Roma, una a Venezia e una in Svizzera in collaborazione con l'associazione locale ATED e il capitolo elvetico.

**SOX** – Stiamo ultimando il controllo qualità della traduzione del libretto "IT Control Objectives for Sarbanes-Oxley" edito da ISACA di cui abbiamo avuto una preziosa presentazione da Robert Roussey durante il Convegno di Cortona.

**Statuto** – abbiamo rivisto lo Statuto per allinearli alle attuali esigenze e anche per meglio conformarci al bylaws consigliato da ISACA. Nella prossima Assemblea il testo, dopo che vi sarà stato inviato in anticipo per consentirvi un'attenta lettura, sarà sottoposto al vostro esame e quindi alla votazione.

### **Conclusione**

Il mese scorso durante la pausa caffè di una Sessione di Studio un associato di *antica data* ha espresso una considerazione che ho trovato molto gratificante: "anni fa l'AIEA era in fondo un club di amici ora siamo un'Associazione".

Se mi concedete di riassumere in poche righe quanto vi ho sopra riportato, posso dire che benché siamo "over 25" abbiamo ancora tanto fiato, grinta a volontà e voglia di migliorare e di crescere, insomma quello che ci si aspetta da un'Associazione a tutti gli effetti giovane.

Personalmente anch'io vorrei avere venticinque anni, mi accontenterei di .... dimostrarli tutti ma ahimè sembra che non sia possibile.

## *COBIT Online Release 3.2*



Sul sito [ww.isaca.org](http://ww.isaca.org) è stata rilasciata la *release* 3.2 di COBIT ON LINE, nuove funzionalità a disposizione degli associati ISACA e dei sottoscrittori del servizio. La nuova *release* comprende i benefici e le funzioni della precedente versione e aggiunge le seguenti nuove funzionalità:

- \* migliori e più avanzate modalità di benchmark
- \* "perché applicare un controllo" a livello di framework
- \* migliorate funzionalità di personalizzazione (filtering)
- \* accesso più facile alle "Pratiche di controllo IT"
- \* possibilità di scaricare dei db access modificabili contenenti le informazioni del modello.



## Il Governo dell'Outsourcing IT

Introduzione alla traduzione dell'articolo di **Hugh Parkers, CISA, FCA**, tratto da *Control Journal*, rivista bimestrale di *ISACA*, volume 5 del 2004.

di A. Pederiva

Un bel articolo, di natura introduttiva, per un tema affascinante: la gestione della relazione fra outsourcer ed outsourcee. Una relazione che può essere difficile, così come può portare a grandi soddisfazioni e vantaggi per entrambe le parti.

La relazione che si instaura nell'ambito dei contratti di outsourcing è se vogliamo speculare; gli stessi punti di attenzione debbono essere presi in considerazione da entrambe le parti, naturalmente con obiettivi e interessi diversi, talvolta convergenti, spesso divergenti.

Ecco perché gli strumenti e le modalità di governo di tale relazione sono fondamentali: si tratta di fare sintesi di una pluralità di fattori (di tipo organizzativo, economico, legale, tecnologico, e umano) che debbono essere congruenti con le aspettative e le possibilità di due soggetti a loro volta complessi e con esigenze talvolta contrastanti.

L'articolo di Parkes sottolinea in particolare tre aspetti. Il primo, è il fatto che nelle relazioni di outsourcing rischi e contromisure (sistema di governo e controllo interno) poste in essere dal management sono il relazione alla criticità dei sistemi e dei processi esternalizzati. In particolare, al livello più alto di criticità l'autore pone l'esternalizzazione del sistema informativo incluse le attività di gestione dei dati (es.: gestione delle anagrafiche, data entry, etc.), mentre al livello più basso di criticità l'autore pone l'esternalizzazione della manutenzione delle periferiche utente (PC, terminali, etc.).

Il secondo aspetto, è che una volta individuato il sistema di governo più appropriato per la specifica relazione di outsourcing, le parti si debbono dotare di un adeguato sistema di reporting relativo allo stato ed al funzionamento in termini di efficacia ed efficienza del sistema di controllo interno. Tale reporting evidentemente è complementare al reporting sul soddisfacimento nel tempo dei livelli contrattuali concordati; infatti, il reporting sul sistema di controllo interno si può considerare come una sorta di analisi sulla capacità futura di continuare a soddisfare i livelli di servizio concordato.

Il terzo aspetto, infine, è che il reporting destinato al management deve essere sintetico, e riportare con immediatezza gli elementi rilevanti e su cui il management deve intervenire. Parkes propone di utilizzare la grafica, ed anche se i diagrammi presentati nell'articolo sono didascalici, purtuttavia nello spazio a disposizione fanno vedere bene come con la grafica si possano trasmettere i messaggi desiderati in modo veloce ed efficace.

### Bibliografia:

- \* [La qualità e i contratti per l'informatica](#)  
La Banca e il Sistema Informativo Contratti e Garanzia di qualità - Edizioni ABI, 2002
- \* [Guida all'outsourcing in banca: sicurezza e servizi tecnici](#)  
Autore: Marcello Giustiniani, Guido Maria Rossi – Edizioni ABI, 1998
- \* [La banca e il sistema informativo: l'outsourcing della manutenzione del software](#) - Edizioni ABI, 1999
- \* [La banca e il sistema informativo: manutenzione massiva del software](#) - Edizioni ABI, 1999
- \* [Bancaforte n° 6/2002 – Speciale Outsourcing](#) - Edizioni ABI
- \* [Shaping the It Organization: The Impact of Outsourcing and the New Business Model](#)  
Autore: Ian Gouge - Edizioni Springer-Verlag (Luglio 2003) - ISBN 1852337273
- \* [Successful It Outsourcing: From Choosing a Provider to Managing the Project](#)  
Autore: Elizabeth Sparrow – Edizioni Springer-Verlag (Agosto 2003) - ISBN: 1852336102

IT Governance

## Il Governo dell'Outsourcing IT

di **Hugh Parkers, CISA, FCA**

Da *Control Journal*, rivista bimestrale di *ISACA*, volume 5 del 2004.  
Liberamente tradotto da A. Pederiva (\*)

L'IT Governance è una componente della corporate governance. Si riferisce agli strumenti ed all'efficacia con cui un'organizzazione governa e controlla le attività che richiedono l'impiego di sistemi informativi. L'importanza dell'IT Governance è evidente: sia nel privato che nella pubblica amministrazione vi sono ormai poche attività davvero importanti che non siano supportate da sistemi informativi; in molti casi, come ad esempio nel commercio elettronico, l'IT si è financo componente costitutiva essenziale del processo stesso.

E' importante sottolineare che l'IT Governance determina come tutti gli aspetti che interessano l'IT debbono essere controllati, e non si limita pertanto alle attività della Direzione dei sistemi informativi, né al solo governo dell'infrastruttura tecnologica. In effetti, l'IT Governance è destinata ad assicurare la disponibilità e l'utilizzo efficace ed efficiente di tutte le informazioni necessarie al successo del business.

L'outsourcing, o esternalizzazione, nella sua forma più comune si concretizza nella stipula di un accordo con una organizzazione terza a cui vengono affidate una o più attività precedentemente svolte da unità organizzative interne.

