



Associazione Italiana
Information Systems Auditors



Il successo del nostro XXIII Convegno Nazionale

Questo numero esce con qualche giorno di ritardo, perché volevamo dare ai soci, che non sono potuti venire al Convegno di Pisa, alcune informazioni sull'evento.

Come già da alcuni anni, anche a Pisa la platea dei soci è stata numerosa e partecipe. Al convegno hanno anche partecipato alcuni studenti della facoltà di Informatica

Un grazie a tutti i partecipanti ed ai relatori che, con la loro professionalità, hanno esposto temi interessanti ed innovativi, suscitando l'interesse della platea.

Un particolare ringraziamento al Prof. Baiardi ed al dott. Telmon che ci hanno permesso di accedere al prestigiosa sede della facoltà di Scienze matematiche, Fisiche e Naturali. Grazie anche a loro, inoltre, abbiamo potuto visitare, nella serata del 21 maggio, il Museo di Scienze Naturali, collocato presso la Certosa di Calci.

Quest'anno, i presenti sono stati 100.

I commenti nel "foyer" e la lettura dei questionari di valutazione ci aiuteranno a migliorare sempre più l'organizzazione di eventi.

AIEA ha partecipato

Nel mese di marzo 2009 si è concluso il Gruppo di Lavoro sulle "Competenze nella sicurezza delle informazioni" istituito dal "Forum delle competenze digitali", associazione senza scopo di lucro, alla quale partecipa AIEA, che promuove, valorizza ed accresce la diffusione della cultura e delle conoscenze in materia di competenze e professionalità nel settore dell'ICMT (Information, Communication & Media Technology) e delle Tecnologie Digitali.

Il Gruppo di lavoro, cui ha partecipato AIEA nella persona del socio Silvano Bari, ha prodotto un Rapporto in cui vengono analizzati gli schemi di accreditamento e certificazione esistenti in materia di sicurezza delle informazioni, individuati alcuni metodi di mappatura delle competenze, e proposta una lista delle principali certificazioni.

In particolare, nel Capitolo "La certificazione delle competenze nella sicurezza delle informazioni", curato da Silvano Bari, si analizzano:

- a) la tipologia e le diverse caratteristiche delle attestazioni concernenti le competenze del personale (prima, seconda e terza parte);
- b) il processo di accreditamento e certificazione con riferimento alle varie figure coinvolte;
- c) le norme e le guide di riferimento;
- d) lo stato dell'arte delle certificazioni delle competenze nella sicurezza delle informazioni, distinte per tipologia.

Il Rapporto sarà reso disponibile, a breve, a tutti i soci AIEA.



Assemblea Annuale

Il 1° luglio 2009 si terrà l'Assemblea annuale che sarà anche un'occasione per partecipare ad una "edizione speciale" di una Sessione di Studio, con un'interessante relazione, da parte del socio Stefano Aiello sul tema "Soluzioni organizzative e capacità manageriali mirate all'industrializzazione dei Servizi IT".

A breve vi daremo tutte le informazioni.

Elezioni probiviri triennio 2009-2012

Nei primi giorni di giugno è stata inviata, a tutti i soci, la documentazione e le istruzioni per l'elezione dei 3 Proviviri, previsti da statuto. Ricordiamo che il 30 giugno è in scadenza il mandato dell'attuale Comitato.

Come da istruzioni inviate, i soci sono pregati di inviare la scheda di votazione entro e non oltre il 15 giugno, in modo da poter chiudere lo spoglio delle schede ed arrivare alla designazione entro fine mese.

Un sollecito a votare, quindi, ai soci che ancora non lo avessero fatto.

Il trentennale di AIEA

L'otto ottobre di trent'anni fa nasceva AIEA. Un gruppo di pochissime persone, unite da comuni esperienze di lavoro ed obiettivi, fondava l'Associazione Italiana EDP Auditors. Con il tempo, il nome ha perso la sua natura di acronimo e ha assunto il significato di Associazione Italiana Information Systems Auditors ed i soci sono quasi 800. Il CD ha deciso di festeggiare il trentennale, organizzando in contemporanea a Milano, Roma e Torino tre Sessioni di Studio, di cui quella di Milano di una intera giornata

Gruppi di Ricerca

Gruppo di Lavoro "Traduzione Cobit 4.1"

COBIT 4.1 – sono stati tradotti e resi disponibili nell'area Downloading del sito l'"Executive Summary" ed i seguenti processi: ME1, ME2, ME3, ME4; DS1, DS2, DS3, DS4, DS5, DS6; AI1, AI2, AI3, AI4.

Business Continuity

Il Gruppo di ricerca è formato da una rappresentanza di ciascuna delle Associazioni AIEA, AUSED e ANSSAIF.

Il testo del documento è completo ed è ora avviata la procedura di approvazione da parte delle Associazioni promotrici in vista della pubblicazione della Guida AIEA. In particolare il testo è ora all'esame dei presidenti delle associazioni. Un grazie al socio Massimiliano Rinalducci che ha coordinato il GdR. Non appena il testo sarà approvato il contenuto sarà consultabile dai soci.

CobIT e legge 262

Il Gruppo di Ricerca AIEA è articolato in 6 sottogruppi chiamati Focus Group.

I partecipanti alla ricerca sono ben 17 soci divisi in 6 Focus Group i cui Relatori sono:

Alessandro Arca (FG5)

Giuliano Flesia (FG4)

Luca Nurisso (FG1 e FG6)



Dino Ponghetti (FG3)
Luca Turri (FG2)

Le tematiche dei Focus Group sono le seguenti:

- FG1: Introduzione e normativa di riferimento
- FG2: Dimensionamento delle verifiche e analisi dei rischi
- FG3: Controlli generali
- FG4: Controlli applicativi
- FG5: Campionamenti
- FG6: Valutazione del sistema di controllo e attestazioni finali

Le relazioni dei Focus Group 1, 2, 3, 4 e 6 sono giunte alla finalizzazione, come da programma, entro l'estate ed ora passano alla fase di convalidazione fra tutti i partecipanti al GdR; tale fase dovrà concludersi entro due mesi lavorativi e pertanto entro l'autunno, considerato il periodo di ferie estive. L'attività del Focus Group 5 è in svolgimento e si prevede che sarà ultimata essa pure entro l'autunno

Gruppo di Lavoro "Traduzione Val IT 2.0"

Sta lavorando, con il coordinamento di Guido Leone, il Gruppo di Lavoro che si occupa della traduzione della versione aggiornata di Val IT 2.0. In particolare delle seguenti pubblicazioni:

Enterprise Value: Governance of IT Investments - The Business Case
Enterprise Value: Governance of IT Investments - Getting Started with Value Management
Enterprise Value: Governance of IT Investments - The Val IT Framework 2.0
Sono stati rilasciati, in occasione del convegno di Pisa, i primi due documenti.

Sono stati rilasciati, in occasione del convegno di Pisa, i primi due documenti.

E' in corso la traduzione del terzo ("*The Val IT Framework 2.0*"), il rilascio della quale è previsto per l'ultimo trimestre dell'anno.

Dodicesima edizione Global Information Security Survey Ernst & Young

Ernst & Young, leader mondiale nei servizi professionali, ha annunciato l'avvio della dodicesima edizione della Global Information Security Survey (GISS), consolidata ricerca annuale diventata nel corso degli anni punto di riferimento per la comprensione dei principali driver, trend e sfide inerenti la sicurezza informatica.

Si tratta infatti di una ricerca condotta su scala mondiale (l'edizione 2008 ha coinvolto circa 1400 organizzazioni in più di 50 Paesi) con l'obiettivo di evidenziare come le più importanti aziende, enti pubblici ed organizzazioni no-profit si stanno attrezzando per continuare a garantire un adeguato livello di protezione delle informazioni in linea con le esigenze di business, specialmente in questo momento particolarmente difficile per alcune delle maggiori economie mondiali. La ricerca offre ai partecipanti l'opportunità di confrontare la propria situazione aziendale in materia di sicurezza con quella di aziende similari per dimensioni, fatturato, paese d'appartenenza o settore industriale di riferimento.

La survey 2009 si focalizza su aspetti di governance della sicurezza, organizzazione ed integrazione



con le altre funzioni aziendali, metriche di valutazione, analisi e gestione dei rischi, driver ed attività che guidano la gestione della sicurezza, standard di riferimento e business continuity.

Modalità di partecipazione:
La survey consiste di 35 domande che richiedono circa 45 minuti per la compilazione on line. Nel momento in cui i risultati saranno resi disponibili, tutti i partecipanti riceveranno un documento di sintesi generale dei trend in materia di sicurezza, nonché report personalizzati di comparazione tra la propria situazione ed i trend relativi al settore industriale di riferimento. Il tutto è completamente gratuito ed è gestito in maniera anonima.

Per maggiori informazioni e per partecipare alla survey vi invitiamo ad inviare una e-mail di richiesta all'indirizzo EY.InformationSecurity@it.ey.com

La fase di raccolta dei dati termina il 31 luglio 2009, data entro la quale i questionari devono essere completati.

Prolungato il termine della rilevazione per la Survey KPMG

Per rendere maggiormente significativa la rilevazione e tenendo conto del periodo "festivo" di fine maggio, il termine della survey è stato prolungato. Ricordiamo che la IT Internal Audit Survey in Italia È stata promossa da AIEA e KPMG. Infatti, AIEA e KPMG, a supporto dello sviluppo professionale dei propri associati, stanno programmato una rilevazione sullo stato dell'arte della funzione di IT Internal Audit. La rilevazione interessa un campione rappresentativo dei soci, scelto con un algoritmo che prevede l'individuazione di un solo socio per azienda.

I risultati della rilevazione saranno presentati alla Sessione di Studio organizzata a Milano, il prossimo 8 ottobre, ricorrenza del trentennale della fondazione di AIEA.

Insieme ai dati della rilevazione in Italia, KPMG presenterà i risultati della medesima iniziativa, già svolta a livello europeo.

AIEA sul numero di maggio del Global Communiqué ISACA

A pagina 3 del numero di maggio compare una intera colonna sulle attività svolte, nel 2008, per promuovere il capitolo di Milano nelle Università.

Ricordiamo che il referente di AIEA per le Università è Daniela Bolli, Consigliere AIEA.

Milan Chapter Academic Relations

In 2008, the ISACA Milan Chapter collaborated with the Association of International Education Administrators (AIEA) to promote the chapter to two Italian universities.

The goals for meeting with students at these universities included:

- *Making students aware of IT audit, security and governance topics*
- *Promoting AIEA as a strategic contact point for the job market*
- *Establishing a link between academic, professional and business entities*
- *Promoting AIEA as a knowledge base through its close relationship with ISACA The first session took place in the first quarter of 2008 at the University of Rome II, with about 40 students who were attending the second year in business administration.*

Students appreciated the session as an opportunity to face and, to some extent, discover a new profession, as well as to meet a world different from the academic one.

Subsequent sessions at University of Rome II targeted students attending the final year of schooling in various fields. The interest in those sessions was even higher than the first,



in large part because the focus was on real job opportunities.

The initial session at Florence University also took place in the first quarter of 2008 and involved about 30 students. In the second half of 2008, two more sessions were offered: the first one at the Turin Politecnico (engineering) IT department, with about 50 attendees, and the second at Milan Politecnico, with about 30 attendees. The latter, due to the presence of many foreign students, was held in English.

In all, both students and professors expressed interest in the IT topics presented. Students were mainly interested in ISACA certifications as an opportunity to achieve a formal professional qualification. Professors were interested in exploiting the contact with ISACA and AIEA to broaden their relations and knowledge at an international level. During 2009, the ISACA Milan Chapter plans to maintain the relationships established with these universities, by delivering, as they have requested, more sessions. Plans are also underway to contact other universities.

Riceviamo da Protiviti

In allegato, la Newsletter Protiviti n. 24 dal titolo **“Gestire e comunicare la crisi: un caso di successo”**.

Una crisi aziendale richiede grandi capacità di gestione sotto stress da parte del Management. Gestire una crisi aziendale come se fosse “normale operatività” è un atto i cui effetti potrebbero ripercuotersi all’interno e all’esterno dell’azienda, in un’escalation di eventi di difficile controllo; un’adeguata gestione della crisi può servire, al contrario, a comprendere il contesto in cui si è sviluppata e ad allestire adeguati presidi contro potenziali eventi di rischio.

Protiviti, in questo Insight, presenta l’approccio metodologico di Crisis Management & Communications e analizza un caso reale di successo.

I prossimi eventi di AIEA

Calendario Eventi AIEA

GIUGNO 2009

18..... Torino - Sessione di Studio

LUGLIO 2009

1.....Milano – Assemblea soci



Calendar of Events

Dates of conferences/events are indicated in **RED**; other dates and deadlines are indicated in **BLACK**.

