Information Systems Audit and Control Association®
A recognized global leader in IT governance, control and assurance.
Rome Chapter Newsletter
Email: isacaroma@isacaroma.it Web: www.isacaroma.it/newsletter Settembre 2004, numero 6

Sommario

Editoriale

Harmonisation Project

Gentili associati, nelle scorse settimane ho partecipato allo Standard Board di ISACA International ove sono state discusse e annunciate importanti novità per la nostra associazione. Vi confermo che, pur senza rinunciare alle radici storiche dell'IS Auditing, ISACA ha confermato di volersi concentrare fortemente sull' ICT Security a seguito, anche, delle richieste giunte, in tal senso, dagli associati in tutto il mondo. In pratica, come prima mossa in tale direzione saranno create due linee indipendenti di servizi agli associati: una per i CISA – che si concentrerà sull'IS Auditing e IS Governance - e l'altra per i CISM – focalizzata sulla sicurezza.
Una seconda novità, sulla medesima falsariga, è che lo Standards Board ha avviato l'**Harmonisation Project**, consistente nel rivedere tutti i documenti pubblicati (standard, guideline e procedure) e nel separarli tra documenti di Audit e documenti di Security (ri) scrivendo quelli mancanti, in modo da avere due set completi, uno per ogni settore.
Infine è stato annunciato che ci sarà un survey tra tutti gli associati per raccogliere idee e suggerimenti sui prossimi progetti da avviare.
ISACA International ribadisce, inoltre, l'invito a tutti gli associati a partecipare attivamente ai gruppi di studio e ricerca, ai quali, come ISACA Roma abbiamo già collaborato lo scorso anno; chiedo perciò a voi tutti di dichiararci la vostra disponibilità di massima, in modo da poter essere inseriti nei prossimi gruppi.
Per quanto riguarda il nostro capitolo, ho il piacere di annunciarvi che le prossime **giornate di studio** saranno il 28 ottobre e il 14 dicembre; a breve renderemo noto la pianificazione degli incontri per l'intero 2005 in modo da permettere, a tutti gli associati, una più agevole pianificazione degli impegni; tutto ciò grazie ad Ugo il nuovo responsabile dell'education di IsacaRoma.
Vi segnalo, infine, una nuova "sezione" della newsletter dedicata al mondo universitario: in questo numero si comincia con un'indagine sulla diffusione di CobiT in ambito accademico (**CobiT in Academia Program**).

A tutti un cordiale saluto.

Claudio Cilli, CIA, CISA, CISSP, CISM
Presidente ISACA Roma

Education

Intervista a Ugo Spaziani nuovo responsabile dell'education di ISACA Roma

Quando ci saranno le prossime giornate di studio?
Abbiamo organizzato due giornate di studio entro la fine dell'anno: la prima sarà giovedì 28 ottobre dalle 14.30 alle 17.30 presso l'ATAC, via Volturno 65 Roma; la seconda sarà martedì 14 dicembre stesso orario e stessa sede. Il programma del 28 ottobre è già pronto ed è riportato in altra parte della neswletter. Il programma del 14 dicembre è in via di definizione e sarà diffuso tra non molto. La partecipazione, come al solito, è gratuita previo conferma via email a: isacaroma@isacaroma.it indicando come oggetto: "registrazione convegno 28 ottobre" e riportando nel testo il nominativo del partecipante. Ricordo, infine, che la partecipazione a ciascuna giornata di studio permette di ottenere 3 ore di credito nell'ambito della CISA e CISM *Continuing Education Policy* per il mantenimento delle certificazioni.

E per il 2005?
Per il prossimo anno stiamo cercando, anche tenendo conto delle indicazioni che ci sono giunte dagli associati, di organizzare una serie di eventi più articolati.
Obiettivo primario è organizzare un "incontro di education" al mese, esclusi probabilmente giugno, mese dedicato agli esami di certificazione CISA e CISM, ed agosto. La novità principale è che prevederemo sia giornate di studio multi-tema (come è avvenuto sino ad oggi) sia giornate mono-tema; queste ultime saranno orientate ad un approccio più specifico su problematiche proposte direttamente dagli associati e finalizzate alla produzione di documenti tecnici, procedurali ed informativi che possano essere di utilità pratica per tutti coloro che affrontano in azienda le problematiche dell'IS Auding e Security.