E' noto che possono essere esternalizzate attività di varia natura e che anche la forma dei contratti può variare considerevolmente in ragione dei diversi meccanismi e parametri utilizzati per la gestione della relazione fra outsourcee e outsourcer.

Società adeguatamente organizzate non dovrebbero incontrare particolari difficoltà nell'entrare in relazione con altre società parimenti strutturate, fermo restando che lo sforzo necessario dal punto di vista legale sarà in ogni caso significativo, sia per definire opportunamente le clausole contrattuali, sia per definire le modalità con cui il rispetto di tali clausole sarà verificato nel durante della vita del contratto.

Tuttavia, le Direzioni delle società in procinto di sottoscrivere un contratto di outsourcing dovranno verificare reciprocamente se nelle rispettive esperienze siano state in grado di conseguire od assicurare il raggiungimento degli obiettivi che si sono poste nel determinare le decisioni di tipo strategico che hanno portato alla scelta di esternalizzare o di erogare il servizio a terzi.

(Continua a pagina 6)



## Il Governo dell'Outsourcing IT

di Hugh Parkers, CISA, FCA

Da *Control Journal*, rivista bimestrale di *ISACA*, volume 5 del 2004.  
Liberamente tradotto da A. Pederiva (\*)

(Continua da pagina 5)

### Elementi di IT Governance di rilievo per Società che esternalizzano

La sensibilità dell'Alta Direzione rispetto alla necessità di un'IT Governance efficace dipende dall'importanza che le attività e le risorse esternalizzate rivestono rispetto al conseguimento degli obiettivi dell'organizzazione.

Se quanto esternalizzato rappresenta una commodity o un servizio facilmente rimpiazzabile (es.: il servizio di pulizie degli uffici IT..., eccetto che per i rischi di intrusione fisica), allora eventuali difficoltà possono essere facilmente superate sostituendo il fornitore, senza incorrere in particolari rischi.

Qualora invece il servizio esternalizzato sia vitale per la capacità operativa dell'organizzazione, allora gli aspetti di IT Governance e la gestione del reporting sulla qualità del servizio ottenuto diventano essenziali.

In Figura 1 sono indicati numerosi tipi di attività che possono essere esternalizzate; per ciascun tipo di attività sono elencati alcuni fra i principali rischi associati all'esternalizzazione, e per lo stesso tipo di attività sono suggeriti alcuni elementi di IT Governance che in caso di esternalizzazione dovrebbero essere presi in considerazione.

**Figura 1 – Rischi e Punti di Attenzione per l'Outsourcing**

Attività esternalizzate	Rischi associati all'esternalizzazione	Punti di attenzione sull'IT Governance per il management
1. Esternalizzazione dei sistemi informativi e della gestione dei dati (tutte le basi dati, incluse le anagrafiche, i sistemi transazionali, etc.)	<p>Rischio molto alto (in relazione alla criticità delle informazioni la cui gestione è esternalizzata)</p> <ul style="list-style-type: none"> <li>* Conseguenze derivanti dalla perdita o dall'accesso non autorizzato ai dati esternalizzati</li> <li>* Impatto immediato</li> <li>* Esposizione ad un ampio spettro di rischi, inclusi la perdita, il furto, la perdita di integrità, il possibile accesso da parte di competitori</li> <li>* Potere negoziale dell'outsourcer derivante dalla dipendenza dai sistemi informativi</li> </ul>	<ul style="list-style-type: none"> <li>* Clausole contrattuali relative a sicurezza e controllo degli accessi, nonché alla proprietà dei dati</li> <li>* Misure per il backup e il disaster recovery, incluse le modalità di collaudo e documentazione dei risultati del collaudo (anche mediante attestazione del management dell'outsourcer)</li> <li>* Misure di sicurezza relativamente ai dati ed alle modalità di accesso ai dati</li> <li>* Modalità di gestione dei dati (conservazione, utilizzo, monitoraggio dello stato dei dati – rappresentano un asset in custodia presso terzi)</li> <li>* Capacità di utilizzo delle informazioni (incluso il data mining), adeguatezza del patrimonio informativo disponibile rispetto alle esigenze dell'organizzazione utente, capacità di integrare le informazioni disponibili al fine di assicurare la migliore efficienza ai processi dell'organizzazione utente</li> <li>* Compatibilità con gli obiettivi strategici del costo del servizio esternalizzato in relazione al servizio ottenibile</li> </ul>

## Il Governo dell'Outsourcing IT

di **Hugh Parkers, CISA, FCA** da *Control Journal*, rivista bimestrale di *ISACA*, volume 5 del 2004.  
Liberamente tradotto da A. Pederiva (\*)

**Figura 1 – Rischi e Punti di Attenzione per l'Outsourcing (continua)**

Attività esternalizzate	Rischi associati all'esternalizzazione	Punti di attenzione sull'IT Governance per il management
<p>2. Sistemi di knowledge management aziendali quali archivi di documentazione amministrativa (storia aziendale), archivi di documenti tecnici (progettazione di prodotto, tecnologie di processo o altro know how aziendale), archivi di documenti riservati relativi alle attività riservate del management (ad es. per la corrispondenza riservata)</p>	<p>Rischio alto o molto alto (in relazione alla criticità dei documenti la cui gestione e archiviazione elettronica è stata esternalizzata)</p> <ul style="list-style-type: none"> <li>* Rischi di furto di proprietà intellettuale, disfunzionalità dei processi sviluppo/utilizzo del know aziendale</li> <li>* Perdita di credibilità come conseguenza della dipendenza da terzi per lo sviluppo di nuovi progetti aziendali (ad es., in caso di esternalizzazione dei sistemi di progettazione)</li> </ul>	<ul style="list-style-type: none"> <li>* Misure per il backup e il disaster recovery, incluse le modalità di collaudo e documentazione dei risultati del collaudo (anche mediante attestazione del management dell'outsourcer)</li> <li>* Misure di sicurezza relativamente ai dati ed alle modalità di accesso ai dati (incluse le modalità di accesso da remoto)</li> <li>* Dipendenza dall'outsourcer per lo sviluppo e la manutenzione di nuovi sistemi; comprensione della localizzazione delle competenze</li> <li>* Modalità di gestione dei progetti per nuovi sistemi e prestazioni realizzabili (efficienza del "motore IT" dell'azienda)</li> <li>* Verifica presso terzi della capacità dell'outsourcer di rispettare i livelli di servizio concordati</li> </ul>
<p>3. Esternalizzazione dei principali sistemi hardware e dei servizi a supporto</p>	<p>Rischio medio-alto</p> <ul style="list-style-type: none"> <li>* Grandi centri di elaborazione dati, gestiti da outsourcer affermati e di dimensioni adeguate, possono ridurre i rischi legati alle operations IT grazie alle economie di scala, all'esperienza, a processi di gestione dell'IT appropriati ed alla specializzazione dei processi di supporto</li> <li>* Le società che esternalizzano debbono assicurarsi che le facility dell'outsourcer siano gestite in modo adeguato e concordare contrattualmente le modalità di accesso a fini di verifica, anche per il tramite di terze parti indipendenti dotate di adeguate competenze</li> <li>* Rischi specifici possono emergere qualora l'organizzazione utente non monitori il servizio ricevuto o lo stato al passare del tempo dei sistemi informatici sui quali fa affidamento</li> </ul>	<ul style="list-style-type: none"> <li>* Accordi per il backup ed il disaster recovery contrattualizzati, incluse le modalità di collaudo e verifica degli esiti dei collaudi</li> <li>* Esame dei rapporti sui risultati delle verifiche di terze parti, incluse le verifiche su prestazioni e livelli di servizio</li> <li>* Verifiche presso altri utenti sul rispetto da parte del potenziale outsourcer dei livelli di servizio concordati</li> </ul>