I prossimi eventi ISACA:

June

- 11 June.....Deadline for contributions to volume 3, 2009, of *COBIT Focus*
- 13 June.....CISA, CISM and CGEIT exam administration
- 15-19 June **ISACA Training Week**, Vienna, Austria

July

- 1 July Early-bird registration deadline for the ISACA Training Week, Toronto, Ontario, Canada
- 15 July Early-bird registration deadline for Latin America CACS, San Jose, Costa Rica
- 15 July Early-bird registration deadline for Information Security and Risk Management Conference, Las Vegas, Nevada, USA
- 19-22 July **International Conference**, Los Angeles, California, USA

ISACA Benefit of the month

Member Benefit of the Month: **Listservs/Discussion Forums**

ISACA and the IT Governance Institute® (ITGI™) have established several listservs to enable individuals to find the group most suited to their professional interests. Each of the listservs offers excellent opportunities to share advice, seek assistance and raise pertinent questions. Information on each listserv and how to join is available at www.isaca.org/listserv.

Riceviamo da ISACA **Certification Update**

March Certifications

1,168 CISA certifications, 282 Certified Information Security Manager® (CISM®) certifications and 835 Certified in the Governance of Enterprise IT® (CGEIT®) certifications were awarded in March 2009.



Associazione Italiana
Information Systems Auditors



Certification Revocation Alert

Certified individuals who have not reported 2008 CPE hours, although they have paid the certification maintenance fee, are subject to revocation. Individuals can update their CPE hours in their certification profile. Renewal payment can be made online through the renewal process.

Avviso ai soci 1

Preghiamo i soci che, per vari motivi, modificano la loro anagrafica (recapiti telefonici, indirizzo, azienda di appartenenza o altro...) di comunicare i nuovi dati in segreteria aiea@aiea.it. La mancanza di tali comunicazioni potrebbero impedire, al socio, la ricezione delle comunicazioni.

Avviso ai soci 2

E' in linea, sulla homepage del sito, il calendario degli eventi AIEA.

Rinnoviamo l'invito ai soci di fornire le proprie indicazioni su argomenti o temi che desiderano vengano trattati nel corso del 2009 sia nelle Sessioni di Studio sia in Workshop.

Chi volesse dare il proprio contributo, è pregato inviare una mail a aiea@aiea.it, specificando, nell'oggetto "ARGOMENTI DI INTERESSE"

In una successiva newsletter provvederemo ad elencare tutti i temi proposti.

Partecipazione di soci ad eventi

Tutti i soci possono segnalare eventi, fatti e informazioni di possibile interesse comune da segnalare ad esempio nella newsletter.

In particolare, se partecipate ad un evento in qualità di organizzatore, relatore o chairman, valutate la possibilità di partecipare a nome AIEA. La partecipazione dell'Associazione ad un evento "deve" però essere decisa dal Consiglio Direttivo: siete quindi pregati di contattare il CD con ragionevole anticipo!

In caso non fosse possibile la partecipazione a nome AIEA, vi invitiamo ad indicare, nel profilo professionale la vostra appartenenza ad AIEA, Capitolo di ISACA

Bibliografia

E' on line il nuovo numero di InterLex (<http://www.interlex.it>)

Vi informiamo che sul sito www.cnipa.it sono disponibili molti documenti di interesse per i nostri soci. Ricordiamo che alla stesura di numerosi documenti hanno partecipato diversi nostri soci e che inoltre CNIPA organizza incontri o seminari aperti anche ai soci AIEA.

Le Newsletter delle altre Associazioni

E' disponibile on line, la **Newsletter CLUSIT** del 31 maggio 2009 (disponibile in PDF all'indirizzo www.clusit.IT/newsletter_31_05_09.pdf)

- Sono disponibili e qui allegate le Newsletter n.ro 333 e 334 del Garante Privacy

E' disponibile on line, la **Newsletter ANSSAIF** all'indirizzo www.anssaif.it



- PRIVACY E DIRITTO D'ISPEZIONE AL LIBRO SOCI: TUTELATI GLI INTERESSI DEGLI AZIONISTI
- E-MAIL E FAX INDESIDERATI: NUOVO STOP DEL GARANTE
- COMUNI, AMMINISTRATORI DI CONDOMINIO E TASSA SUI RIFIUTI
- MIGLIORARE LA PRIVACY: LE AUTORITÀ EUROPEE PRONTE A FARE LA LORO PARTE

Privacy e diritto d'ispezione al libro-soci: tutelati gli interessi degli azionisti

Gli azionisti di una società per azioni hanno diritto di conoscere l'indirizzo e i dati degli altri soci, al fine di contattarli e di poter tutelare i propri legittimi interessi. La legge sulla privacy non limita la conoscibilità da parte degli azionisti dei dati personali contenuti nel libro soci e non si pone in contrasto con la trasparenza dell'attività societaria.

Lo ha chiarito il Garante intervenendo in seguito alla segnalazione di un cittadino cui non erano stati messi a disposizione i dati completi contenuti nel libro-soci dell'azienda di cui deteneva alcune azioni. La decisione dell'Autorità assume particolare rilevanza in particolare per i piccoli azionisti.

L'interessato - in base al diritto d'ispezione garantito dal codice civile (art.2422) - aveva chiesto di consultare e di ottenere copia integrale digitale del libro soci, senza che venissero oscurati gli indirizzi dei soci-azionisti. La richiesta era motivata anche dalla volontà di poter eventualmente convocare l'assemblea e di esercitare i diritti di denuncia previsti dalla legge.

La società aveva invece consentito l'accesso solo ai nominativi contenuti nel libro-soci, ma senza i recapiti, sostenendo di non poter fornire tali informazioni perché esse erano tutelate, in quanto dati personali, dal Codice della privacy. L'azienda aveva peraltro aggiunto a sostegno della sua posizione l'impossibilità di richiedere il necessario esplicito consenso a tutti i quasi 700.000 soci interessati.

L'Autorità, con un provvedimento di cui è stato relatore Giuseppe Chiaravalloti, ha precisato quanto stabilito in un provvedimento adottato nel 2000, affermando che la legge sulla privacy non impedisce affatto al socio, nell'esercizio del suo potere d'ispezione, di poter accedere ai dati personali e agli indirizzi degli altri azionisti e di ottenere estratti del libro soci "a proprie spese". L'accesso a tali informazioni, peraltro, essendo previsto da un preciso obbligo di legge, non richiede il consenso dei soci.

E' stata invece dichiarata inammissibile la richiesta avanzata dall'azionista di ordinare alla società di consentire l'ispezione al libro-soci, dal momento che tale potere non è rimesso al Garante della privacy. Per vedere tutelati tali diritti, l'interessato dovrà infatti rivolgersi all'autorità giudiziaria ordinaria.

E-mail e fax indesiderati: nuovo stop del Garante

Anche se i dati sono estratti dalle Pagine Gialle o dai registri pubblici, quando si usano sistemi automatizzati è obbligatorio acquisire prima il consenso dei destinatari. Continua l'azione del Garante contro lo spamming e il marketing disinvoltato. L'Autorità ha vietato l'ulteriore trattamento illecito dei dati personali a cinque società che inviavano pubblicità tramite fax e posta elettronica senza il preventivo consenso degli interessati.

Il Garante è intervenuto a seguito delle segnalazioni di alcuni utenti che continuavano a ricevere e-mail e fax indesiderati nonostante non avessero mai manifestato alcun consenso all'uso dei loro dati per questo scopo. Lo società coinvolte (due inviavano lo spam tramite posta elettronica, tre tramite fax) in alcuni casi fornivano l'informativa e la richiesta di consenso contestualmente all'invio del primo fax o della prima e-mail che avevano già un contenuto di carattere commerciale.

L'Autorità ha ribadito, invece, che l'uso di sistemi automatizzati per inviare messaggi promozionali, anche quando si tratti di dati estratti da elenchi categorici o da albi, impone la preventiva acquisizione del consenso da parte dei destinatari. Alle cinque società è stato dunque vietato l'ulteriore trattamento illecito dei dati degli utenti interessati, i quali non potranno dunque più essere disturbati. La mancata osservanza del divieto del Garante espone anche a sanzioni penali.

Comuni, amministratori di condominio e tassa sui rifiuti

L'amministratore non gli dà ascolto e al condomino arrivano due cartelle Tarsu. E' accaduto ad un inquilino milanese che, ritenendo scorretto ed arbitrario l'utilizzo dei propri dati personali, è ricorso al Garante per la privacy.

Oggetto della segnalazione il fatto che l'amministratore, trasmettendo agli uffici del Comune il modello contenente la denuncia di "occupazione e detenzione di locali e aree" ai fini del calcolo e del versamento della tassa per lo smaltimento dei rifiuti solidi urbani (c.d. Tarsu) riferito alla sua posizione tributaria, non avrebbe tenuto in debito conto la sua intenzione – comunicata diversi mesi prima – di procedere direttamente a tale adempimento.

L'amministratore, dal canto suo, ha rappresentato all'Autorità di aver svolto lecitamente il trattamento dei dati del condomino in questione, dando esecuzione agli obblighi derivanti dal regolamento comunale, in particolare la compilazione di una scheda riepilogativa recante i totali dei dati raccolti, relativamente alle unità immobiliari del complesso abitativo.

Il Garante, pur riconoscendo l'effettiva liceità del trattamento posto in essere dall'amministratore, ne ha contestato il mancato rispetto del principio di correttezza. Se l'amministratore, infatti, avesse avuto cura di verificare che la dichiarazione del condomino era effettivamente già stata resa ai competenti uffici del Comune avrebbe evitato i disagi poi effettivamente verificatisi.

Il Garante ha dunque prescritto all'amministratore di porre in essere, prima di espletare le procedure relative procedure di calcolo delle tasse, ogni scrupolosa verifica delle denunce già effettuate da parte degli occupanti dello stabile amministrato.

Migliorare la privacy: le Autorità europee pronte a fare la loro parte

Alla recente conferenza europea delle Autorità di protezione dati di Edimburgo (23-24 aprile), i riflettori sono stati puntati sulla capacità del quadro attuale di norme e meccanismi di regolazione di fare fronte alle nuove "sfide" tecnologiche e globali. Significativi i risultati raggiunti.

- Nella Dichiarazione finale i Garanti hanno affermato con forza il patrimonio di esperienza e conoscenza che l'Europa può e deve apportare alla ricerca di soluzioni ed approcci sempre più condivisi per garantire la tutela dei dati personali a livello mondiale. La Dichiarazione

sottolinea, in proposito, la necessità di guardare ai molti punti in comune che già contraddistinguono il quadro normativo europeo e internazionale. Ma soprattutto invita i soggetti coinvolti, pubblici privati e istituzionali, a lavorare per mettere a punto norme e standard che - a partire dai principi di protezione dati già affermati - siano in grado di garantire e promuovere i diritti e le libertà fondamentali; di sviluppare nelle tecnologie approcci che prevedano la privacy come elemento essenziale ("privacy by design"); di realizzare una efficace protezione dei dati personali guardando in particolare ai rischi per i singoli e per la società nel suo complesso.

- E' stata adottata anche una Risoluzione sugli accordi bilaterali e multilaterali stipulati fra Paesi europei e non-europei per quanto riguarda la cooperazione giudiziaria e di polizia in materia penale (il cosiddetto "III Pilastro"). Considerata l'esistenza di troppe difformità nelle garanzie fissate da tali accordi per quanto riguarda la protezione dei dati, i Garanti chiedono agli Stati di garantire livelli uniformi di tutela anche attraverso l'inserimento di clausole-standard concernenti la protezione dei dati personali.

- La Conferenza di Edimburgo ha anche confermato a capo del Gruppo di lavoro europeo in materia di cooperazione giudiziaria e di polizia (WPPJ), per un successivo mandato di altri due anni, il presidente dell'Autorità italiana, Francesco Pizzetti. La Conferenza ha infine adottato il "manuale" elaborato dal Gruppo per definire alcuni criteri applicabili alle attività di ispezione e monitoraggio concernenti la materia del III Pilastro.

L'attività del Garante. Per chi vuole saperne di più Gli interventi e i provvedimenti più importanti recentemente adottati dall'Autorità

Misure in materia di propaganda elettorale - Esonero dall'informativa - provvedimento del 2.4.2009 (G.U.n. 85 dell'11 aprile 2009)

Conferenza dei Garanti europei a Edimburgo - Comunicato del 22.4.2009

Pizzetti: migliorare e rendere più effettiva la protezione dei dati dei cittadini europei - Comunicato del 23.4.2009

Pizzetti confermato presidente del gruppo di lavoro dei garanti europei sulla cooperazione giudiziaria e di polizia - Comunicato del 27.4.2009

NEWSLETTER

del Garante per la protezione dei dati personali
(Reg. al Trib. di Roma n.258 del 7/6/99).
Direttore responsabile: Baldo Meo.

Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n.121 - 00186 Roma.
Tel: 06/69677751 - Fax: 06/69677755. *Newsletter* è consultabile sul sito Internet www.garanteprivacy.it



- INFORMAZIONE SCORRETTA AL TEMPO DI FACEBOOK
- BIGLIETTI ON LINE, PRIVACY PIÙ GARANTITA
- SANITÀ: SISTEMA INFORMATIVO PER LE DIPENDENZE E PRIVACY
- VIDEOSORVEGLIANZA ED ESIGENZE DI SICUREZZA

Informazione scorretta al tempo di Facebook

I giornalisti che utilizzano notizie, fotografie e dati personali tratti dai social network devono sempre verificare le informazioni raccolte per esercitare con correttezza il diritto di cronaca.

E' quanto ha ribadito il Garante intervenendo su segnalazione di due cittadini, i quali avevano visto pubblicata da alcuni quotidiani la propria immagine presa da Facebook erroneamente associata a persone omonime decedute. In un caso si trattava di un incidente stradale, nell'altro di una vittima del terremoto avvenuto in Abruzzo.

I nomi pubblicati nei servizi di cronaca erano corretti, ma le fotografie ad essi associate erano state trovate facendo una semplice ricerca su Internet e scaricando l'immagine presente nei profili che i due segnalanti avevano aperto nel famoso social network. I giornalisti non avevano, dunque, verificato l'ipotesi che si potesse trattare di semplici casi di omonimia e hanno dato per decedute le persone sbagliate. Nel caso della vittima del terremoto, la fotografia errata, pubblicata da un quotidiano, era stata riproposta anche da due testate televisive nazionali.

Queste immagini - ha stabilito il Garante, con due provvedimenti di cui è stato relatore Mauro Paissan - non dovranno essere più pubblicate, diffuse né riproposte nell'archivio on-line delle testate coinvolte.

Associando l'immagine di una persona all'identità di un'altra, sono stati diffusi dati errati, mettendo in atto in tal modo un illecito trattamento dei dati personali.

Il Garante ha, pertanto, vietato alle testate, due locali e tre nazionali, di diffondere ulteriormente le fotografie dei segnalanti. L'Autorità ha imposto la cancellazione delle immagini anche dal sito web e dall'archivio storico on-line di uno dei quotidiani interessati che - dopo aver informato seppur tardivamente i lettori dello sbaglio commesso - continuava a rendere comunque accessibile da Internet la fotografia pubblicata per errore.

Biglietti on line, privacy più garantita

Il consenso all'uso dei dati non deve mai essere condizionato

Il consenso all'uso dei nostri dati non può mai essere condizionato, ma libero e consapevole. Non si può negare un servizio richiesto a chi non vuole sottoscrivere un modulo in cui non viene garantita la libertà del consenso. E' per questo motivo che il Garante ha vietato ad una società che opera su Internet l'ulteriore trattamento dei dati personali dei clienti.

La società, specializzata nella vendita on line di biglietti per eventi musicali, teatrali, sportivi e culturali, al momento della registrazione sottoponeva ai clienti un modulo che non permetteva di prestare un consenso specifico e differenziato. Era presente infatti una sola casella, per giunta già contrassegnata con l'apposito segno di "spunta". In questo modo i clienti oltre a dare il consenso all'uso dei propri dati personali, indispensabile per poter usufruire del servizio, lo prestavano automaticamente anche per le finalità di marketing. Chi non sottoscriveva il modulo così com'era non riceveva il servizio.

Intervenuto a seguito della segnalazione di un cittadino, il Garante ha vietato alla società l'ulteriore trattamento dei dati illegittimamente acquisiti, disponendo, inoltre, la riformulazione del modulo di iscrizione al sito con l'obbligo di fornire ai clienti la possibilità di prestare consensi differenziati.

"Il consenso che noi diamo all'uso dei nostri dati non può mai essere condizionato, ma deve poter essere espresso liberamente e in maniera consapevole - ha commentato il relatore del provvedimento, Giuseppe Fortunato - Non si possono imporre scelte ai clienti e ai consumatori o chiedere un consenso generico per usi diversi. Non si può negare un servizio o una prestazione a chi non vuole fornire i propri dati per finalità di marketing".

Sanità: sistema informativo per le dipendenze e privacy

Maggiore protezione per i dati di tossicodipendenti e alcolisti che si sottopongono a programmi di recupero socio-sanitari: elevate misure di sicurezza dei flussi di dati e delle reti telematiche, uso di dati anonimi quando non sia possibile ricorrere a codici, selettività e tracciabilità degli accessi.

E' un sì condizionato quello che il Garante privacy ha reso al Ministero del lavoro, della salute e delle politiche sociali sullo schema di decreto che istituisce il sistema informativo per le dipendenze (Sind). regioni e province autonome mettono a disposizione del Sind informazioni relative a strutture, attività e personale dei servizi che si occupano delle dipendenze. Tra gli obiettivi che si intendono raggiungere mediante il Sind, il monitoraggio dell'attività dei servizi, del volume delle prestazioni, delle caratteristiche dell'utenza e la valutazione del grado di efficienza e di utilizzo delle risorse.

Nel parere l'Autorità chiede innanzitutto che nel decreto siano indicate con maggiore precisione le finalità che si intendono perseguire e che giustificano la raccolta dei dati. Il Garante chiede, poi, che le regioni e le province autonome che non sono in grado di rendere non direttamente identificabili i pazienti (perché non dispongono di sistemi di codifica) utilizzino solo dati anonimi. Nello schema dovranno essere inoltre specificati gli uffici e il personale del ministero, delle regioni e delle province cui è consentito il trattamento delle informazioni e che il Ministero potrà avere accesso all'insieme delle informazioni raccolte nel Sind, mentre regioni e province potranno trattare solo le informazioni che inseriscono. Particolare attenzione deve essere inoltre posta nel caso in cui persone tossicodipendenti abbiano chiesto di mantenere l'anonimato nei rapporti con i servizi sanitari. Per innalzare ulteriormente le garanzie per i pazienti il Garante ritiene necessario che lo schema sia integrato con indicazioni mirate in materia di sicurezza: in particolare, perfezionando la disposizione che prevede il ricorso a tecniche di cifratura dei dati sensibili e prevedendo il tracciamento delle operazioni di accesso al sistema dedicato alla memorizzazione dei dati. Dovranno essere infine individuate modalità per la distruzione sicura dei supporti (hard disk, cd etc.) che contengono dati sensibili.

Videosorveglianza ed esigenze di sicurezza

Nei musei di Napoli le telecamere potranno conservare le immagini più a lungo

Il polo museale napoletano potrà conservare per trenta giorni le immagini raccolte da sistemi di videosorveglianza installati presso alcune aree museali,

fino a che permangono specifiche e comprovate esigenze di sicurezza.

Lo ha stabilito il Garante per la protezione dei dati personali che ha accolto la richiesta della Soprintendenza campana di poter prolungare, nel rispetto dei principi generali che regolano l'installazione e la gestione di sistemi di videosorveglianza, il tempo di conservazione delle immagini delle riprese video in alcuni musei. La Soprintendenza si era attivata in seguito all'allerta per un sopraggiunto allarme terroristico, inoltrata dal Comando dei carabinieri-tutela del patrimonio culturale. Al fine di prevenire eventuali attentati, l'Arma dei carabinieri aveva quindi suggerito di rimodulare il piano di sicurezza predisposto per la tutela e la conservazione delle opere, aumentando anche il tempo di conservazione delle immagini registrate dagli impianti di videosorveglianza. In base ai principi generali indicati nel Codice della privacy e nel provvedimento generale sulla videosorveglianza del 2004, le immagini e i dati relativi a persone identificate o identificabili possono essere conservate per un periodo limitato. Tale limite, tuttavia, può essere modificato in relazione alla necessità eccezionale derivante da un evento accaduto o realmente imminente, o in seguito alla richiesta dell'autorità giudiziaria o della polizia, motivata da un'attività investigativa in corso.

Il Garante, con un provvedimento di cui è stato relatore Giuseppe Chiaravalloti, ha quindi autorizzato la Soprintendenza a conservare sino a trenta giorni le riprese dei sistemi di videosorveglianza dei siti museali più esposti al rischio terrorismo, evidenziando però che il permesso temporaneo continuerà a valere solo nel caso in cui persistano comprovate esigenze di sicurezza.

L'attività del Garante. Per chi vuole saperne di più

Gli interventi e i provvedimenti più importanti recentemente adottati dall'Autorità

Conservazione dei dati di traffico: proroga dei termini - 29 aprile 2009 - provvedimento del 2.4.2009 (G.U. n. 107 dell' 11 maggio 2009)

Niente più nomi dei medicinali sullo scontrino fiscale rilasciato dalle farmacie – Comunicato del 7.5.2009

“Social Network: attenzione agli effetti collaterali” – Opuscolo informativo del Garante – 11.5.2009

Pazienti Udine su Facebook: il Garante privacy ha avviato accertamenti – Comunicato del 14.5.2009

NEWSLETTER

del Garante per la protezione dei dati personali
(Reg. al Trib. di Roma n.258 del 7/6/99).
Direttore responsabile: Baldo Meo.

Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n.121 - 00186 Roma.
Tel: 06/69677751 - Fax: 06/69677755. Newsletter è consultabile sul sito Internet www.garanteprivacy.it



Insight

N. 24 – Maggio 2009

Gestire e comunicare la crisi: un caso di successo

Il termine “crisi” suggerisce istintivamente un momento, nella vita di una persona o di un’azienda, dalle conseguenze non prevedibili e generalmente sfavorevoli.

Tuttavia, da un punto di vista etimologico, “crisi” indica una “separazione”, un “momento di svolta” (dal greco *krisis*) e in questo senso sottolinea non il momento specifico del suo manifestarsi, ma il cambiamento che fenomeni di questo tipo sono in grado di determinare.

Nella fase storica che stiamo vivendo, “crisi” è uno dei termini più ricorrenti nei media e nell’opinione pubblica, in riferimento all’impatto economico-finanziario che essa sta esercitando a livello globale.

Accanto a questo significato ne esiste un altro, ed è quello che qui ci interessa, applicato al ciclo di vita del business di un’azienda, per il quale una crisi va intesa come “evento o serie di eventi che possono generare un impatto significativo sulla continuità del business o sulla reputazione dell’azienda e/o dei propri marchi e prodotti”.

Le due definizioni sono strettamente connesse: è infatti vero che una crisi a livello globale può ripercuotersi a cascata sulle singole realtà; ed è vero anche l’opposto, cioè che crisi di singole aziende (si vedano ad esempio i casi Enron e Worldcom) possono imporre l’adozione di provvedimenti per l’intero mercato, e non solo per la specifica azienda coinvolta.

Nel presente contesto economico e finanziario le tematiche legate al Crisis Management & Communication sono di grande attualità: lo scenario è quello di aziende coinvolte in riorganizzazioni aziendali, riduzioni del personale, chiusure di sedi o dismissioni di stabilimenti.

Queste iniziative vanno considerate e gestite sia in termini di impatti sui processi interni, sia in quanto fonti di possibili conflitti con dipendenti o altri stakeholder e richiedono pertanto di identificare i rischi e definire le migliori strategie per mitigare le conseguenze sul business.

In scenari come quelli descritti, l’adozione di un piano di Crisis Management & Communication si dimostra determinante per il contenimento dei possibili impatti, fornendo inoltre l’occasione per l’analisi e la revisione dei processi interni alle aziende, nell’ottica di una maggiore robustezza rispetto a eventi che ne possano compromettere la continuità.

Una crisi aziendale è forse il momento nella vita di un’azienda che richiede le più grandi capacità di gestione sotto stress da parte del Management.

Gestire una crisi aziendale come se fosse “normale operatività” è un atto i cui effetti potrebbero ripercuotersi sull’azienda e al suo esterno in un’escalation di eventi di difficile controllo.

Al contrario, un’adeguata gestione della crisi fornisce elementi essenziali sia per la comprensione del contesto esistente, sia per allestire adeguati presidi contro potenziali eventi di rischio.