Ritieni che l'education sia una componente fondamentale per la professionalità degli associati?
Credo che la formazione continua sia un obbligo per gli specialisti del nostro settore se si vuole mantenere un adeguato e completo livello di preparazione; occorre, quindi, garantire uno scambio di esperienze e risorse e l'associazione è nata, e si sviluppa, anche per questo! Ciò a tutto vantaggio delle aspettative e delle esigenze dei clienti.

Parlaci un po' di te: oltre che di sicurezza ed auditing, di cosa ti occupi?
All'inizio della mia carriera professionale mi sono occupato prevalentemente di *document* e *knowledge management.* Parlando d'altro, sono pilota di aereo (non solo piccoli velivoli ma anche l'MD80 per capirci…) grazie ai miei trascorsi in aeronautica militare e skipper!

Ugo Spaziani, CISA, lavora in Telecom Italia e si occupa di ICT da più di vent'anni. È responsabile per l'education di ISACA Roma. Può essere contattato via email al seguente indirizzo: u.spaziani@tin.it (inserire nell'oggetto: ISACA Roma – Education)

Certificazioni professionali

Pubblichiamo la terza parte dell'approfondimento sulle certificazioni professionali per i professionisti dell' ICT Auditing e Security. Parleremo di BS7799 Lead Auditor e PMP – Project Manager Professional.
Nei precedenti numeri sono state presentate: CISSP, CIA, OPSA, Security+ e GCFW.
Un sentito ringraziamento agli amici ed amiche che hanno collaborato a questo approfondimento.

Lead Auditor BS7799 manuale di sopravvivenza

di Corrado Giustozzi, CISM, BS7799 Lead Auditor

Una certificazione professionale interessante per chi si occupa di sicurezza logica soprattutto sotto il profilo dell'audit e controllo, e che sta oltretutto acquistando una buona considerazione sul mercato, è quella di *Lead Auditor* secondo lo standard BS7799. Per essere più precisi si tratta della seconda parte della norma nella sua edizione 2002, ossia in sigla formale BS7799-2:2002.
Come noto si tratta di quella parte della BS7799, ancora non recepita dall'ISO, che specifica i requisiti per stabilire, implementare, gestire, controllare, revisionare, aggiornare e migliorare un Sistema di Gestione della Sicurezza delle Informazioni documentato, e come tale riguarda specificamente l'implementazione dei controlli di sicurezza necessari. A tal fine la norma prevede l'uso di 127 controlli raggruppati in dieci famiglie, che vanno dalle policy di sicurezza alla conformità ai requisiti legali.

Il corso di preparazione all'esame per Lead Auditor dura quattro giorni, dal lunedì al giovedì, ed è davvero "full-immersion": la norma infatti prevede una formazione obbligatoria di quaranta ore, ossia dieci al giorno! In pratica la giornata di corso si svolge normalmente sino alle 18, poi prosegue con almeno un paio d'ore di esercitazioni e simulazioni in aula per poi finire con un'appendice di… compiti a casa da farsi necessariamente dopo cena! Non è un corso leggero, quindi pianificate una settimana di vera assenza dal lavoro se volete uscirne vivi. Da questo punto di vista è assai consigliabile il corso residenziale, ossia quello fatto in un albergo di un'altra città: lontani dagli impegni del lavoro e della famiglia sarete molto più tranquilli e concentrati, e se ne avvantaggerà anche la qualità del necessario lavoro di gruppo da svolgersi nelle inevitabili sessioni notturne.
L'esame, che si svolge il venerdì mattina, consiste in quattro sezioni scritte di difficoltà (e punteggio…) variabili: si va da alcuni quiz "di riscaldamento", che in tutto quotano 15 punti sul totale, alla stesura di un rapporto di audit che da solo ne quota 30. Il punteggio massimo è 100, e per superare l'esame occorre fare almeno 70. Attenzione: il tempo è deliberatamente limitato, per simulare la condizione di stress che si instaura in un reale audit, quindi occorre gestirlo al meglio. Ma non lasciate che la fretta condizioni la qualità della vostra calligrafia o del vostro stile: l'esaminatore può infatti sottrarvi fino a sei punti per disordine, errori o comunque pecche formali del vostro elaborato! Le statistiche dicono che circa il 30% degli esaminati passa al primo colpo, ed infatti l'esame si può ripetere gratuitamente (e senza rifrequentare il corso) entro dodici mesi; la percentuale di successo alla seconda prova sale al 70% circa. Se tutto va bene, entro un mese otterrete direttamente dall'Inghilterra il tanto sospirato diploma.
Ultimo consiglio: non ragionate da consulenti! Scopo dell'auditor è rilevare le eventuali non conformità a quanto dichiarato, non mettersi a sindacare se le cose sono state fatte bene o male. Si tratta di un cambio di punto di vista forse ovvio ma assai difficile da adottare quando, avendo lavorato come consulenti per tanti anni, viene spontaneo soprattutto cercare di migliorare ciò che si vede.