## Il Governo dell'Outsourcing IT

di Hugh Parkers, CISA, FCA

Da *Control Journal*, rivista bimestrale di *ISACA*, volume 5 del 2004.  
Liberamente tradotto da A. Pederiva (\*)

**Figura 1 – Rischi e Punti di Attenzione per l'Outsourcing (continua)**

Attività esternalizzate	Rischi associati all'esternalizzazione	Punti di attenzione sull'IT Governance per il management
4. Esternalizzazione di reti e sistemi di comunicazione	<p>Rischio medio-alto</p> <ul style="list-style-type: none"> <li>* Rischi di accesso illegale o a scopo di danneggiare, attacchi di tipo denial-of-service, perdita di integrità delle informazioni, furto di proprietà intellettuale, virus, worm, trojan e altro malicious software.</li> <li>* Rischio di presenza di single point of failure</li> <li>* Possibile rallentamento dei processi aziendali o ritardi nel servizio ai clienti dovuti a insufficiente capacità di trasmissione delle informazioni</li> </ul>	<ol style="list-style-type: none"> <li>1 Accordi per il backup ed il disaster recovery contrattualizzati, incluse le modalità di collaudo e verifica degli esiti dei collaudi</li> <li>2 Sicurezza delle reti di comunicazione, delle connessioni ad Internet (ISPs), sicurezza dei siti web aziendali</li> <li>3 Adeguatezza della banda di rete o comunque della capacità di trasmissione delle informazioni rispetto alle esigenze aziendali presenti e pianificate</li> <li>4 Verifiche presso altri utenti sul rispetto da parte del potenziale outsourcer dei livelli di servizio concordati</li> </ol>
5. Fornitura di apparecchiature e sistemi hardware, PC, server, terminali e apparecchiature di rete	<p>Di norma rischio moderato</p> <ul style="list-style-type: none"> <li>* Disponibilità di fornitori alternativi</li> <li>* Il servizio concordato non soddisfa nel tempo i bisogni aziendali</li> <li>* Servizi carenti possono ridurre la produttività</li> <li>* I sistemi utilizzati/messi a disposizione dall'outsourcer non vengono aggiornati nel tempo</li> </ul>	<ul style="list-style-type: none"> <li>* Conformità ai termini contrattuali (servizio erogato/ pagamenti effettuati – eventuali conflitti vengono di norma risolti dal middle management)</li> <li>* Attenzione dell'Alta Direzione richiesta solo in caso di gravi difficoltà, di norma per la necessità di finanziare il ripristino dell'operatività corrente</li> </ul>

## Il Governo dell'Outsourcing IT

di **Hugh Parkers, CISA, FCA** Da *Control Journal*, rivista bimestrale di *ISACA*, volume 5 del 2004.

Liberamente tradotto da A. Pederiva (\*)

(Continua da pagina 7)

### Reporting semplice, chiaro ed efficace

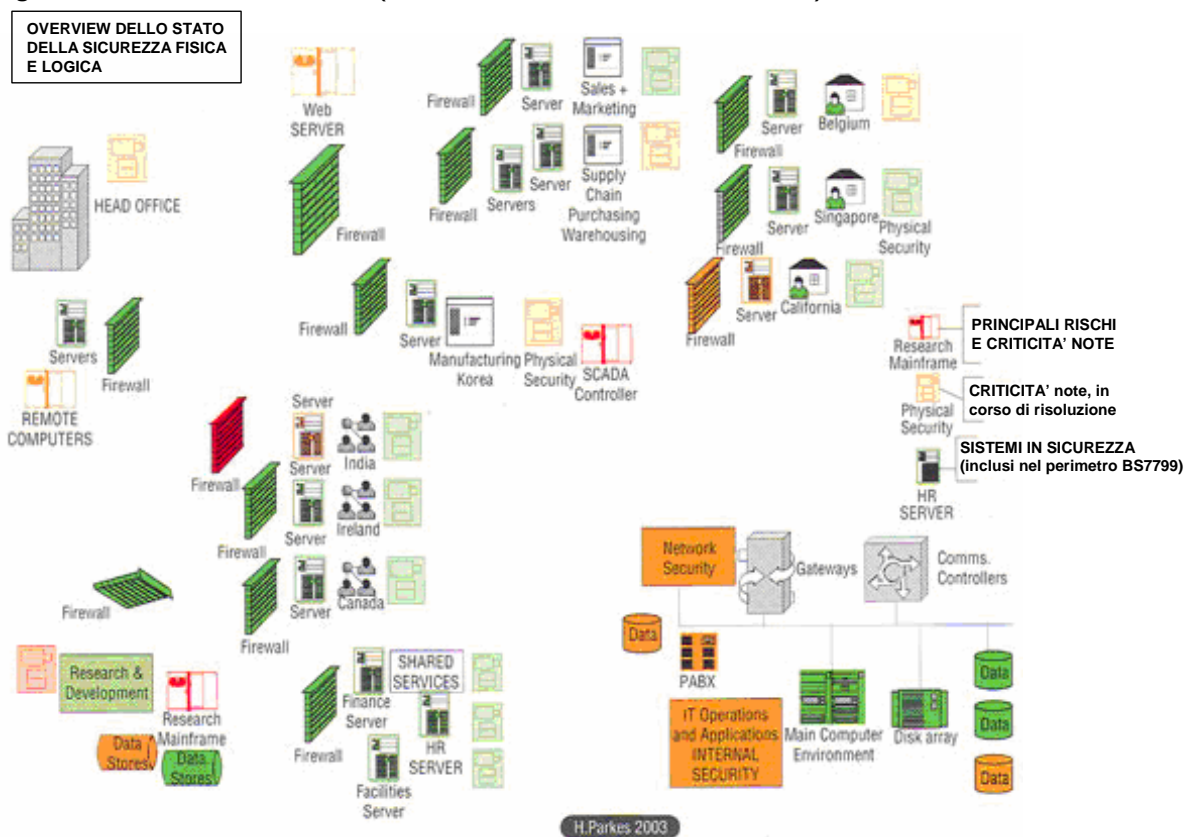
E' di norma possibile presentare all'Alta Direzione rapporti chiari e di immediata comprensione sotto forma di flowchart e diagrammi che rappresentino le attività esternalizzate, eventuali aree di criticità conseguenti all'esternalizzazione ed i legami con le attività non esternalizzate.