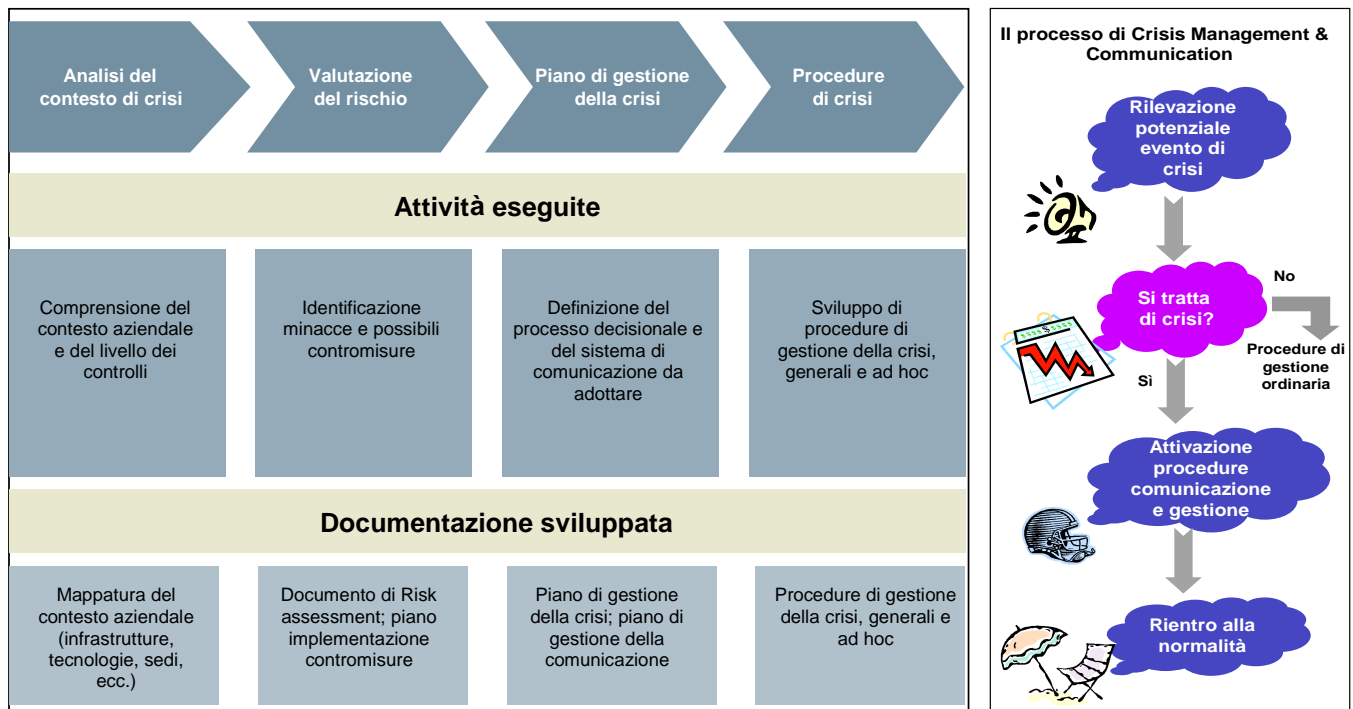
Una metodologia efficace di gestione della crisi deve prevedere un approccio integrato, che non ne isoli singole componenti per implementare contromisure discontinue, ma che concepisca la gestione della crisi come un processo, i cui elementi interagiscono strettamente e contribuiscono alla sopravvivenza e continuità dell’azienda.

L'approccio al Crisis Management & Communication

L'obiettivo primario di una soluzione di Crisis Management & Communication è la definizione e lo sviluppo dei meccanismi per affrontare e governare il contesto di crisi e, in particolar modo, identificare e ridurre i potenziali impatti negativi sul business e prevenire o limitare i danni a persone e beni.

In tale ambito anche la comunicazione riveste un ruolo importante ed è necessario definire i protocolli più efficaci per comunicare a tutti gli stakeholder coinvolti, con l'obiettivo di fornire istruzioni o rassicurazioni e proteggere gli asset e la reputazione dell'azienda.

Una soluzione di Crisis Management & Communication deve fare i conti con contesti dinamici, in cui gli scenari possono sovrapporsi e di conseguenza moltiplicare reciprocamente i possibili effetti. Da ciò consegue la necessità di un approccio che non consideri in modo isolato il singolo episodio, ma che affronti in modo organico tutti i fenomeni, prima in un'ottica di contenimento e quindi di miglioramento continuo. Un approccio metodologico coerente con questa esigenza prevede gli elementi sotto riportati:



Nel dettaglio:

Analisi del contesto di crisi

Comprensione del contesto aziendale: organizzazione, processi, infrastrutture, tecnologie e livello dei controlli in essere (ad esempio, il grado di sicurezza fisica).

Valutazione del rischio e identificazione delle contromisure

Identificazione delle minacce rispetto alla continuità dei processi aziendali, valutate in termini di probabilità di accadimento e gravità dell'impatto. Attraverso l'identificazione delle contromisure, per ogni rischio sono definite le azioni preventive e correttive e il relativo effetto di mitigazione. E' fondamentale in questa fase identificare tutte le misure che possono essere messe in atto per prevenire il verificarsi di situazioni di crisi, o contenerne preventivamente l'estensione e gli effetti.

Piano di gestione della crisi

Definizione del processo decisionale e del sistema di comunicazione da adottare nel corso della crisi. Il piano si basa sull'identificazione di una serie di scenari rispetto ai quali si sviluppano le procedure di gestione e comunicazione. In particolare, nel piano sono definiti:

- il comitato di gestione della crisi (Crisis Management Team - CMT), ossia il gruppo di persone dotate di potere decisionale e di coordinamento. Il gruppo è generalmente costituito da alcuni componenti permanenti, più altri designati ad hoc, a seconda del fenomeno in corso. Al fine di conseguire agilità e autonomia decisionale, il CMT dovrebbe essere costituito da un numero limitato di rappresentanti del Top Management;
- il sistema di governo del processo di Crisis Management & Communication, in termini di gestione del processo decisionale e di comunicazione, di identificazione degli eventi critici e delle corrispondenti linee guida per la gestione. In altri termini, per ogni evento identificato, sono specificati ruoli, responsabilità, azioni ed eventuali raccomandazioni;
- la gestione della comunicazione, che mira a governare il processo comunicativo durante la crisi. Ne sono componenti centrali, ad esempio, le procedure per la comunicazione, i template di comunicati e le Domande & Risposte per gestire i rapporti con i media, le autorità, i sindacati e le linee guida per il press monitoring.

Procedure di crisi

Sviluppo di procedure, generali e ad hoc, per gestire gli eventi di crisi e le relative contromisure, come, ad esempio, la gestione della produzione o l'erogazione dei servizi in situazione di emergenza o di controllo degli accessi del personale agli impianti o alle sedi. Le procedure sono richiamate all'interno del piano di gestione della crisi.

Data l'estensione degli impatti che una crisi può determinare, essa deve essere gestita attraverso competenze trasversali e un approccio multidisciplinare.

Le competenze richieste, finalizzate all'individuazione delle opportune contromisure, sono di varia natura e riguardano competenze specifiche della soluzione di Crisis Management & Communication quali:

- **gestione del rischio;**
- **gestione della continuità operativa;**
- **sicurezza fisica e degli accessi;**
- **sicurezza logica;**
- **gestione della comunicazione e coaching.**

Accanto a queste specifiche competenze, vanno annoverate anche quelle riguardanti aspetti generali, di business o di altra natura, che possono essere richieste a seconda dei contesti di crisi che si analizzano:

- **processi di business dell'azienda;**
- **gestione del personale;**
- **sicurezza sul lavoro;**
- **competenze legali.**

Il Crisis Management & Communication è una delle componenti del Business Continuity Management, ovvero dell'insieme di soluzioni per proteggere i processi critici di un'azienda da eventi che ne

potrebbero interrompere l'operatività, esponendola di conseguenza a danni rilevanti.



Nell'ambito del Business Continuity Management, il Crisis Management & Communication costituisce il primo passo per il ripristino dell'operatività aziendale. Accanto ad esso troviamo:

- **Business Resumption Planning, mirato al ripristino delle funzioni e dei processi critici per l'operatività del business;**
- **IT Disaster Recovery Planning, mirato al ripristino degli asset critici ICT (applicazioni, sistemi, reti di telecomunicazioni).**

Data la complessità della tematica e gli impatti sull'organizzazione, non è possibile fronteggiare una crisi attraverso interventi puntuali e discontinui. L'assenza di una strategia in questo senso rappresenta una limitazione che costituisce una delle principali fonti di rischio.

L'analisi degli scenari e la determinazione delle procedure per gestirli deve essere effettuata in modo preventivo, poiché al momento della crisi spesso non si possiedono la necessaria lucidità e il tempo richiesto per affrontare coerentemente gli eventi.

Una compagnia statunitense su 4 ha dichiarato di avere attraversato un “disastro” negli ultimi 5 anni.

Su 5 aziende colpite da un disastro esteso, 2 non sono in grado di riavviare l'attività; 1 riesce a riavviare l'attività, ma fallisce entro due anni.

(fonte: Contingency Planning & Management Magazine)

Dopo l'attacco dell'11 settembre, il 70% delle aziende coinvolte e prive di piani di gestione della continuità operativa è fallito.

(fonte: SEC – Security Exchange Commission)

Un caso reale

A causa di spinte congiunturali e difficoltà legate al mercato, un'azienda manifatturiera ha rivisto le proprie strategie, decidendo di chiudere uno dei siti produttivi e riassorbire la capacità produttiva nei restanti.

Tale ristrutturazione avrebbe potuto configurarsi come contesto di crisi qualora le reazioni da parte dei dipendenti e delle aziende collegate avessero minacciato la continuità del business o l'immagine dell'azienda.

I dipendenti dell'azienda (e delle aziende ad essa collegate) costituivano la principale fonte di rischio, in quanto avrebbero potuto organizzare scioperi e dimostrazioni tali da bloccare la produzione o la distribuzione, con conseguenti ripercussioni economiche (nel caso peggiore, la perdita di clienti).

Ancora, avrebbero potuto verificarsi episodi di danneggiamento verso cose o persone, o incidenti dovuti alla negligenza nella manutenzione dei macchinari, nonché ad atti di sabotaggio.

Ci si potevano attendere reazioni da terze parti (da un lato clienti e fornitori, dall'altro sindacati, istituzioni locali, clienti, media, etc.), che miravano a scendere in campo per influenzare la decisione presa dall'azienda ed evitare la chiusura dell'impianto.

Un'ulteriore fonte di rischio era legata alla possibilità di danneggiamento o furto della documentazione relativa ai contratti con i clienti, che avrebbe potuto

fornire ai competitor importanti informazioni commerciali.

Senza la definizione e implementazione di adeguati presidi, l'escalation di questi eventi avrebbe potuto essere ingovernabile. Si veda in merito la figura sottostante, che mostra con un esempio di come lo scenario di crisi possa generare nuovi elementi di crisi, se non sono predisposti adeguati interventi.

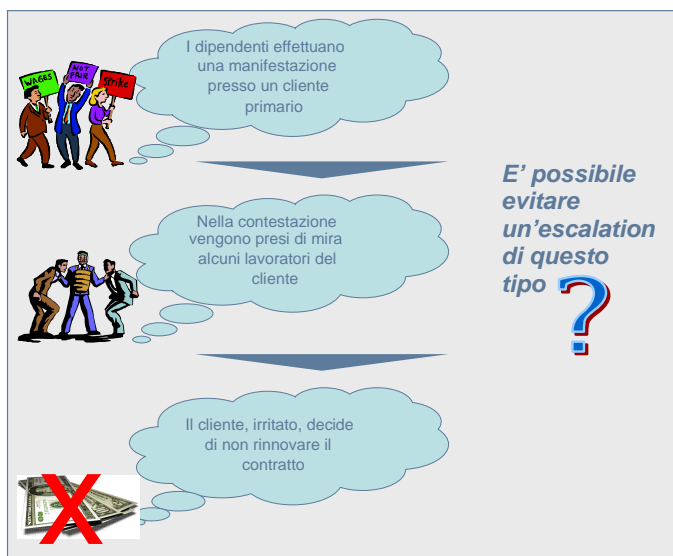
Il team Protiviti specializzato sulla tematica Crisis Management & Communication è stato coinvolto per analizzare la situazione e disegnare possibili interventi. Poiché al momento dell'avvio delle attività la decisione aziendale non era stata ancora annunciata, Protiviti ha adottato tutte le misure necessarie a garantire la totale segretezza circa gli obiettivi e l'ambito del mandato.

Il team coniugava competenze metodologiche sulle tematiche di Crisis Management & Communication, quali:

- **framework di Risk Assessment e Crisis Management**
- **Business Continuity Management**
- **comunicazione**

con competenze più specialistiche, quali

- **sicurezza fisica in impianti industriali**
- **supporto legale.**



Come si può comunicare durante la crisi senza far salire la tensione?

Come si dovrebbe affrontare un'occupazione dei dipendenti?

Qual è il modo migliore per rispondere alle provocazioni di un giornalista?

Come si può evitare la diffusione di informazioni riservate?

Come si possono limitare i danni all'immagine aziendale?

L'intervento consulenziale ha previsto innanzitutto la definizione del contesto di crisi e delle sue possibili conseguenze, attraverso una serie di interviste e riunioni con il management.