Corrado Giustozzi: giornalista scientifico (UGIS), esperto e consulente di sicurezza informatica (CISM, BS7799 Lead Auditor).
Collabora con il Comando Generale e con il Reparto Operativo Speciale dell'Arma dei Carabinieri, e fa parte del Comitato Scientifico della Polizia delle Telecomunicazioni. Ha condotto importanti progetti di audit ed assessment e progettato infrastrutture di sicurezza presso grandi aziende e pubbliche amministrazioni.
Attualmente è Security Evangelist presso Innovia S.p.A. Può essere contattato via email al seguente indirizzo:
corrado.giustozzi@innovianet.it

Project Management Institute
® Building professionalism in project management.®

Project Management Professional (PMP)

Quello di PMP è probabilmente il titolo che più di ogni altro certifica la competenza e la professionalità di un Project Manager. E' un titolo riconosciuto universalmente e viene assegnato dal PMI (*Project Management Institute*) che è un'organizzazione considerata leader a livello mondiale nel campo del Project Management con oltre 100.000 membri distribuiti in 125 paesi e la propria presenza in 67 nazioni con 200 Chapter. Il PMI è rappresentato in Italia dai Chapter di Roma, Milano e Napoli (http://www.pmi.org/prod/groups/public/documents/info/GMC_ChapterListingOutsideUS.asp#P1091_18782).
Per poter conseguire il titolo di PMP (*Project Management Professional*) è necessario innanzitutto dimostrare di aver maturato alcuni requisiti specifici in termini di addestramento e di esperienza e bisogna aderire ad un codice di deontologia professionale. Successivamente bisogna passare un esame basato su un test di tipo multiple-choice pensato per valutare obiettivamente e misurare la conoscenza della disciplina di project management del candidato. L'esame viene superato se in 4 ore si risponde correttamente al 70% di domande sulle 200 proposte. Il test viene amministrato centralmente ma viene proposto, via computer, attraverso delle aziende locali riconosciute e certificate dal PMI stesso per svolgere questa attività. La data della prova può essere concordata con la società stessa ed il test può essere svolto in Italiano. Il programma di esame si basa sui contenuti del PMBOK (*Project Management Body of Knowledge*) che rappresenta la "bibbia" per il buon Project Manager secondo il PMI. Il PMBOK descrive la "metodologia" di Project Management secondo il PMI e scompone questa disciplina in 9 aree di conoscenza. Si va dalla gestione di tempi, costi e risorse di progetto fino a quelle di rischio e di approvvigionamento. Dopo aver conseguito la

certificazione, per mantenere il titolo di PMP è necessario dimostrare un continuo impegno nella disciplina del Project Management soddisfacendo ai requisiti previsti dal Continuing Certification Requirements Program. Bisogna cioè accumulare un determinato punteggio nell'arco dei tre anni successivi a quelli in cui si è conseguita la certificazione. I punti si accumulano partecipando ad eventi, iniziative didattiche ovvero dimostrando la continua evoluzione della propria conoscenza nell'ambito della disciplina del Project Management. Rispetto alla certificazione CISA, che è prettamente rivolta al mondo dell'Information System, il PMP è tarato sulla gestione di Progetti in senso lato dove quelli informatici rappresentano solamente una piccola parte di questi. Alcuni riferimenti al project management si trovano nel Dominio 6 (Sviluppo) del Manuale Tecnico CISA, mentre alcune affinità possono essere individuate in alcune tecniche descritte nei Domini 2 e 7 dedicati rispettivamente all'Organizzazione ed all'Analisi dei Rischi, con le ovvie considerazioni dovute ai differenti contesti in cui ci si trova ad operare.Recentemente è stata introdotta dal PMI anche una certificazione denominata CAPM (*Certified Associate in Project Management*) rivolta a chi, pur ricoprendo il ruolo di Project Manager, è relativamente nuovo in questa professione. Come per il PMP, anche i candidati CAPM devono prima incontrare requisiti in termini di addestramento e di esperienza e quindi passare un esame. Per maggiori informazioni riguardo il PMP ed il CAPM, si suggerisce di far riferimento al sito del PMI (www.PMI.org).