L'IT Governance interessa un grande numero di questioni legate alla gestione dei rischi, all'organizzazione ed alla definizione dei processi (operations), ed alla impostazione delle politiche commerciali. Sovente gli interlocutori preferiscono acquisire una visione d'insieme dell'intreccio di tali questioni da rappresentazioni schematiche basate su diagrammi piuttosto che dall'analisi di lunghi rapporti in gergo tecnico.

In assenza di reporting di agevole comprensione e a fronte del quale reagire tempestivamente (actionable), l'Alta Direzione può incontrare difficoltà ad individuare soluzioni di IT Governance praticabili ed efficaci.

Le seguenti figure 2 e 3 esemplificano come è possibile trasmettere informazioni anche complesse su aspetti di IT Governance mediante diagrammi, in modo esaustivo e fornendo immediata evidenza degli aspetti sui quali focalizzare l'attenzione.

**Figura 2 – Overview sulla Sicurezza (rilevante nell'ambito dell'IT Governance)**



(Continua a pagina 10)



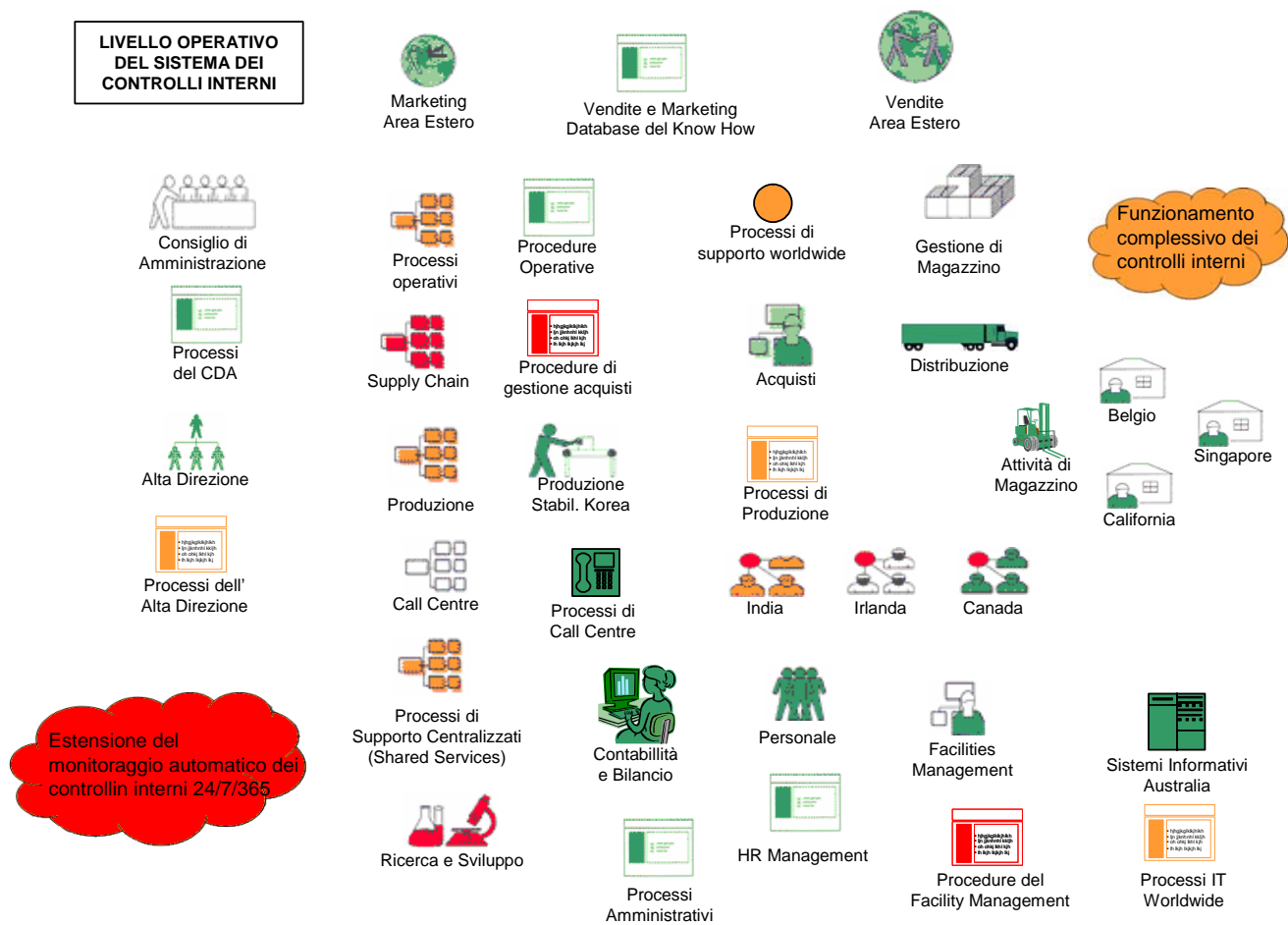
## Il Governo dell'Outsourcing IT

di Hugh Parkers, CISA, FCA

Da *Control Journal*, rivista bimestrale di *ISACA*, volume 5 del 2004.  
Liberamente tradotto da A. Pederiva (\*)

(Continua da pagina 9)

Figura 3 – Diagramma per il Reporting sull'IT Governance



### Legenda:

	Controlli interni adeguati - Monitoraggio automatico (oppure audit effettuato entro gli ultimi 12 mesi)
	Criticità individuate, in corso di correzione; stato di avanzamento sotto monitoraggio
	Criticità severe. Necessità di intervento da parte dell'Alta Direzione (CEO, Board)
	Non valutato. Ultima revisione anteriore ai 12 mesi o fuori perimetro (oppure informazioni non sufficienti per valutare lo stato dei controlli interni)

(Continua a pagina 11)

(Continua da pagina 10)

## Elementi di IT Governance per le Società che erogano servizi in outsourcing

La controparte in una relazione di esternalizzazione è l'outsourcer, l'organizzazione che eroga il servizio esternalizzato. In qualità di controparte, l'outsourcer si pone nella relazione da una prospettiva diversa rispetto alla organizzazione che esternalizza, anche per gli aspetti di IT Governance. Le principali aspetti di interesse per l'outsourcer sono evidenziate in figura 4. Come si vede, i punti di attenzione rimangono fondamentalmente gli stessi, ma cambio la prospettiva e la percezione dei rischi (Nota del Traduttore).