A seguire, sono state svolte alcune visite ai siti produttivi e ai centri direzionali, per valutare i rischi e il livello dei controlli esistenti.

Sulla base di questa analisi, Protiviti ha sviluppato il Piano di Gestione della Crisi indirizzando i seguenti elementi:

- l'identificazione delle **contromisure preventive** per mitigare i rischi rilevati (accordi con fornitori e partner commerciali per gestire discontinuità nella produzione e nella logistica, identificazione delle potenziali integrazioni ai sistemi di sorveglianza degli impianti, modalità di gestione della manutenzione degli impianti per prevenire sabotaggi, etc.);
- la definizione del **Crisis Management Team**;
- la determinazione del **flusso informativo** per la gestione della crisi;

- la definizione delle linee guida per la **gestione della comunicazione** (identificazione dei Key Message e delle principali Question & Answer, definizione dei template per i comunicati, predisposizione di press release);
- l'identificazione dei **potenziali eventi di crisi** e, per ciascuno di essi, le linee guida da seguire (modalità per gestire la produzione e la logistica, requisiti per il servizio di vigilanza ed identificazione del fornitore, gestione del customer service);
- le **procedure operative** (in particolare, la procedura per la vigilanza ed il controllo degli accessi) e la procedura per la protezione della documentazione commerciale.

In chiusura dell'intervento, Protiviti ha erogato una sessione di **formazione per il Management** del cliente, mirata allo sviluppo e all'affinamento delle tecniche e modalità di comunicazione.

* * *

Per maggiori informazioni, rivolgetevi all'ufficio Protiviti più vicino o a Enrico Ferretti (enrico.ferretti@protiviti.it – 06 42049801) e Giuseppe Blasi (giuseppe.blasi@protiviti.it - 02 65506301).

Global COMMUNIQUÉ

ISACA Unveils Evolved Strategy

All members and certification holders will shortly receive a brochure outlining the ISACA® strategy, resulting from the recent market research study undertaken. Members can immediately access the brochure at www.isaca.org/strategy.

The research was undertaken while recognizing ISACA's strengths and its challenges within a shifting marketplace and evolving constituency base. The study and strategy initiative were prompted by a desire to stay ahead of the curve.

As noted by International President Lynn Lawton, CISA, FBCS CITP, FCA, FIA, "...in today's world, events and the environment are always changing, and if the organization does not change as well, it can quickly find itself behind the times."

The strategy was designed to address a vision and mission built on the following basic tenets:

- Users and organizations must feel trust in their information systems, and they must realize value from them. Trust and value are the outcomes of our members' endeavors.
- ISACA has a global leadership position in knowledge, certifications, community, advocacy and education.
- ISACA focuses on certain specific professional spaces—information systems assurance and security, enterprise governance of IT, and IT-related risk and compliance.

Although the specific wording of the vision and mission may still be in draft stage, the concepts are clear. The initiatives outlined in the strategy reinforce each other and support the mission and

vision, and are grouped within five major strategic themes:

- 1. Realize full potential of *Control Objectives for Information and related Technology (COBIT®)*.** COBIT is widely known and adopted, giving it a leadership position and favorable brand recognition. To build on that reputation, ISACA will create new intellectual property (IP) and incorporate existing IP under the COBIT architecture. Through an open source model, volunteers will drive development of COBIT levels 3 and 4 controls material.
- 2. Enhance commitment to the core constituency of IT audit and controls.** To address constituents' evolving need for

Continued on page 3

Inside This Issue

MAY 2009, VOLUME 5

ISACA Unveils Evolved Strategy	Page 1
New Web Site Features Help Members Stand Out in a Tough Economy	Page 1
President's Message.....	Page 2
Distance Learning.....	Page 2
Chapter Spotlight: Milan Chapter Academic Relations	Page 3
Notice of the 2009 Annual Meeting of ISACA	Page 4
Report of the Nominating Committee	Page 4
Global Events.....	Page 5
ISACA Looks Back: 1983-1986	Page 6
What's New at the Bookstore	Page 6
Certification Update.....	Page 7
Highlights of March 2009 Board Meetings	Page 7
Conference Q&A: 2009 International Conference	Page 8
Conference and Education Update.....	Page 9
Using Technology to Cut In-house Fraud Off at the Pass	Page 10
Research Q&A: COBIT and Application Controls.....	Page 11
Research News.....	Page 11
2009 ISACA Calendar of Events.....	Page 12

New Web Site Features Help Members Stand Out in a Tough Economy

In April 2009, ISACA launched a new web site section called Stay Competitive—Stand Out. As part of ISACA's response to the global economy, five new member services have been developed to help members succeed in challenging times:

- **NEW COBIT discounts**—Members get COBIT® Quickstart free as part of their membership and 75 percent off the full subscription to COBIT Online®—a US \$150 value.
- **NEW e-Library**—For instant, self-directed learning, reference and support, members will soon be able to access an on-demand, customized collection of ISACA and third-party books, videos and other resources in a fully searchable, web-based environment powered by Books24x7.
- **NEW Career Centre enhancements**—The Career Centre will include more jobs, including those posted on other job boards, and more robust tools for job seekers. Coming soon, a free job board for freelancers will be available. Members will be able to post freelance/contract positions free of charge for other members to view and pursue.

• **NEW employer handout**—Ensure Success for Your Enterprise is a quick summary sheet of the top five reasons to invest in employees' ISACA memberships and certifications. Using this handy guide, members can be equipped to demonstrate the value of membership to their employer and colleagues.

• **NEW free CPE table**—This handy new reference itemizes 52 free continuing professional education (CPE) credits available from ISACA for certified members.

ISACA International President Lynn Lawton cites three reasons for this new web section: to help members keep a competitive edge in their current jobs to help members take their next professional steps while in transition and to help members ensure the success of their enterprises.

The new web section can be accessed from the ISACA web site home page or at www.isaca.org/standout. Take a look today!

President's Message

In the 2008 *IT Governance Global Status Report*, issued by the IT Governance Institute® (ITGI®), researchers from PricewaterhouseCoopers found that when survey participants were asked how frequently information technology is included on their organization's board agenda, the response for "always" (32 percent) increased significantly from 2005 (by 7 percent) and 2003 (by 10 percent). Not surprisingly, the response "IT is never included" has virtually disappeared (only 1 percent). Additional results from the study show that it is clear that IT needs to be a primary driver of the overall enterprise strategy before it is considered at the board level on a day-to-day basis. In fact, among those who report that IT issues are always being addressed at the board level, 84 percent state that IT is very important to delivery on the enterprise's strategy.

These results are strong reminders of the growth and maturity of our field and of how absolutely vital our work is for enterprises around the world.

I mention this now because in conjunction with celebrating ISACA's 40th anniversary this year, we are embarking on an exciting new challenge. First, a bit of history. Just under a year ago, in June 2008, ISACA's Strategic Advisory Group (SAG) recognized that we were at an opportune time to review and, if needed, update our organization's strategy. SAG recommended that we engage McKinsey & Company to provide the supporting research, working from external and internal sources.

Some may question why we are doing this now. We have been extremely successful over the

years, experiencing unprecedented membership growth and financial stability, building a sterling reputation around the world for our leadership, and benefiting from an incredibly large and active group of volunteers. As we are all very aware, though, in today's environment, everything can evolve very quickly. If an enterprise doesn't anticipate and welcome change, it can quickly fall out of step and lose its strength and vitality. We recognize this simple fact and are proactively working to ensure that ISACA and ITGI remain in their strong leadership positions.

The research findings helped us to confirm some things and learn more about how we are perceived and what our constituents value. For example, we heard loud and clear that members are most hungry for practical, how-to information. We also now have clear insight into the core competencies that have made us successful, and what enhancements we need to make to continue creating opportunities. One important facet is that chapters will continue to play a critical role in maximizing the value of ISACA and ITGI to current and future members.

The Board of Directors recently unanimously approved—with great enthusiasm—the foundation of an updated strategic direction. We still have a lot of work to do to turn what are concepts into tactical reality, but we are very excited about the progress made so far. Please stay tuned over the next few weeks for additional details as they are available.

The Board of Directors thanks everyone who participated in the online survey or interviews, as well as all of those who have contributed their



**Lynn Lawton, CISA,
FBCS CITP,
FCA, FIIA
2008-2009
ISACA
International President**

expertise to the strategy initiative. We received recommendations and comments from people in different industries and with unique viewpoints from around the world. Based on these responses, we are confident that the conclusions drawn represent the very best thinking of a diverse group of ISACA members and constituents. As the feedback showed, ISACA isn't "broken." We are in the fortunate position of having passionate members and a strong network of chapters, which will help us build on the successes already achieved.

Lynn Lawton, CISA, FBCS CITP, FCA, FIIA
2008-2009 ISACA International President

Distance Learning Update

May 2009 e-Symposium

The May ISACA® e-Symposium is scheduled for Tuesday, 26 May 2009. To register for the May e-Symposium and take the first step toward earning three free CPE credits, please visit <http://isaca.brighttalk.com>. All e-symposia are recorded and archived for viewing on demand. For more information, please visit www.isaca.org/elearning.

ISACA e-Learning Campus

The CISA® Online Review Course is available on the ISACA e-Learning Campus. This interactive, web-based course was developed to provide Certified Information Systems Auditor™ (CISA®) exam candidates and ISACA members with an efficient and cost-effective tool for exam preparation and for performing information systems audits and reviews. For more information, please visit www.isaca.org/elearning.

EuroCACS and North America CACS Online

ISACA has created a webcast library from outstanding sessions recorded at the March 2009 European Computer Audit, Control and Security (EuroCACSSM) conference and the May 2009 North America CACSSM. Learners can earn 1.5 CPE credits by purchasing and completing each of the online sessions. Discounted pricing is available exclusively to ISACA members. The webcasts are available on the ISACA e-Learning Campus. For more information or to register, visit www.isaca.org/elearning.

ISACA Unveils Evolved Strategy

Continued from page 1

pragmatic, useful information, the strategy will focus on the development of more practical, how-to, benchmark and topical information, and on input and response to major regulations affecting IT controls. More recognition through certificate programs and additional credentialing will also be explored.

3. **Distinctly serve the certification needs of IT professionals.** Many IT professionals have professional interests and concerns within ISACA's areas of expertise. To address that audience, additional offerings will be investigated on the topics of using proper IT controls to identify, quantify and manage business and technology risks, and to comply with regulations impacting information systems. An enterprise certification based on CoBIT will be explored as well.
4. **Maximize return on marketing.** The strategy identifies many opportunities for ISACA to maximize its return on marketing expenditures: an expanded member retention program, regional growth efforts, segmented messaging, and use of Web 2.0 functionality to build and enable ISACA's community.
5. **Build ISACA's capabilities to deliver benefits to its constituents.** Growth and diversity have necessitated new development and delivery mechanisms to enable the association to keep up with member needs. ISACA must rethink some of its processes, even its branding. ISACA will embrace open innovation to engage members in developing deeper content and new products, will partner more proactively with other organizations, and will seek efficiencies within its own organizational structure and governance.

Not all elements of the strategy are finalized; it will be a living "document," granting ISACA the flexibility to respond as needed to changing circumstances.

What's Next

The next steps will be transitioning the strategic initiatives to tactical plans and weaving those plans into the program of work already scheduled for the year. Many of the plans are beginning right away and some of the results will be available by the end of 2009. Progress will be reported regularly via the web site and print articles.

ISACA is extremely grateful to the more than 1,800 members, certification holders, chapter leaders, and key board and committee chairs who participated in the interviews and surveys that guided and informed the strategy development. That input, coupled with the many discussions of the Board of Directors, Strategic Advisory Group and ISACA staff, has resulted in a strategy that reflects the best thinking of a broad sample of members and constituents. And, the opportunities for member engagement continue. Many individuals and groups will be involved in executing the strategy: chapters, key boards and committees, subject matter experts, and a host of others. The support of all those who have participated to date and those whose expertise will be needed in the future is gratefully acknowledged.

For more information on this topic, please view the webcast by Lynn Lawton archived at www.isaca.org/strategy.

Chapter Spotlight

Milan Chapter Academic Relations

In 2008, the ISACA Milan Chapter collaborated with the Association of International Education Administrators (AIEA) to promote the chapter to two Italian universities.

The goals for meeting with students at these universities included:

- Making students aware of IT audit, security and governance topics
- Promoting AIEA as a strategic contact point for the job market
- Establishing a link between academic, professional and business entities
- Promoting AIEA as a knowledge base through its close relationship with ISACA

The first session took place in the first quarter of 2008 at the University of Rome II, with about 40 students who were attending the second year in business administration. Students appreciated the session as an opportunity to face and, to some extent, discover a new profession, as well as to meet a world different from the academic one.

Subsequent sessions at University of Rome II targeted students attending the final year of schooling in various fields. The interest in those sessions was even higher than the first, in large part because the focus was on real job opportunities.