Gian Luca Di Stefano, CISA, PMP, lavora in Computer Associates presso gli IM Services. Può essere contattato via email al seguente indirizzo: gianluca.distefano@ca.com

Iniziative del capitolo

Giornata di studio del 28 ottobre

ATAC – via Volturno 65

Programma sintetico

Ore 14.30 - Apertura dei lavori
Francesco Pica L'Internal Auditing nelle previsioni del d.lgs 231/2001.
Carla Trinchero Analisi dei rischi con CRAMM
Pausa caffè
Sergio Rubichi Logistica integrata - controllo su SLA e KPI relativi ad un sistema di outsourcing
Dibattito
Ore 17.30 - Termine dei lavori

La partecipazione all'evento è gratuita previo conferma via email a: isacaroma@isacaroma.it indicando come oggetto: "registrazione convegno 28 ottobre" e riportando nel testo il nominativo del partecipante; la partecipazione permette di ottenere 3 ore di credito nell'ambito della CISA e CISM *Continuing Education Policy* per il mantenimento delle certificazioni.

Giornata di studio del 14 dicembre

Il programma è in via di definizione e sarà pubblicato nel prossimo numero della newsletter.

Nuovi certificati CISA del capitolo

Riportiamo l'elenco degli associati che hanno superato l'esame di certificazione CISA lo scorso giugno. Complimenti!

Cognome	*Nome*	*Società*	*email*
Bernini	Fabrizio	Consip	fabrizio.bernini@tesoro.it
Cavallari	Manuele	Secure-Edge	Manuele.Cavallari@fastwebnet.it
Di Stefano	Gian Luca	Computer Associates	gianluca.distefano@ca.com
Giuliani	Antonello	Bull Italia	antonello_giuliani@tin.it
Palma	Ombretta	Siemens Informatica	ombretta.palma@siemens.com
Rizzi	Antonio	Computer Associates	

Santosuosso	Felice	Computer Associates	
Spaziani	Ugo	Telecom	u.spaziani@tin.it
Viola	Enrico	ECLAT	enrico_viola@yahoo.it

Per eventuali comunicazioni scrivere a isacaroma@isacaroma.it

Security
Intervista a Giulio Carducci

In che direzione va il mestiere del Security Consultant? Ne parliamo con Giulio Carducci, figura storica del panorama italiano della sicurezza informatica

Giulio Carducci ha maturato quattro decenni di esperienze professionali occupandosi di telecomunicazioni, informatica e direzione aziendale. Ha lavorato, in particolare, per grandi multinazionali, ha ricoperto il ruolo di direttore generale in un'Agenzia U.E. per il controllo degli aiuti finanziari, si è occupato di ricerca di risorse umane come associato di una tra le maggiori organizzazioni mondiali del settore. Il suo incontro con la ICT Security risale al 1994, con la fondazione di Securteam, oggi parte di Marconiselenia Communications (gruppo Finmeccanica). Da allora, tramite conferenze e articoli, oltre ovviamente all'attività professionale condotta con Securteam, di cui è presidente, ha contribuito concretamente alla promozione di una cultura moderna e consapevole per la protezione delle informazioni. Può essere contattato per mezzo del sito web: www.giuliocarducci.com