**Figura 4 – La prospettiva dell'Outsourcer**

Attività	Rischi associati	Punti di attenzione sull'IT Governance per il management dell'outsourcer
<p>1. Esternalizzazione dei sistemi informativi e della gestione dei dati (tutte le basi dati, incluse le anagrafiche, i sistemi transazionali, etc.)</p>	<p>Rischio molto alto (in relazione alla criticità delle informazioni la cui gestione è esternalizzata – e a quanto l'outsourcer ne è consapevole)</p> <ul style="list-style-type: none"> <li>* Perdita dei dati dei clienti dovuta ad accesso non autorizzato</li> <li>* Perdita di integrità dei dati o incapacità di erogare il servizio</li> <li>* Rischio di perdita di credibilità sul mercato</li> <li>* Incapacità di rispettare i termini contrattuali/rischio di azioni di risarcimento</li> <li>* Costi di ripristino</li> </ul>	<ul style="list-style-type: none"> <li>* I contratti devono includere clausole relative all'accesso ai dati ed alla individuazione delle responsabilità relative alla proprietà dei dati (ad esempio: dove sta il confine fra la responsabilità dell'outsourcer e dell'utente in merito alla correttezza dei dati?)</li> <li>* Profittabilità del servizio anche in relazione al costo dei livelli di servizio effettivamente erogati</li> <li>* Misure per il backup e il disaster recovery, incluse le modalità di collaudo e documentazione ai clienti dei risultati del collaudo (anche mediante attestazioni del management)</li> <li>* Clausole contrattuali relative a sicurezza e controllo degli accessi, nonché alla proprietà dei dati e conformità ed adeguatezza delle misure di sicurezza effettivamente in essere</li> <li>* Qualità delle informazioni prodotte, adeguatezza del patrimonio informativo disponibile rispetto alle esigenze dell'organizzazione utente, capacità di informare e supportare il cliente in caso di criticità relative alla integrità delle informazioni</li> </ul>
<p>2. Sistemi di knowledge management aziendali quali archivi di documentazione amministrativa (storia aziendale), archivi di documenti tecnici (progettazione di prodotto, tecnologie di processo o altro know how aziendale), archivi di documenti riservati relativi alle attività riservate del management (ad es. per la corrispondenza riservata)</p>	<p>Rischio alto/molto alto (in relazione alla criticità dei sistemi la cui gestione è esternalizzata)</p> <ul style="list-style-type: none"> <li>* Incapacità di assicurare i livelli di servizio concordati</li> <li>* Capacità nel tempo di sviluppare nuovi sistemi/ funzionalità come necessario e di proteggere il relativo know how</li> <li>* Capacità di mantenere nel tempo le funzionalità esistenti e/o di portarle su nuovi paradigmi tecnologici ove necessario</li> <li>* Necessità di assicurare la manutenzione di sistemi basati su tecnologie obsolete</li> </ul>	<ul style="list-style-type: none"> <li>* Misure per il backup e il disaster recovery, incluse le modalità di collaudo e documentazione ai clienti dei risultati del collaudo (anche mediante attestazioni del management)</li> <li>* Clausole contrattuali relative a sicurezza e controllo degli accessi, nonché alla proprietà dei dati e conformità ed adeguatezza delle misure di sicurezza effettivamente in essere</li> <li>* Misure di sicurezza relative alle reti di comunicazione</li> <li>* Monitoraggio e reporting interno e verso i clienti sul rispetto dei livelli di servizio</li> <li>* Modalità di gestione delle attività di sviluppo e manutenzione e modalità di gestione/ prioritizzazione del portafoglio progetti</li> <li>* Adeguatezza dei processi di gestione del personale per gli aspetti di selezione ed assunzione, formazione, sviluppo e retention</li> </ul>



(Continua da pagina 11)

**Figura 4 – La prospettiva dell’Outsourcer (continua)**

Attività esternalizzate	Rischi associati all'esternalizzazione	Punti di attenzione sull'IT Governance per il management dell'outsourcer
3. Esternalizzazione dei principali sistemi hardware e dei servizi a supporto	<p>Rischio medio alto</p> <ul style="list-style-type: none"> <li>* Costi di manutenzione in efficienza dei data centre e di rispetto dei livelli di servizio concordati</li> <li>* Costi di investimento per ricerca ed attivazione di nuove tecnologie, per il mantenimento della credibilità e della sostenibilità nel tempo della posizione di mercato</li> <li>* Rischi di cambiamenti radicali nei processi di gestione del know how dei clienti che possono richiedere modifiche rapide e sostanziali delle infrastrutture tecnologiche</li> </ul>	<ul style="list-style-type: none"> <li>* Misure per il backup e il disaster recovery, incluse le modalità di collaudo e documentazione ai clienti dei risultati del collaudo (anche mediante attestazioni del management)</li> <li>* Accorgimenti per contenere l'impatto delle attività di audit esterno (commissionate dagli utenti); valutare l'opportunità di concentrare tali attività su un unico fornitore terzo indipendente</li> <li>* Monitorare le prestazioni del data centre e la conformità ai livelli di servizio concordati contrattualmente</li> <li>* Accertarsi che i servizi erogati ai clienti non eccedano quanto concordato contrattualmente (senza autorizzazione del management) o che i clienti stiano pagando per servizi che ricevono ma che non sono stati concordati contrattualmente (senza autorizzazione del management del cliente)</li> </ul>
4. Esternalizzazione di reti e sistemi di comunicazione	<p>Rischio medio alto</p> <ul style="list-style-type: none"> <li>* Rischi di accesso illegale o a scopo di danneggiare, attacchi di tipo denial-of-service, perdita di integrità delle informazioni, furto di proprietà intellettuale, virus, worm, trojan e altro malicious software.</li> <li>* Necessità di provvedere a ridondanza delle linee e degli apparati</li> <li>* Rischio di carenza di capacità trasmissiva</li> </ul>	<ul style="list-style-type: none"> <li>* Misure per il backup e il disaster recovery, incluse le modalità di collaudo e documentazione ai clienti dei risultati del collaudo (anche mediante attestazioni del management)</li> <li>* Sicurezza complessiva della rete, sistemi di monitoraggio e prevenzione degli accessi non autorizzati, sistemi di monitoraggio dei guasti e di gestione degli interventi, sistemi di protezione da attacchi di tipo DoS e/o da danni alla rete fisica</li> <li>* Sistemi di pianificazione e gestione della capacità di trasmissione</li> </ul>
5. Fornitura di apparecchiature e sistemi hardware, PC, server, terminali e apparecchiature di rete	<p>Di norma rischio moderato</p> <ul style="list-style-type: none"> <li>* Mercato a forte concorrenza</li> <li>* Non conformità del servizio erogato agli accordi contrattuali</li> <li>* Capacità insufficiente rispetto alla domanda di servizi dei clienti (es.: numero insufficiente di manutentori disponibili)</li> </ul>	<ul style="list-style-type: none"> <li>* Monitoraggio della conformità agli accordi contrattuali (servizi erogati vs. corrispettivi richiesti)</li> <li>* Sistemi di monitoraggio della soddisfazione degli utenti (a livello utente finale e a livello di corrispondente contrattuale)</li> </ul>

**Hugh Parkes, CISA, FCA**

è dirigente della Parkes & Parkes, consulenti di direzione, con sede a Melbourne, Victoria, Australia. Parkes ha una vasta esperienza nella consulenza legata ai sistemi informativi, prevalentemente nel settore banche e finanza. La sua esperienza include la gestione delle relazioni fra outsourcer ed outsourcee e la gestione di organizzazioni per l'erogazione di servizi esternalizzati. Già membro dell'IT Governance Board, dell'International Board of Directors dell'ISACA e dell'Australian Auditing Standards Board, Parkes attualmente opera come presidente o membro indipendente di numerosi Audit Committee in Australia.

**(\*) Andrea Pederiva, CISA, è manager in Deloitte ERS**

## CISA and CISM: Internationally Recognized for Future Success

di Leslie Macartney, CISM, CISA

da *Certification Magazine*, 2004.