The initial session at Florence University also took place in the first quarter of 2008 and involved about 30 students. In the second half of 2008, two more sessions were offered: the first one at the Turin Politecnico (engineering) IT department, with about 50 attendees, and the second at Milan Politecnico, with about 30 attendees. The latter, due to the presence of many foreign students, was held in English.

In all, both students and professors expressed interest in the IT topics presented. Students were mainly interested in ISACA certifications as an opportunity to achieve a formal professional qualification. Professors were interested in exploiting the contact with ISACA and AIEA to broaden their relations and knowledge at an international level.

During 2009, the ISACA Milan Chapter plans to maintain the relationships established with these universities, by delivering, as they have requested, more sessions. Plans are also underway to contact other universities.

NOTICE of the 2009 ANNUAL MEETING of ISACA

ISACA will hold its Annual Meeting on Monday, 20 July 2009, at the Hyatt Regency Century Plaza in Los Angeles, California, USA. In accordance with the association's bylaws, the Nominating Committee submits the following slate as the proposed 2009-2010 Board of Directors.

2009-2010 ISACA Board of Directors Slate

Emil D'Angelo, CISA, CISM	International President
George Ataya, CISA, CISM, CGEIT, CISSP	Vice President
Yonosuke Harada, CISA, CISM, CAIS	Vice President
Ria Lucas, CISA.....	Vice President
Jose Angel Pena Ibarra, CGEIT.....	Vice President
Robert E. Stroud, CGEIT.....	Vice President
Kenneth L. Vander Wal, CISA, CPA	Vice President
Rolf von Roessing, CISA, CISM, CGEIT.....	Vice President
Lynn Lawton, CISA, FBCS CITP, FCA, FIIA.....	Past President
Everett C. Johnson Jr., CPA.....	Past President

Included on the agenda will be the president's annual report, the treasurer's report, ratification of significant board actions from the 2008-2009 administrative year and comments from the newly inducted international president.

All ISACA members are invited to attend.

Report of the Nominating Committee

By Robert S. Roussey, CPA, Chair

The charge of the ISACA Nominating Committee, as described in sections 7.02 and 9.01 of the ISACA bylaws, is to prepare a slate of candidates for the ISACA Board of Directors for installation at the annual meeting held at the International Conference. The Nominating Committee is chaired by a past international president of ISACA, and its members include two additional past international presidents and three to four members with significant ISACA experience and diverse geographic representation.

The committee takes very seriously its obligation to prepare a slate that represents ISACA's geographic distribution; its professional areas of interest; and a diversity of job titles,

professional experience levels and ISACA activity. Both the immediate needs and the future requirements of the association are taken into account. One of the committee's goals is to build "bench strength" on the board, that is, to populate it with creative individuals committed to serve for several years, so that ISACA gains the benefit of their growing expertise and knowledge.

The process is managed with attention to detail: the proper forms must be submitted in the correct way and by the published deadline. Nominations are treated with unbiased consideration, and strict confidentiality is maintained.

The 2008-2009 Nominating Committee is pleased to present the slate for the 2009-2010 ISACA Board

of Directors. As chair of the committee, I affirm that the committee's deliberations were carried out in accordance with the bylaws and good governance principles.

The 2008-2009 Nominating Committee members include:

- Robert S. Roussey, CPA, USA, Chair
- Everett C. Johnson Jr., CPA, USA (past international president)
- Marios Damianides, CISA, CISM, CA, CPA, USA (past international president)
- Abdul Hamid Abdullah, CISA, CPA, Singapore
- Manuel Aceves, CISA, CISM, CGEIT, CISSP, Mexico
- Bent Poulsen, CISA, CISM, CGEIT, Denmark
- Wayne Jones, CISA, Australia

Asia:

- The Hyderabad (India) Chapter (<http://isaca.org.in>) has held several educational events for its members thus far in 2009. Topics covered have included IT governance and its effectiveness in business performance, a demonstration of computer-assisted audit techniques software (CAATs), IDEA, auditing UNIX systems, protecting brand reputation and trust through business continuity, securing a desktop, and a discussion on the new IT risk framework. The chapter has also undertaken an initiative to conduct workshops for chapter members for the purpose of reviewing and providing collective feedback of exposure drafts issued by ISACA International.
- The Cochin (India) Chapter (www.isacacochin.org) hosted a seminar on information security and risk management. Several educational sessions were offered on topics including, information security threats and challenges in the corporate and banking sector, threats to information assets from insiders, information security—threat mitigation solutions, and software asset management and compliance issues. An inaugural presentation was given by Ajay Kumar, Ph.D., IT secretary from the Government of Kerala. Seminar attendees were able to earn seven CPE hours.
- The Indonesia Chapter (www.isaca.or.id) conducts monthly events on various industry topics for its members. At one session earlier this year, Hogan Kusnadi from Unipro spoke about improving an organization's "audit ability" in relation to information security. In today's dynamic environment, companies are subject to more and more regulations, which creates numerous compliance and audit issues. Kusnadi discussed the compliance and audit challenges in Indonesia and explored the tools available to improve a company's audit functions, including change management, configuration management, log management and event/incident management. In March, Sumit Bansal from Symantec spoke about best practices for IT compliance. Attendees learned how best practices are being implemented by industry leaders, enabling them to reduce security risks and incidents and thereby reducing related downtime.

Latin America:

- The Brasilia (Brazil) Chapter received its ISACA chapter charter in October 2008. While very busy getting operations up and running, the chapter has found time to offer valuable educational opportunities for its members. The first-ever seminar for the chapter was dedicated to governance applied within a government

environment. Two major organizations, Brasil Telecom and TCU (the federal audit court), presented their experiences with governance, control and compliance during the four-hour session. TCU discussed how the government is preparing to align with governance by adopting CoBiT as the main framework for its audit process. Future chapter events are in the works with topics influenced by the fact that more than 80 percent of the chapter's members are civil servants.

- The Monterrey (Mexico) Chapter (www.isacamty.org.mx) has conducted two presentations for its members this year. The first topic was titled Enterprise Risk: Identification, Risk Management and IT Governance, and the second covered supporting the management and auditing of business continuity using ISO/IEC 27001. For further details about these and other chapter activities, please visit the chapter web site.

Europe/Africa:

- The Budapest (Hungary) Chapter (www.isaca.hu) holds monthly seminars on the second Wednesday of every month for members to train in various IT-related topics and earn CPE credits. The regular Certified Information Security Manager® (CISM®) and CISA exam preparation courses have commenced, and the chapter board plans to hold a conference on computer crime later this year. The chapter is currently working toward accreditation of the CISA, CISM and Certified in the Governance of Enterprise IT® (CGEIT®) certifications in Hungary, and would like to accredit CGEIT training as a possible doctoral degree, as well. Additionally, preparations have also already begun for EuroCACS 2010, which will take place in Budapest (www.isaca.org/eurocacs).
- The Rome (Italy) Chapter (www.isacaroma.it) has many events planned through July 2009, each focused on different aspects of ICT security and/or auditing. The main topics covered will be security, law and information technology, and diversity management. In June, the chapter will host the second CoBiT Day, in association with the University of Rome (<http://mastersicurezza.uniroma1.it/>), and the first-ever Certification Day, in association with LUISS University (www.luiss.it).

North America:

- The Greater New Orleans (Louisiana, USA) Chapter (www.isaca-nola.org) hosted an interactive three-hour SANS@Home demonstration of the SANS 560 Penetration

Testing course. The seminar covered the penetration testing mind-set, accessing Windows without login credentials, rainbow tables and remote password cracking.

- Late last month, the Harrisburg (Pennsylvania, USA) Chapter (www.isaca-harrisburg.org) held a program on virtualization security. The discussion was led by Allen C. Johnson, Ph.D., from the University of Alabama at Birmingham and Chris Hutchinson of Cellular South Inc. Virtualization was demonstrated, as were technical assessments of the requirements, advantages, basic principles and advanced features of virtualized systems and networks. A specific emphasis was placed on security challenges and strategies required in devising an approach to virtualization.
- The Virginia (USA) Chapter (www.isaca-va.org) offered a timely session in March titled Navigating Your IT Assurance Career Through a Recession. The session provided participants with insight into actions IT assurance professionals can take (and avoid) to ensure continued visibility and impact. The session also included a discussion of the skills necessary to navigate a career successfully through a tough economy.
- A recent Atlanta (Georgia, USA) Chapter (www.isaca-atlanta.org) meeting provided attendees with detailed information about Payment Card Industry (PCI) compliance and e-discovery. Charles Burke from InfoSec Integrators addressed how secure coding best practices from the Open Web Security Project (OWASP) map to PCI Requirement 6 and 10. Ken Koch from KPMG LLP and Chris Willis from Rogers & Hardin LLP covered electronic data discovery (EDD) program development and leading practices around making EDD a repeatable process, mitigating risk and reducing cost.
- Earlier this year, the Vancouver (British Columbia, Canada) Chapter (www.isaca-vancouver.org) hosted a breakfast speaker session titled Overview of COSO's Guidance on Monitoring Internal Controls. Doug Steele, the British Columbia leader for Grant Thornton's special advisory services group and a specialist in internal controls, led the session that reviewed the new exposure draft document from the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is designed to help organizations monitor the quality of their internal control systems and provide practical guidance—a critical component to reporting on the effectiveness of internal controls. Other educational events conducted by the chapter this

Continued on page 6

ISACA Looks Back: 1983-1986



ISACA, then the EDP Auditors Association (EDPAA), experienced a great deal of growth and expansion in the mid-1980s.

Demand for the CISA certification continued to increase rapidly. A 1984 advertisement for the CISA exam noted that it would be held at 50 test centers. Just two years later, the number of test sites had surged to 92, and more than 1,700 candidates sat for the 1986 CISA exam. Today, the exam is offered at more than 200 locations twice a year.

In 1985, EDPAA experienced unprecedented growth, reaching 9,000 members in 48 countries.

The year 1986 was a busy one for EDPAA. Among the year's activities, an initial draft of *General Standards for Information Systems Auditing* was approved by the Standards Board for exposure. Additionally, *Control Objectives* was printed in Spanish for the first time, and the CISA examination became available in Japanese (it was also offered in English and Hebrew). That same year, EDPAA achieved a significant milestone with the formation of its 100th chapter, in Victoria (British Columbia, Canada).

The Asia-Pacific CACSSM and EuroCACS conferences were introduced that year, and were held in Singapore and Norway.

Also in 1986, an article titled "Will EDP Auditors

Be an Extinct Species by 2000 A.D.?" ran in volume 3 of the *EDP Auditors Journal*. The article stated, "Changing technology is doing more than just nipping at the heels of the EDP auditor as the two race toward the 21st century. Technology is overtaking... People coming out of college with accounting and other business majors will be well trained in using computers. So good will their training be that all auditors will audit through the computer and with a computer."

The same issue of the *Journal* also ran a telegram sent by then-US President Ronald Reagan to EDPAA in honor of the association's International Conference. He wrote, "You are leading the way toward the controlled and managed use of information systems to establish self-regulated, worldwide standards of professional accountability" and praised the association for recently doubling its membership.

The four international presidents who led EDPAA during this time were Ingrid Overson, Donald A. Grant, John W. Lainhart IV and Michael P. Cangemi.

For additional information on ISACA's history and its 40th anniversary, please visit www.isaca.org/40thanniversary.

Continued from page 5

year included a session titled Delivering on the Promise of IT Through Effective Governance, and a special workshop to promote Val ITTM and IT governance.

- In April, the Victoria (British Columbia, Canada) Chapter (www.isacavictoria.ca) conducted a seminar on the audit, control and security of mobile technology. The seminar focused on understanding the risks involved in using mobile technologies and the key controls one can use to manage that risk. Attendees learned how to utilize software, encryption and registry settings to properly control the various mobile tools in use today, and gained an understanding of the key areas of focus for security assessments and the specific areas of vulnerability. This month, the chapter is hosting a three-day intensive seminar on ISO 27001 implementation.

Oceania:

- The Brisbane (Queensland, Australia) Chapter (www.isaca-brisbane.org) is hosting a moderated panel discussion titled Business Reform and Change Enabled by IT—An Alternative Perspective, which will take place at the monthly meeting in May or June. The panel will include Tony Hayes, chair of ISACA's IT Governance Committee, a value governance integrator and a value governance implementer.
- The Canberra (ACT, Australia) Chapter (www.isaca-canberra.org.au) provides professional updates for its members on the third Tuesday of each month at 5:00 p.m. at the Canberra Club. Sessions and light refreshments are provided free of charge by the chapter to both members and nonmembers. A recent session, The Global Financial Crisis and the IT Profession, was presented by Milind Sathye, professor of banking and finance at the University of Canberra.