Giulio, come vedi il mercato italiano dell' ICT Security?
Il mercato della ICT non può non risentire dell'attuale situazione economica generale un po' sotto tono. Questa tendenza potrebbe essere tuttavia positivamente compensata da una crescita di consapevolezza circa la necessità di protezione da parte degli utenti. Esistono ancora spazi notevolissimi nelle aziende, nella P.A. e nell'utenza privata. La crescita di consapevolezza registrata presso gli utenti nel corso dell'ultimo decennio è ancora limitata e insoddisfacente. Servirebbe, sia in ambito P.A. che in ambito privato, un organismo preposto alla promozione della cultura e alla garanzia della qualità dei piani e delle soluzioni di sicurezza. Organismi che, raccordandosi a livello nazionale con le strategie e l'operatività di ENISA, http://www.enisa.eu.int, l'agenzia europea per la sicurezza delle reti e delle informazioni recentemente costituita, svolgessero un'attività intelligente e moderna per incrementare la fiducia di enti, aziende e privati negli investimenti in materia di sicurezza ICT.

Cosa intendi per attività moderna e intelligente?
Guarda, per anni, e a tutt'oggi, si è creduto e si ritiene che la promozione della sicurezza possa avvenire attraverso conferenze spesso assai generiche e ripetitive e con la pubblicazione di documenti e *white paper* che riciclano consigli, suggerimenti, profili minimi di protezione. I produttori continuano poi a presentare ai clienti i propri prodotti valutando solo in modo marginale la loro capacità di gestire nel tempo i prodotti stessi. Basterebbe che una piccola percentuale (diciamo un quindici per cento) degli investimenti in sicurezza fossero destinati ad attività di pianificazione e gestione (quella che io chiamo, insieme ad altri, "governo della sicurezza") per far funzionare molto più efficacemente le cose.
Un modo intelligente e moderno per la promozione della sicurezza significa, a mio avviso, rivedere lo scenario normativo, oggi pressoché esclusivamente affidato in Italia al Codice della Privacy, in un'ottica "infrastrutturale" e non solo di contenuti (dati sensibili, pornografia etc.), incentivare le aziende a investire in infrastrutture di gestione della sicurezza e non solo in componenti hardware e software, promuovere strumenti di garanzia delle soluzioni di protezione e, perché no, istituire riconoscimenti d'immagine ed economici per le aziende riconosciute "sicure".

La sicurezza in Italia è nata con un approccio "di nicchia": aziende come "Securteam" hanno fatto "cultura" su questi argomenti. Credi che questo sarà ancora possibile o il futuro è solo delle grandi corporation che possono offrire verticalizzazione e servizi standardizzati?
Sono vere entrambe le opzioni. Da un lato, e mi duole constatarlo, la caduta di vocazione per l'eccellenza che, con la scusa della riduzione dei costi, caratterizza le aziende non solo italiane porta, anche per la sicurezza, a scelte che, per forza di cosa, privilegiano le soluzioni e le forniture "standard", quelle, cioè, in cui le grandi corporation sono più competitive dei piccoli. Per contro, chi se lo potrà permettere o semplicemente

comprenderà l'importanza dell' "abito su misura" ricorrerà al "piccolo", a patto che questi abbia inventiva e professionalità tali da giustificare i maggiori prezzi dei propri servizi. Questa considerazione mi consente di introdurre qualche considerazione sull'evoluzione in corso della professione dell'ICT Security Consultant: una grande competenza tecnica sarà sempre l'ingrediente di base, cui tuttavia dovranno affiancarsi una visione maggiormente integrata della "business security" nel suo insieme e una maggiore considerazione degli aspetti di analisi del rischio e della organizzazione e gestione della sicurezza.

Il nuovo "Codice in materia di protezione dei dati personali" (d.lgs. 30 giugno 2003, n. 196) ha introdotto numerose novità in materia di sicurezza ICT: qual è la tua opinione a riguardo?
Anche a metà degli anni '90 quando a furor di popolo si contestava l'allora vigente d.lgs. 675/96 ho sempre sostenuto che uno dei grandi meriti di quella norma era l'aver prescritto un profilo minimo di sicurezza per le infrastrutture informatiche. Il d.lgs. da te citato ammoderna e amplia questo meritoria funzione. Il rovescio della medaglia è costituito dal rischio che si ritenga di aver fatto il massimo, con questa norma, quanto a prescrizioni per la sicurezza delle reti e delle infrastrutture ICT. In realtà, come ho già accennato, la normativa privacy, quanto a prescrizioni per la sicurezza, ha un orientamento prevalentemente contenutistico e specifico (tra l'altro non riguarda i cittadini privati), mentre, a mio avviso, si rendono necessarie prescrizioni minime di carattere infrastrutturale, indipendenti dai contenuti che, se critici, possono comportare misure aggiuntive.