Attaining the right certification has become especially important now that Sarbanes-Oxley in the United States and increased scrutiny worldwide have focused attention on enterprise finances and the IT processes that support financial system control and reporting. In fact, the recent "IT Governance Global Status Report" from the IT Governance Institute (ITGI) found that more than 93 percent of global CEOs and executives surveyed recognize that information technology is vital to deliver the organization's strategy. The role of IT has become so important, according to the report, that 58 percent of respondents regularly have IT on their organization's board agenda.

These changes in the business environment make finding the best-qualified professionals critically important. Internationally respected certifications provide employers with one way to determine if someone is the right person for the job. According to David Foote, president and chief research officer for Foote Partners, an IT workforce research firm and management consultancy, "Many IT and business line managers interviewed in recent research support the notion that certification is a more meaningful measure of comparing IT workers than untested or self-reported skills competence."

Among the most sought-after certifications are two offered by the Information Systems Audit and Control Association (ISACA), the global leader in information governance, security and assurance. The Certified Information Systems Auditor (CISA) and the Certified Information Security Manager (CISM) have been cited as leading certifications for information professionals.

According to surveys by Foote Partners LLC, IT professionals holding the CISA certification earned the largest gains in premium bonus pay among the 56 certifications surveyed during 2002 and 2003. With a 25 percent increase in 2003 and a 38 percent increase over 2002 and 2003, the CISA certification experienced "the biggest increase for all certifications surveyed." This increase is especially significant since the report found that premium pay for all certifications declined by 5.6 percent during 2003.

A 2003 survey of CISA-certified ISACA members revealed that the majority (67 percent) believed that obtaining the certification helped advance their careers. When all respondents, CISA or not, were asked if they thought gaining the CISA would help their careers in the future, 71 percent of responses were positive.

"Earning the CISA designation demonstrates attainment of a highly regarded qualification and commitment to stay current in a fast-changing technological world. It brings with it recognition and positive reputation for certified professionals worldwide in the IS audit and control field," said Ria Lucas, chair of the CISA Certification Board. "We have found that employers around the world prefer to hire and retain those who achieve and maintain the CISA designation."

*Nel 2004 la rivista **Certification Magazine** ha pubblicato un articolo che ha presentato e sottolineato l'importanza delle certificazioni **CISM e CISA**.*

*L'articolo si può trovare al seguente indirizzo:*

*[www.certmag.com/articles/templates/cmag\\_department.asp?articleid=992&zoneid=63](http://www.certmag.com/articles/templates/cmag_department.asp?articleid=992&zoneid=63)*

First offered in 1978, the CISA program has measured excellence in the area of IS auditing, control and security. Today, the CISA certification has been earned by more than 35,000 professionals since its inception, and more than 14,000 individuals regis-

*(Continua a pagina 14)*



## CISA and CISM: Internationally Recognized for Future Success

di Leslie Macartney, CISM, CISA

da *Certification Magazine*, 2004

(Continua da pagina 13)

tered for the 2004 exam.

Part of the reason behind CISA's success is that earning a CISA goes far beyond just taking the exam. The CISA certification requires candidates to:

- Successfully complete the CISA examination, which is offered in 11 languages and administered at more than 220 locations around the world.
- Submit evidence of at least five years of professional experience in IS auditing, control or security.
- Follow the Code of Professional Ethics to guide professional and personal conduct.
- Attend continuing professional education.
- Adhere to the Information Systems Auditing Standards adopted by ISACA.

Responding to the need for a higher-level information security credential that goes beyond the practitioner level, ISACA developed the CISM credential in 2002. CISM has rapidly earned a spot among the top certifications and was among 10 new programs that *Certification Magazine* said "...represent innovative topics or subject focus, certify interesting and useful skill and knowledge or represent ways to involve IT professionals early in programs that require years of documented work experience."

Offered for senior professionals who manage an organization's information security and possess the knowledge and experience to implement and direct an IT security structure that manages risk effectively, the CISM designation is for managers who understand and support the closely linked relationship between business strategy and security.

Businesses today face increasingly complex security threats, and the CISM designation provides assurance to senior executives and boards of directors that their information security managers have the expertise to reduce risks and protect the organization. Professionals and their companies have responded positively to the CISM certification. In less than two years, more than 5,000 professionals have been certified, and the CISM exam

(Continua a pagina 15)

### EXAM PREPARATION: TRAINING AND MATERIALS

In addition to offering certification examinations around the world each year, ISACA offers training at selected conferences. Many ISACA chapters around the world also hold highly regarded preparation sessions for candidates. Each year, ISACA also develops and publishes comprehensive study materials, including CISA exam reference materials, such as:

- "CISA Review Manual 2005" (available in English and soon to be available in Italian, Japanese and Spanish)
- "CISA Review Questions, Answers & Explanations CD-ROM 2005" (650 questions available in English in December 2004 and Spanish in February 2005)
- "CISA Review Questions, Answers & Explanations Manual 2005" (550 questions available in English now, and soon to be available in Japanese and Spanish)
- "CISA Review Questions, Answers & Explanations Manual 2005 Supplement" (100 questions available in English now and soon to be available in Italian, Japanese and Spanish)

CISM exam reference materials include:

- "CISM Review Manual 2005" (available January 2005)
- "CISM Review Questions, Answers & Explanations Manual 2004" (100 questions available now)
- "CISM Review Questions, Answers & Explanations Manual 2005" (100 questions to be available in January 2005)

Detailed descriptions and ordering information for CISA and CISM materials are available on the ISACA Web site at [www.isaca.org/bookstore](http://www.isaca.org/bookstore).

## **CISA and CISM: Internationally Recognized for Future Success**

**di Leslie Macartney, CISM, CISA**

*da Certification Magazine, 2004*

*(Continua da pagina 14)*

saw a 160 percent increase in registrations during its second year.

To earn a CISM designation, candidates must:

- Successfully complete the CISM examination, which is administered at more than 220 locations around the world.
- Adhere to the Code of Professional Ethics.
- Attend continuing professional education.
- Submit verified evidence of at least five years of information security work experience, with a minimum of three years of information security management work experience in three or more of the job practice areas. Waivers for general information security work experience are available, if certain education or certification requirements are met.

The CISA and CISM certifications have gained the importance they now enjoy in part due to ISACA's unique position in the industry. The organization first got its start in 1967, when a small group of individuals with similar jobs—auditing controls in the computer systems that were becoming increasingly important to the operations of their organizations—met to discuss the need for a centralized source of information and guidance in the field. When the group formalized in 1969, it became the EDP Auditors Association. In 1976, the group formed an education foundation to conduct large-scale research, expanding its knowledge and value to the field of IT governance and control. The group also set the IS audit and control standards practiced by professionals worldwide.

Now known as ISACA, the organization has more than 35,000 members who live and work in more than 100 countries. Members cover a variety of IT and business-related positions. They represent all levels of the profession, from newcomers to veteran IT pros in senior positions. ISACA members work in nearly all industry categories, including financial, banking, public accounting, government, the public sector, utilities and manufacturing. This diversity enables members to learn from one another, exchange ideas and challenge the status quo.