To share a chapter event and have it considered for inclusion in a future issue of *Global Communiqué*[®], please send a brief (i.e., three to five sentences) description (in English) of an upcoming or recent chapter event to chapters@isaca.org. Note: Deadlines for copy are six weeks prior to the first day of the month in which the information is published.

What's New at the Bookstore

The ISACA Bookstore offers the following useful resources for Sarbanes-Oxley:

- *IT Control Objectives for Sarbanes-Oxley, 2nd Edition**
- *The Sarbanes-Oxley Section 404 Implementation Toolkit: Practices for Managers and Auditors*
- *Sarbanes-Oxley IT Compliance Using Open Source Tools, 2nd Edition*
- *Sarbanes-Oxley Guide for Financial and Information Technology Professionals, 2nd Edition*
- *Profitable Sarbanes-Oxley Compliance*
- *CobIT[®] and the Sarbanes-Oxley Act*
- *Essentials of Sarbanes-Oxley*
- *How to Comply with Sarbanes-Oxley Section 404: Assessing the Effectiveness of Internal Control, 3rd Edition*

- *Essential Project Investment Governance and Reporting: Preventing Project Fraud and Ensuring Sarbanes-Oxley Compliance*
- *Making IT Governance Work in a Sarbanes-Oxley World*

(*Published by ISACA and ITGI)

Search www.isaca.org/bookstore by product name/title: Sarbanes-Oxley. Contact the Bookstore at bookstore@isaca.org or +1.847.660.5650.

Certification Update

Exam Admission Tickets

- Admission tickets will be sent by post and e-mail approximately four to six weeks prior to the 13 June CISA, CISM and CGEIT exams. Only fully paid candidates will be issued an exam admission ticket for admittance into the exam. Candidates may use either the hard copy admission ticket or a printout of the e-mailed e-ticket for entry into the exam. Candidates who have not received their exam admission ticket by 1 June 2009 should contact exam@isaca.org.
- Admission tickets include the date, registration time and location of the exam; the schedule of events for the day; materials required for the exam; and the reporting time on exam day. Candidates will not be admitted to the exam once the instructions have begun. To ensure prompt arrival the day of the exam, it is recommended that candidates become familiar with the exam location and the best travel route to the exam site prior to the date of the exam.

- In addition to the admission ticket, candidates should bring several sharpened No. 2 or HB pencils, an eraser, and an acceptable form of photo identification (ID), such as a driver's license, passport or government ID. This ID must be a current and original government-issued ID that is not handwritten and contains both the candidate's name as it appears on the admission ticket and a photograph.
- Candidates should review the admission ticket details carefully. If any of the information on the exam admission ticket is incorrect, the candidate should contact exam@isaca.org immediately with the specific problem(s).
- Detailed information on what can and cannot be brought into the exam can be found at www.isaca.org/cisabelongings, www.isaca.org/cismbelongings or www.isaca.org/cgeitbelongings.

Certification Revocation Alert

Certified individuals who have not reported 2008 CPE hours are subject to revocation, even if they have paid the certification maintenance fee. CPE hours can be updated online in the individual's certification profile. Renewal payments can be made online through the renewal process.

Five-year Application Deadline for CISA and CISM

Once successfully passing the CISA, CISM or CGEIT exam, individuals have five years to apply for certification. If an application is not submitted within this five-year time frame, the individual will be required to retake the exam. Reminder e-mails were sent in February to those candidates who passed the CISA or CISM exam in 2004 and have not yet applied for certification.

Please contact the certification department at +1.847.660.5660 or e-mail certification@isaca.org with any questions.

Highlights of March 2009 Board Meetings

The 2008-2009 ISACA Board of Directors and ITGI Board of Trustees held their final meeting of the administrative term in March 2009, in Frankfurt, Germany, in conjunction with EuroCACS. The Board of Directors and Board of Trustees discussed a wide variety of association and institute activities, as summarized below.

- **Strategic Advisory Group (SAG)**—SAG presented the wrap-up report of the strategy development project that has been underway since June 2008. The proposed strategic direction, which will be communicated via numerous outlets, focuses on a vision and mission that reflect the current focus of the organizations; ISACA's and ITGI's expertise in knowledge creation, professional guidance, certification and education; and a use of Web 2.0 technology to engage more volunteers in knowledge creation and validation. Execution of selected strategic initiatives will begin immediately, with more planned to begin in 2010 and 2011.

- **Governance Advisory Council (GAC)**—GAC gathered comments and potential revisions on the boards' charters and charter of expectations. Those charters, and the charters of all key boards and committees, will be revised as needed to align with the newly adopted strategic direction.
- **Constituency committees**—All three committees—Assurance, Security Management and IT Governance—reported on recent activities and decisions.
- **Web Site Implementation Task Force**—The task force reported on the status of the update of the ISACA and ITGI web sites. The revisions, which will enable ISACA communities, social media, member customization and additional e-commerce functionality, are targeted to go live by the end of 2009.

- **Professional Issues Task Force (PITF)** — PITF is working on further guidance related to COSO monitoring and expects the exposure draft to be available by late July 2009. The resulting document will be offered as a free download from the ISACA site.
- **Financial update and forecast**—In keeping with global economic conditions, ISACA is approaching its 2009 expenditures conservatively and making adjustments as needed to align with changing circumstances. The association is expected to be able to make its budgeted contribution to reserves for the year.

The next meeting of the boards will take place in Los Angeles, California, USA, at the site of the International Conference. The new boards for the 2009-2010 administrative term will be sworn in during the Annual Meeting of the Membership.

Conference Q&A: 2009 International Conference

Cheryl Santor, CISA, CISM, CGEIT, International Conference Program Committee Chair

Q Tell us a little about yourself; how long have you been involved with ISACA?

A In 2001, I became interested in ISACA when I was hired as the IT auditor for a bank. I knew if I was to perform well, I would benefit from an organization that would provide me information about my audit efforts. I went back to information security less than a year later and found ISACA was the best organization for information and support for those efforts.

Q How did you come to the International Conference Program Committee? What interested you in ISACA education and specifically this conference's development?

A I have taken a key role in helping with the development of this year's conference because it is being held in my chapter's area, Los Angeles, California, USA. Involvement has provided additional enrichment to my career. I have met many extraordinary people who give their time to help make ISACA beneficial to us members.

Q What do you find to be the greatest benefit of volunteering on the Program Committee? Why would you encourage others to volunteer to be involved in the planning of conferences in their region?

A The greatest benefit to my latest experience on the Program Committee has been the opportunity to meet great people willing to give of themselves and their time to provide worthwhile education to benefit the industry and ISACA members. Volunteering has been a great experience. Involvement as an ISACA volunteer allows you to be exposed to the experiences of ISACA's international members and build relationships that will benefit the industry, ISACA, and your own career and organization.

Q Please describe the speakers for this year's conference and how they were chosen?

A The International Conference Program Committee received an overwhelming number of session proposals from the call for papers. The committee members carefully reviewed each proposal to evaluate the topic, the way the potential speaker would be addressing the topic, and the speaker qualifications. The Program

Committee's goal was to select experts who could offer a global perspective on relevant topics to add maximum value to the conference attendees.

ISACA volunteer leaders for the 2009 International Conference include:

- Brian Barnier, member of the team developing the new IT risk framework
- Henny Claessens, chair of the Conferences and Education Board
- Urs Fischer, chair of the ISACA Audit Committee and leader of the team developing the new IT risk framework
- Phil Lageschulte, member of the Conferences and Education Board
- Debbie Lew, member of the COBIT Steering Committee
- John Pironti, member of the Conferences and Education Board
- Jo Stewart-Rattray, chair of the Security Management Committee
- Rob Stroud, chair of the COBIT Steering Committee and ISACA international vice president
- Ken Vander Wal, ISACA international vice president

The conference development also benefited from the involvement of the following past ISACA international presidents:

- John Lainhart, member of the IT Governance Committee
- Paul Williams, chair of ISACA's Strategic Activities Council
- Everett C. Johnson, member of the ISACA Board of Directors

Industry leaders participating in the event provide a variety of perspectives. These leaders include:

- Ninette Caruso, IT audit director for Nationwide Insurance
- Gene Schultz, chief technology officer (CTO) for Emagined Security
- Jennifer Bayuk, former senior managing director for Bear Stearns, JPMC
- George Dolicker, former chief information security officer (CISO) for Lenovo Computers
- Hugh Penri-Williams, former senior security advisor for Accenture France
- Steve Orrin, director of security solutions for Intel Corp.

Q Is there an overarching theme to this year's conference? Please describe the theme and the reasons that it was chosen for this year's conference.

A With ISACA's tagline of "Serving IT Governance Professionals," it was meaningful to provide a well-rounded, current, topical conference that extends to a global audience. Innovation is a continuous process in IT; this conference provides education and information for being innovative. Additionally, with the 40th anniversary, this year's International Conference is a celebration of how far ISACA and the industry have come and how ISACA continues to stay current and meaningful for its members.

Q What can we expect from the tracks and topics of the 2009 International Conference?

A The International Conference Program Committee developed sessions that embrace current and upcoming ISACA and ITGI research initiatives and strategies. These include:

- COBIT
- Val IT
- *The IT Governance Implementation Guide: Using COBIT® and Val IT™*
- *The IT Assurance Guide: Using COBIT®*
- *COBIT® and Application Controls*
- The new IT risk framework (upcoming)
- *Monitoring of Internal Control Systems and IT* (upcoming)
- *Business Model for Information Security* (upcoming)
- *Information Security Program Metrics* (upcoming)

Other key topics the Program Committee selected for the 2009 International Conference include:

- Offshoring and outsourcing issues
- Auditing IT projects
- Adaptive business controls
- Transforming information security to information risk management
- International financial reporting standard

For more information and to register for the 2009 International Conference, please visit www.isaca.org/international.

Conference and Education Update

ISACA offers a variety of training opportunities designed to provide knowledge and CPE credits on technical and managerial topics pertinent to IT audit, security and governance professionals. The event and training descriptions provided here will assist in planning personal and departmental training. For additional events, details and registration information, please visit www.isaca.org/conferences.

2009 Event Calendar

	North America CACS SM	ISACA [®] Training Week	ISACA Training Week	International Conference	ISACA Training Week
DATES	3-7 May 2009	18-22 May 2009	15-19 June 2009	19-22 July 2009	17-21 August 2009
LOCATIONS	Orlando, Florida, USA	Denver, Colorado, USA	Vienna, Austria	Los Angeles, California, USA	Boston, Massachusetts, USA
CPE HOURS	44	38	38	40	38

North America CACS

3-7 May 2009
Orlando, Florida, USA



Now in its 39th year, North America CACS provides comprehensive training for IT audit, security and governance professionals. The conference features seven tracks that focus on the latest strategies to address IT audit and security challenges from business, managerial and operational perspectives. The conference will feature keynote speaker Gary B. Jordan, vice president, director of internal audit for PBS&J Corp. In his keynote presentation, Jordan will discuss data mining and monitoring—critical components in creating preventive environments rather than traditional detective-oriented approaches. He will examine how the proactive approach fits into the future state of the IT profession and how professionals can continue positioning themselves and their departments toward organizational value optimization.

The conference will feature lectures, panel discussions and facilitated discussions divided into seven tracks:

- IT Audit Core Competencies
- IT Audit Tools and Competencies
- IT Audit Techniques for Evaluating Business Practices
- Compliance Issues
- Control Methodologies and IT Governance
- Information Security Practices
- IT Risk Management

Pre- and postconference workshops are also available. For more information, please visit www.isaca.org/nacacs.

ISACA Training Week

18-22 May 2009
Denver, Colorado, USA

15-19 June 2009

Vienna, Austria

17-21 August 2009

Boston, Massachusetts, USA

ISACA Training Week is a unique educational experience, designed specifically for IT audit, security and governance professionals. Courses provide in-depth coverage of relevant topics, a lively interactive format, world-class presenters and opportunities for networking. Course offerings include Fundamentals of IT Assurance and Audit, IT Assurance and Audit Practices, Information Security Management, and COBIT[®]: Strategies for Implementing IT Governance.

For more information about locations, course offerings and to register, please visit www.isaca.org/trainingweek.



International Conference

19-22 July 2009
Los Angeles, California, USA



The International Conference is the leading event for IT professionals around the world. This conference has long occupied the spotlight in the global IT community for providing in-depth coverage of leading and cutting-edge technical and managerial issues facing IT governance, control, security, audit and assurance professionals. Now in its 37th year, the International Conference continues to attract a cadre of international industry experts and world-class presenters. The International Conference serves as a stage where experience and knowledge on best practices, system security, audit tools and processes, and other topics that impact IT professionals the world over converge. This is an extraordinary and opportune occasion to network with peers and discover the differing ways similar problems are solved around the globe. Attendees can earn up to 40 CPE credit hours—19 for attending the conference and seven for each day of the conference workshops.