Parliamo di formazione e certificazioni professionali: oggi tutti parlano di BS 7799… Qual è la tua opinione a riguardo?
Il problema è che, in Italia, quando si parla di certificazione, la forma prevale nettamente sulla sostanza. Se si dovessero contare e accreditare tutte le certificazioni di qualità rilasciate nell'ultimo decennio, l'Italia vanterebbe livelli medi di eccellenza invidiabili quanto a efficienza dei processi aziendali. E quindi una competitività mondiale la cui assenza è sotto gli occhi di tutti. Pochi hanno presente, quando valutano la certificazione di qualità di un'azienda, che per capire bene come stanno le cose, occorrerebbe andare a vedere in dettaglio quali processi e quale perimetro è stato effettivamente certificato.
Le stesse considerazioni valgono per le certificazioni di sicurezza. Si tratta quindi di uno strumento interessante e lodevole che tuttavia, per essere efficace, dev'essere accompagnato da una notevole dose di consapevolezza e maturità da parte delle aziende.

Che progetti hai? Di cosa ti stai occupando? Hai qualche lettura interessante da consigliare ai nostri associati?
In questo momento sto guardando con molto interesse a quanto sta avvenendo, in termini di iniziative per la sicurezza ICT, a livello UE. La costituzione dell'agenzia Enisa mi sembra un evento importante, di cui i governi nazionali dovrebbero tenere conto, attrezzandosi per collaborare e trarne il maggior vantaggio possibile.
Sul piano più personale, continuo i miei studi sui modelli di analisi del rischio e ho iniziato a lavorare al mio nuovo libro dal titolo provvisorio (o definitivo?) "Sicurezza compatibile". Ho visto con piacere che negli ultimi anni alcuni dei tanti giovani ex colleghi in Securteam hanno pubblicato libri in materia di sicurezza: è stato per me fonte di soddisfazione e li incoraggio a proseguire.
Quanto a letture da consigliare, per restare in qualche modo nel nostro settore, trascurando gli indispensabili aggiornamenti tecnici, suggerisco un vecchio libro dell'86 di Ulrich Beck (ma solo nel 2000 tradotto in italiano) "La società del rischio", http://lgxserver.uniba.it/lei/rassegna/030607a.htm, attualissimo e il "Codice della privacy", recente, degli stimatissimi Riccardo e Rosario Imperiali. Nella loro opera i due autori hanno avuto modo e capacità di commentare il d.lgs. 196/2003 in modo egregio, aprendo contestualmente a una serie di riferimenti e citazioni di fonti che fanno del testo una "summa" attualissima della tematica complessiva della sicurezza delle informazioni a livello sia italiano che europeo.

Università
Cobit in Academia Program

Inauguriamo una nuova sezione dedicata ai rapporti fra l'IS Auditing ed il mondo universitario; analizzeremo, in particolare, la diffusione del framework COBIT in ambito accademico. In questo articolo presentiamo le iniziative di ISACA International ed ISACA Roma per le università ed approfondiamo l'uso di COBIT presso l'Università di Venezia, la Scuola Universitaria Professionale della Svizzera Italiana e la prima Università di Roma, La Sapienza.

Iniziative di ISACA

Cobit in Academia Program
È un'iniziativa volta a sostenere la diffusione del framework Cobit in ambito accademico. ISACA International sta predisponendo e rilascerà entro il 31

dicembre 2004, per ora solo in lingua inglese, il seguente materiale didattico specifico:

- una presentazione generale del framework;
- uno "student book";
- una serie di case study.

Ulteriori informazioni possono essere richieste a: research@isaca.org

Academic Advocate Program

L'Academic Advocate program, promosso dall' Academic Relations Committee di ISACA, gestisce i rapporti e le collaborazioni, finalizzate alla reciproca conoscenza per ottenere reciproci benefici, tra l'associazione, le aziende ed il mondo accademico. Al programma partecipano, ad oggi 72 istituzioni universitarie.