With chapters in more than 60 countries, the organization's vibrant chapter network provides education, resource sharing, advocacy and networking.

There is no doubt that certification will continue to be an increasingly important facet of any professional's career, and ISACA's CISA and CISM are among the most valued and internationally respected credentials available.

Registration is already underway for the next CISA and CISM exams, which will be held June 11, 2005. Bulletins of information for each certification can be obtained via ISACA's Web site ([www.isaca.org/certification](http://www.isaca.org/certification)) in a downloadable format or requested from the certification department ([certification@isaca.org](mailto:certification@isaca.org)). Online registration is available and will save applicants \$35 (U.S.).

**Leslie Macartney**, CISM, CISA, is chair, CISM Certification Board for the Information Systems Audit and Control Association, and a member of the British Standards Institute's BDD/2 committee responsible for information security standards in the United Kingdom.



## Qualità dei servizi, qualità dei sistemi e controlli

di Donatella Rosa (\*)

da *ICT Security*, 2004.

Ai tempi del Mainframe, i tabulati che venivano "sforati", raccoglievano dati su tutto: livello di occupazione della memoria, tempo di idle della cpu, tempi di risposta delle transazioni CICS e tante altre informazioni dettagliate su grandezze e sulla tecnologia.

Allora, il riferimento erano le risorse informatiche dell'azienda e si ragionava in termini di **qualità dei sistemi**.

Nessuna attenzione veniva data alla qualità dei servizi erogati all'utente.

Di contro, l'utente, che nutriva un rispetto sacro nei confronti degli informatici e spesso non capiva il loro linguaggio, difficilmente riusciva a contestare che "...le cose non andavano così bene...".

L'avvento del personal computer ha portato alla trasformazione dei tabulati in report, riducendo la quantità dei dati, ma non il loro, già scarso, livello di comprensibilità.

Le architetture client/server, pur difficili da gestire e controllare, si sono contrapposte alla immediatezza dell'uso del personal computer, mentre l'utente ha cominciato ad acquisire maggiore familiarità con gli strumenti informatici e con il linguaggio. L'utente si è reso conto che il mezzo informatico è uno strumento e, come tale, va finalizzato al perseguimento degli obiettivi aziendali.

Questa semplice "presa di coscienza" ha prodotto un mutamento notevole nel modo di gestire i sistemi e le reti.

La qualità dei sistemi ed i dati relativi al funzionamento delle singole apparecchiature hanno perso di interesse, a vantaggio di altri fattori di valutazione, quali il livello di servizio, lo svolgimento delle attività end-to-end, la redditività.

Ecco, quindi, farsi avanti il concetto della **qualità dei servizi**.

Nuovi fattori di complessità si sono aggiunti quando siamo entrati nell'era e-.

Infatti, spesso reti e sistemi sono esterni all'azienda, il traffico cambia, per quantità e distribuzione nel tempo, l'utente è spesso "totalmente" sconosciuto.

Le applicazioni tradizionali e quelle per il Web sono 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 giurisdizione è 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.

I livelli di sicurezza non adeguati, l'allungarsi nei tempi di risposta, la scarsa navigabilità di un

(Continua a pagina 17)

## Qualità dei servizi, qualità dei sistemi e controlli

di Donatella Rosa, da *ICT Security*, 2004.

(Continua da pagina 16)

sito, i tempi lunghi di attesa sono:

- \* per l'utente, l'indice di una scarsa qualità del servizio
- \* per l'azienda, misurabili in termini di riduzione di fatturato e, quindi, di perdita di profitto.

Per una azienda, la qualità del servizio erogato si misura anche con una adeguata business continuity e con l'aumento di competitività.

La funzione aziendale di System & Network Management diventa articolata, complessa ed assume un significato strategico, per l'impresa.

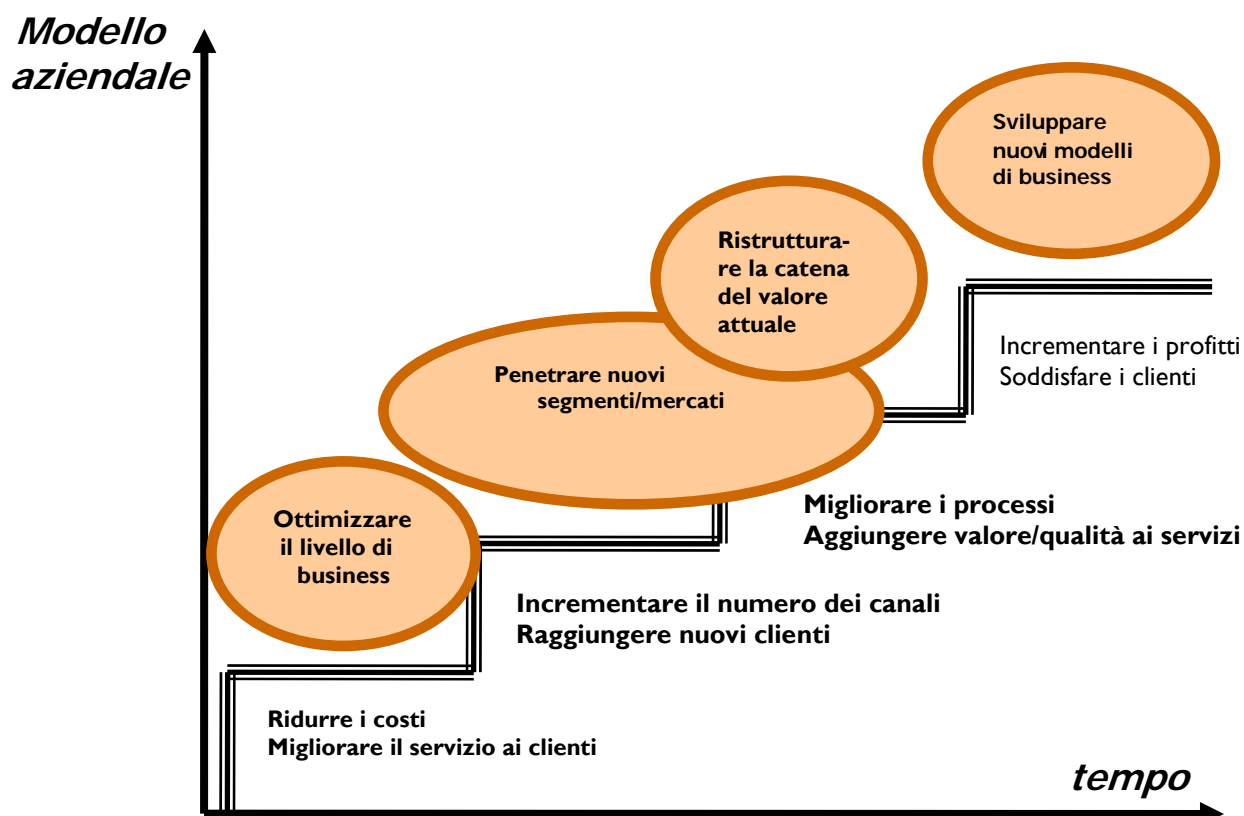
La funzione acquista un peso maggiore: deve fare scelte strategiche; a volte, deve proporre mutamenti radicali, su nuovi investimenti o su "deleghe" ad altri fornitori di servizi specializzati.