To learn more about this year's International Conference, please see the Conference Q&A on page 8 or visit the ISACA web site at www.isaca.org/international.

Using Technology to Cut In-house Fraud Off at the Pass

By Steve Stanek, KnowledgeLeader

Last September, a former chief financial officer (CFO) at Tommy Hilfiger Handbags and Small Leather Goods Inc. pleaded guilty to stealing US \$19 million from the company over nearly seven years. Among other crimes, the CFO admitted to secretly increasing his salary and bonuses, submitting and receiving payments for phony expenses, and adding one of his sons to the payroll for two years and paying him US \$225,000 without the son ever doing any work. How did he manage to get away with such scams for seven years?

"Because he was a manager," said Patrick Taylor, chief executive officer at Oversight Systems, a leading provider of automated continuous monitoring solutions. "Being on top of the organization chart gives a person a lot of power." Companies that use continuous monitoring technology, however, have a lot of power to head off in-house fraud. "The technology casts a wide net, and it becomes hard, if not impossible, to completely perpetrate a fraud," Taylor said.

Human nature and business pressures often come together when executives commit fraud. Taylor said some feel pushed into it in order to meet performance targets. Others are so driven to succeed that they fudge numbers to make themselves look better. Still others, like the Hilfiger executive, do it for personal benefit.

"At these levels of an organization, they know or are close to people who are reporting revenue or earnings, and so they have the access it takes to carry out a fraud," Taylor said. "They know who to talk to to make adjustments. Another factor worth looking at is the slippery slope. Many do not start with the intent of committing major fraud. They may say, 'Just this time, we will have a December 32.' Then, they need a March 33. Then, a June 35. They get there a step at a time."

Lack of Oversight Invites Trouble

In the Hilfiger case, though, the intent to steal from the company was clear. From an earnings standpoint, the fraud did not have a significant impact, "but it is not the kind of thing you want to see happening," Taylor said. "He was able to put into effect a transaction fraud without any cross-checks by giving himself pay raises, 'hiring' his son, faking expense reports, and passing through personal payments. There was no independent check on what he was doing."

Such checks are precisely what continuous monitoring technology can provide, as it examines each transaction from beginning to end, starting

with source systems and everything a transaction touches along the way. For instance, it would have caught the ghost payroll entry for the CFO's son.

"He added his kid to the payroll. Was he also put in the HR system? Was he assigned costs for a department? Did he show up as a registered user on the IT network? A new hire will typically hit a lot of systems," Taylor said.

Monitoring technology would have flagged someone being added to the payroll system that was not also added to other systems. Taylor said more companies are putting continuous monitoring into place along with good processes to resolve exceptions, then presenting that to their external auditors for their own evaluation of how the monitoring process is working.

"Their external auditors are relying on the technology and are involved on a more continuous basis," Taylor said. "The trick is to have a way to understand what is normal. A fraudster is doing something abnormal and hoping it will escape notice. If the continuous monitoring solution can understand normal, the company can be a step ahead of the fraudster."

He added, "It is tricky to do" because it is not practical to define a specific rule for everything that is supposed to happen in an organization. "What is needed is artificial intelligence or expert technology that uses advanced analytics to develop a baseline in a more automated fashion. In that way, it is possible to identify things that are unusual. A second key is to make it efficient for someone to review problems. There will be false-positives, errors and, hopefully, a very small sliver that are fraud. The rarest thing to find is fraud. If you know you will need to deal with that spectrum of issues, you must have an efficient exception-resolution ability in the system."

To develop this ability, Taylor recommends involving internal audit and outside auditors, with the most direct responsibility given to the internal audit department. They, in turn, need to work with people in operations or whoever runs the business process in question. "Those people need to see the errors," Taylor said. "Defects are nuggets to use for process improvement."

Continuous Monitoring Technology Pays for Itself

"On a day-to-day basis, companies that use continuous monitoring technology can expect to find they are not wasting as much money," Taylor said. "A long-term benefit, if you are rigorous in

how you record and document what you find, will be that you will have information you need to drive process improvement."

Internal audit should monitor how well operational management is using the system. For instance, they may notice a unit's exception backlog is increasing, which reduces the effectiveness of the system in finding errors.

"This gets into internal auditors having a positive role as advisors," Taylor said. "At the executive level, internal audit needs to have responsibility for looking at activities. Say the CFO is dismissing exceptions. Internal audit needs to double-check exception resolution activity of upper management."

When issues arise that appear to be more than errors or process problems, internal audit should take a direct role in the investigation. Usually, there will be a series of indicators that suggest fraud. Taylor said internal audit should look at exceptions and do an independent evaluation.

"Time and again we talk to chief audit executives who say, 'I have a pool of risks, new as well as existing routine risks. The more I can automate to cover routine risks, the more time I have to address new risks,'" Taylor explained.

"If we have taken the effort to attack the routine stuff way down, we have freed up the capacity to spend more time identifying and mitigating the other risks. This gives internal auditors more of a chance to think like a fraudster. It enables them to perform an *ad hoc* analysis and investigation. With proper use of continuous monitoring technology, they have effectively increased internal audit's capacity and made the job more compelling and interesting," added Taylor.

Editor's Note:

© 2008 Protiviti Inc. All rights reserved. This article was reprinted with permission from Protiviti's KnowledgeLeader (www.knowledgeleader.com). KnowledgeLeader is a subscription-based web site that provides audit programs, checklists, tools, resources and best practices to help internal auditors and risk management professionals save time, manage risk and add value. ISACA members receive a discount on an annual subscription to the service.

Research Q&A: *COBIT and Application Controls*

COBIT® and Application Controls: A Management Guide is available as a complimentary PDF download for ISACA members at www.isaca.org/downloads and in the ISACA Bookstore for purchase as a PDF format (for nonmembers) and print. The content was developed by a team of practitioners from the Deloitte Canadian and Belgium member firms, with assistance and input from many others within Deloitte Touche Tohmatsu member firms.

Q Why is this publication valuable? What unique content will it provide its readers?

A *COBIT® and Application Controls* is meant to provide additional guidance on application controls. Historically, management and users have focused primarily on the business functionality of the application systems, and the concept of application controls has been the domain of the auditors and compliance practitioners. However, because of the importance of reliable information, this publication is designed to reinforce that application controls do represent business functionality and are not the sole domain of the audit community.

The publication is structured based on the life cycle of application systems—from defining requirements through implementation, operation and maintenance and, finally, providing assurance on application controls. The life cycle activities support management needs to ensure that the controls within the application systems are sufficient to ensure the reliability of the resulting information.

Q For whom is the book written? What titles, roles will benefit the most from the publication and how?

A The primary audience of *COBIT® and Application Controls* is business and IT management and business process owners. Therefore, this publication uses business language and tries to minimize “audit-speak.” The secondary audiences are developers, users, auditors and compliance practitioners. The content is relevant in all global regions of ISACA.

Q What does this publication replace, relate to or complement?

A A new addition to the COBIT family, *COBIT® and Application Controls*, complements *COBIT® 4.1*, dealing more specifically with application controls AC1 through AC6 as defined in *COBIT® 4.1*. Providing this increased detail around application controls will help to improve the reader’s understanding of how application controls help enterprises maintain information integrity.

Q How should this publication be used?

A This is a useful document for raising management awareness of roles and responsibilities related to application controls. It provides guidance for those with responsibilities for the design, implementation, operation, management and assessment of application controls.

Research News

ISACA and ITGI are constantly working with industry professionals to develop new and innovative research for their constituents. The following publications have been released recently or are scheduled to be released soon. For more information on newly released publications, please visit www.isaca.org/deliverables.

COBIT User Guide for Service Managers

This is the first publication in a series planned to provide guidance on how to use COBIT when performing a particular role. The service manager is a significant role with high demand for guidance, and this guide contains:

- An explanation of the service manager role and why it is important for effective IT governance
- An introduction to different business and governance challenges service managers face and how COBIT can help
- The key governance tasks for the service manager role aligned to the IT Infrastructure Library (ITIL) V3 processes and COBIT 4.1 control objectives, with related roles and responsibilities expressed as a controls baseline
- Case examples
- A high-level maturity model for the service manager role
- Links to other references

COBIT® User Guide for Service Managers is available as a complimentary PDF to ISACA members at www.isaca.org/downloads and in the ISACA Bookstore (www.isaca.org/bookstore) for purchase by the public in electronic and print format.

Val IT Mapping: Mapping of Val IT 2.0 to MSP, PRINCE2 and ITIL V3

To support practitioners in understanding how these standards and frameworks can work together, a detailed mapping and comparison between these frameworks is presented in this publication. This document will enable practitioners of enterprise governance of IT to better serve as an interface between the IT audience and the board, executive and business management levels. *Val IT™ Mapping: Mapping of Val IT 2.0 to MSP™, PRINCE2™ and ITIL® V3* is scheduled to be available to ISACA members in June as a complimentary PDF at www.isaca.org/downloads and in the ISACA Bookstore (www.isaca.org/bookstore) for purchase by the public in electronic format.

2009 ISACA Calendar of Events

May

- 3-7 May **North America CACS**, Orlando, Florida, USA
- 13 May Early-bird registration deadline for the International Conference
- 18-22 May **ISACA Training Week**, Denver, Colorado, USA
- 20 May Deadline for contributions to volume 5, 2009, of *ISACA® Journal*
- 26 May **ISACA e-Symposium**

June

- 3 June Early-bird registration deadline for the ISACA Training Week, Boston, Massachusetts, USA
- 11 June Deadline for contributions to volume 3, 2009, of *CoBIT Focus*
- 13 June CISA, CISM and CGEIT exam administration
- 15-19 June **ISACA Training Week**, Vienna, Austria

July

- 1 July Early-bird registration deadline for the ISACA Training Week, Toronto, Ontario, Canada
- 15 July Early-bird registration deadline for Latin America CACSSM, San José, Costa Rica
- 15 July Early-bird registration deadline for Information Security and Risk Management Conference, Las Vegas, Nevada, USA
- 19-22 July **International Conference**, Los Angeles, California, USA
- 20 July **2009 Annual Meeting of ISACA**, Los Angeles, California, USA
- 22 July Deadline for contributions to volume 6, 2009 of *ISACA Journal*

ISACA Board of Directors

- | | |
|---|--|
| Lynn Lawton, CISA, FBSC CITP, FCA, FIA
International President | Frank K. M. Yam, CISA, FHKIoD, FHKCS, CIA, CFE, CCP, CFSA, FFA
Vice President |
| George Ataya, CISA, CISM, CGEIT, CISSP
Vice President | Everett C. Johnson Jr., CPA
Past International President 2005-2007 |
| Yonosuke Harada, CISA, CISM, CAIS
Vice President | Marios Damianides, CISA, CISM, CA, CPA
Past International President 2003-2005 |
| Howard Nicholson, CISA, CGEIT
Vice President | Greg Grocholski, CISA
Director |
| Jose Angel Pena Ibarra, CGEIT
Vice President | Tony Hayes, CPA
Director |
| Robert E. Stroud, CGEIT
Vice President | Jo Stewart-Rattray, CISA, CISM, CGEIT, CSEPS
Director |
| Kenneth L. Vander Wal, CISA, CPA
Vice President | Susan M. Caldwell
Secretary |

Staff

- | | |
|--|---|
| Susan M. Caldwell
Chief Executive Officer | Tom Lamm, CPA
Director of Research, Standards and Academic Relations |
| Scott Artman, CPA
Chief Financial Officer | Diane Nelson |
| Ron Riba
Chief Operations Officer | Brian Selby, CISA, CGEIT, MBCS, MIIA
Director of CoBIT Initiatives |
| Jane Seago
Chief Communications Officer | Manny Singh
Director of IT |
| Terry Trsar, CPA
Chief Professional Development Officer | Joann Skiba
Director of IP |
| Chuck Cribaro
Director of Human Resources | Conrad Stanton
Director of Finance |
| Rob England
Director of Web Strategy and Services | Karyn Waller
Director of Certification |
| John Engman
Director of Membership Services | Jennifer Hajigeorgiou
Senior Editorial Manager |
| Ron Hale, CISM
Director of Information Security Practices | |

Global Communiqué® is published by:

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Telephone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: publication@isaca.org
Web site: www.isaca.org

© 2009 ISACA. All rights reserved.

It is one of the objectives of ISACA to provide a forum for the free expression and exchange of ideas. Statements of position or expression of opinion appearing herein are solely those of the author and are not by fact of publication necessarily those of ISACA.

Member Benefit
of the
Month

KnowledgeLeader Discount

- 1:** A subscription-based web site that provides audit programs, checklists, tools, resources and best practices to help internal auditors and risk management professionals. ISACA members receive a discount on an annual subscription to the service.
- 2:** For more information, please visit www.knowledgeleader.com.