Il gruppo di ricerca del Committee ha realizzato la prima edizione del "*Curriculum for Information Systems Auditing at the University Undergraduate and Graduate Levels*", disponibile via internet in http://www.isaca.org/TemplateRedirect.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=5879 (pdf, 198 k)

Il modulo per l'associazione al programma è disponibile in:
http://www.isaca.org/Content/NavigationMenu/Students_and_Educators/Academic_Relations/AcademicMembershipAppl.pdf (pdf, 37 k)

Ulteriori informazioni in:
www.isaca.org/academicadvocate

IsacaRoma

Il nostro capitolo sta collaborando alle iniziative sopra descritte offrendo assistenza ed informazioni alle università, scuole ed istituzioni accademiche italiane e della Svizzera italiana.

La prima attività che il capitolo romano ha predisposto consiste in un censimento delle iniziative universitarie che utilizzano Cobit allo scopo sia di fare pubblicità ad esse presso i propri iscritti e simpatizzanti sia di costituire una sorta di "network" virtuale fra tali istituzioni (ad esempio per facilitare lo scambio di esperienze).

Università Ca' Foscari di Venezia

COBIT è trattato all'interno del corso "Laboratorio di informatica applicata" (laurea in Informatica) tenuto dal dottor Alessandro Roncato presso il dipartimento di Informatica dell' Università Ca' Foscari di Venezia, http://www.dsi.unive.it/~labia/.

Il corso, da quest'anno completamente dedicato alla tematica dell'IT Audit, ha una durata di 24 ore per un totale di 12 lezioni; Cobit viene trattato in 4 lezioni.

Il materiale didattico utilizzato è quello ufficiale di ISACA liberamente scaricabile dal sito; sono state realizzate, inoltre, delle slide specifiche su COBIT, a cura del dottor Marco Fusaro di KPMG che collabora alla cattedra.

Nell'anno accademico 2003-4, il dottor Orillo Narduzzo, CISA, CISM, vicepresidente di AIEA (il capitolo ISACA di Milano) ha inaugurato la prima lezione del corso con un intervento dedicato a COBIT.

In sede di esame, per la parte Cobit, si richiede agli studenti di analizzare obiettivi di controllo e individuarne i rischi implicitamente correlati; inoltre, si deve fornire una proposta di implementazione di controlli correlati agli obiettivi di controllo.

Abbiamo chiesto un commento al dottor Fusaro sul grado di interesse verso Cobit da parte degli studenti.

"Gli studenti che hanno già affrontato il mondo del lavoro sembrano percepire l'importanza delle tematiche proposte" ci ha risposto Fusaro "gli altri faticano ad avvicinarsi alla materia poiché si tratta di qualcosa di completamente nuovo e distante dagli obiettivi che si sono posti iscrivendosi al corso di laurea."

Ulteriori informazioni e contatti:
Dott. Alessandro Roncato, Università di Venezia, roncato@dsi.unive.it
Dott. Marco Fusaro, KPMG, mfusaro@kpmg.it
La pagina web del corso:
http://www.dsi.unive.it/~labia/
Le slide su Cobit:
http://www.dsi.unive.it/~labia/Lezione6.pdf

MACS, Executive Master in Advanced Computer Science

Nel piano di studi del MACS , Executive Master in Advanced Computer Science*, della SUPSI, la Scuola Universitaria Professionale della Svizzera Italiana, è previsto il corso "DTI 1.36 Introduzione alla revisione informatica".*
Eugenio Corti, responsabile del programma, ci presenta i contenuti del corso e in particolare l'utilizzo di CobiT

Può presentarci il corso "Introduzione alla revisione informatica"?
L'uso sempre più esteso dei computer, delle reti e dell'informatica ha profondamente modificato la società contemporanea e il modo in cui le aziende operano. Nel contesto attuale, con la tecnologia in uno stato di continua evoluzione, l'integrità del sistema informativo è sempre più cruciale per garantire il buon funzionamento di tutta l'azienda. La revisione informatica, grazie ai suoi rapporti oggettivi consente alla direzione di tastare il polso del sistema informativo aziendale e di valutare i rischi e i controlli inerenti le attività gestite con l'ausilio dell'informatica, per esempio, ma non solo, la contabilità. La revisione informatica può inoltre servire per promuovere un uso parsimonioso delle risorse ed è spesso utilizzata per valutare l'avanzamento e la correttezza, dal punto di vista della sicurezza e del controllo, di grossi progetti informatici.
Il corso presenta una panoramica della revisione informatica, introduce i principali temi attuali e illustra gli strumenti solitamente utilizzati nello svolgimento dell'attività.
Il corso è inserito nel MACS (*Executive Master in Advanced Computer Science*), un master professionale rivolto soprattutto a persone attive nel campo dell'informatica che desiderano rinfrescare e migliorare le loro conoscenze.