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

La sicurezza diventa un requisito di qualità.

Ecco, quindi, che, per rispettare i Livelli di Servizio ed assicurare la continuità e qualità dei servizi, occorre controllare e monitorare costantemente le prestazioni erogate, tenere sotto controllo gli indicatori di criticità, verificare i processi organizzativi.

(Continua a pagina 18)





## Qualità dei servizi, qualità dei sistemi e controlli

di **Donatella Rosa**, da *ICT Security*, 2004.

*(Continua da pagina 17)*

Vanno identificate le aree in cui si concentra il "valore aziendale" e vanno individuate le possibili leve per incrementare tale valore.

Occorre orientare gli investimenti tecnologici al valore dell'impresa.

Il tutto va documentato in Report comprensibili dagli utenti, in relazione alla loro attività. Occorre semplificare e rendere concisa, efficace e precisa la comunicazione.

Occorre anche fare periodiche indagini di valutazione del grado di soddisfazione dei servizi, per verificare la qualità degli indicatori posti alla base del Service Level Agreement siglato con l'utente. Le informazioni raccolte in tali indagini e monitorate devono diventare regole, procedure, azioni.

Già in sede di definizione del contratto con l'utente emerge l'opportunità di operare come poco sopra detto. La definizione del contratto, infatti, può produrre riflessi anche in quelli eventualmente siglati con fornitori esterni, di outsourcing e/o di telecomunicazioni.

Poiché nel contratto vengono evidenziati, in modo esplicito, i requisiti utente, diventa possibile correlare costi con fattori prestazionali critici.

Il management diventa in grado di orientare gli investimenti verso gli elementi che possono aumentare la competitività dell'azienda, riuscendo, nel contempo, a svolgere analisi costi/benefici più oggettive.

Assistiamo, allora, ad un cambiamento di atteggiamento, sia da parte delle risorse informatiche, sia da parte degli utenti. A tale cambiamento si aggiungono nuovi processi organizzativi o miglioramenti di quelli esistenti.

Sul concetto di qualità cambia il punto di vista che non è più rivolto verso la tecnologia (qualità dei sistemi) ma verso la soddisfazione dell'utente/cliente (qualità dei servizi). La qualità è percepita come affidabilità, sicurezza, fiducia.

In conclusione, il controllo della qualità dei servizi permette che una Azienda crei clienti soddisfatti, fedeli e motivati a continuare ad esserlo.

La strada può essere lunga, perché, come stima Gartner Group, più del 90% delle aziende non è preparata a gestire i rapporti con la clientela.

*(\*) Donatella Rosa, Vicepresidente AIEA, è consulente di Direzione nel settore ICT*

### ***I prossimi appuntamenti: Sessioni di Studio***

Roma 26 gennaio, Milano 28 gennaio, Roma 9 marzo,  
Milano 18 marzo, Milano 15 aprile, Roma 20 aprile

### ***Termine rinnovo quota assicurativa ISACA 2005: 31 gennaio 2005***

Iscrizione soci ordinari (180,76€), studenti (22€), rinnovo ordinari (154,94€).

### ***Termine iscrizione esame CISA—CISM: 30 marzo 2005***

Roma - 2 dicembre 2004 - Sessione di studio

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

**Sessioni  
di  
studio**

## PROGRAMMA

- 14.15 Introduzione dei lavori da parte del Chairman (Donatella Rosa Vice Presidente AIEA)  
14.30 **Luigi Carrozzi (Coordinatore del GdR AIEA sugli ISMS - Auditor/Lead Auditor BS7799)**  
*Il gruppo di ricerca: obiettivi, organizzazione, risultati*  
14.55 **Michele Bianco (BULL)**  
*An ISMS Framework for Enterprise Organizations: the BULL Value Proposition*  
15.20 **Silvano Bari (Alitalia)**  
*Rilevanza ed impatto dei sistemi di gestione delle informazioni nel contesto della realtà aziendale Alitalia*  
15.45 **Loris Zambon – Claudio Salvati (BNL)**  
*ISMS: l'esperienza BNL*  
16.10 Pausa caffè  
16.25 **Antonio Tomassi – Nicola Mancini – Stefano Spagnoli (GRTN)**  
*ISMS - L'esperienza del GRTN S.p.A*  
16.50 **James A.W. Cheyne (NCR)**  
*ISMS & 6s un binomio vincente*  
17.15 **Luigi Carrozzi (Coordinatore del GdR AIEA sugli ISMS - Auditor/Lead Auditor BS7799)**  
*Il gruppo di ricerca: il futuro*  
17.30 Dibattito con i relatori  
18.15 Conclusione dell'incontro a cura del Chairman  
18.20 Termine dei lavori

Milano - 15 dicembre 2004 - Sessione di studio

Unicredit Servizi Informativi  
via Livio Cambi, 1 (MM1-Lampugnano)

**Sessioni  
di  
studio**

## PROGRAMMA

- 14.15 Introduzione dei lavori da parte del Chairman  
14.30 **Fabrizio Matta (Business-e)**  
*Monitoraggio della sicurezza: Criteri per la classificazione degli allarmi e la gestione degli incidenti*  
15.20 **Andrea Agosti (VP Technologies)**  
*La misura delle prestazioni della sicurezza informatica*  
16.10 Pausa caffè  
16.25 **Michele Barbi (Etnoteam)**  
*IT Governance – modello di gestione*  
17.15 Dibattito con i relatori  
18.15 Conclusione dell'incontro a cura del Chairman  
18.20 Termine dei lavori



**AIEA**  
**Associazione Italiana**  
**Information Systems Auditors**

**ISACA**  
**Information Systems Audit and**  
**Control Association**

**AIEA capitolo di Milano di ISACA**

20131 Milano— Via Accademia, 19  
Tel. +39.02.70608405- Fax +39.02.700507644  
E-mail: aiea@aiea.it  
P.IVA 10899720154

Sede operativa

20141 Milano— Via Valla, 16  
Tel 02 84742.365- Fax 02 84742212

**InfoAIEA**

Dicembre 2004, Volume 2 n.4  
Registrazione al Tribunale di Milano  
n. 372 del 9.6.2003

Direttore Responsabile **Silvano Ongetta**

Editore: AIEA, via Accademia, 19  
20131 MILANO

Redazione: **Orillo Narduzzo**

Hanno collaborato: **Orillo Narduzzo,**  
**Leslie Macartney, Silvano Ongetta,**  
**Andrea Pederiva, Donatella Rosa.**

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, .....

**SCRIVETECCI!!**

E-mail : [infoaiea@aiea.it](mailto:infoaiea@aiea.it), [aiea@aiea.it](mailto:aiea@aiea.it)

Sede: AIEA, Redazione InfoAIEA

Via Accademia, 19 - 20131 Milano

**Consiglio Nazionale 2004-2006**

Presidente: **Silvano Ongetta**

Vice presidenti: **Donatella Rosa,**  
**Orillo Narduzzo**

Segretario: **Enzo Toffanin**

Tesoriere: **Aureliana Radaelli**

**Consiglieri:**

**Renato Alessandrini, 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.*