Chi può frequentare il corso?
Il corso "DTI 1.36 Introduzione alla revisione informatica", frequentabile anche senza essere iscritti al MACS, mira ad avvicinare gli studenti alla revisione informatica e nelle due edizioni tenute finora, oltre che dai studenti iscritti al MACS, è stato frequentato da informatici, capi progetto, specialisti di sicurezza informatica, organizzatori, consulenti, contabili e revisori.
Il modulo "DTI 1.36 Introduzione alla revisione informatica" è stato recentemente inserito nel curricolo post diploma "Sicurezza informatica" coordinato da Silvano Marioni.

Qual è l'importanza di CobiT rispetto al totale dei contenuti del corso?
A CobiT è stata dedicata una lezione della durata di 2 ore più un esercitazione per un totale del 10-15% circa del totale dei contenuti previsti. L'obiettivo è di presentare CobiT nell'ambito di un corso introduttivo che intende toccare un po' tutti gli aspetti della revisione informatica.

Che tipo di materiale didattico viene utilizzato per CobiT?
Il materiale didattico è stato sviluppato autonomamente attingendo dal materiale ufficiale ISACA (Executive Summary, Framework, Implementation Tool Set, Control Objectives, Management Guidelines), da esperienze lavorative, da presentazioni di colleghi nell'ambito del Gruppo di lavoro "Revisione informatica" della Conferenza svizzera dei controlli cantonali delle finanze e da seminari di formazione CobiT.

Utilizzate lo strumento CobiT-on-line?
No. Per il momento, utilizziamo la versione cartacea.

Siete a conoscenza dell'iniziativa "CobiT in Academia Program"?
Si, sommariamente. Ne sono venuto a conoscenza leggendo la rivista "*Global Communiqué*" di ISACA.

Qual è il grado di interesse verso CobiT da parte degli studenti (se misurabile)?

Dall'elaborazione dei moduli di valutazione del corso è emerso che alcuni studenti vorrebbero approfondire meglio alcuni argomenti, tra cui CobiT. Direi che l'interesse dimostrato nei confronti di CobiT è stato buono e varrebbe sicuramente la pena valutare nuove proposte di corsi/contenuti. L'offerta nella Svizzera italiana deve naturalmente tenere in considerazione il bacino dei possibili partecipanti.

In futuro pensate di continuare ad utilizzare CobiT nei vostri corsi?
Si. Oltre alla presentazione generale della metodologia nel corso "DTI 1.36 Introduzione alla revisione informatica", stiamo valutando l'opportunità di proporre un corso specifico su CobiT.

Che giudizio generale dà su CobiT?
La metodologia CobiT rappresenta probabilmente il migliore strumento per il governo e il controllo dell'informatica e pertanto non può mancare in un corso di revisione informatica.
I pregi di CobiT sono i seguenti:

- è uno strumento ben strutturato, esauriente, concreto e preciso che rappresenta una base concordata, autorevole e in continua evoluzione;
- si adatta a tutte le configurazioni gestionali dell'informatica aziendale e assicura che le soluzioni informatiche siano allineate alle esigenze aziendali;
- focalizza l'attenzione sul governo aziendale (Corporate e IT governance);
- responsabilizza la direzione sull'utilizzo delle risorse compreso le risorse informatiche;
- dispone di un quadro di riferimento per la valutazione dei rischi informatici;
- facilita e migliora la comunicazione tra direzione, linea, utenti e revisori;
- assicura il rispetto delle disposizioni dell'organo di vigilanza e della legge.

Per quanto riguarda i punti di debolezza, credo che i limiti principali di CobiT siano:

- CobiT è una metodologia generale e non risolve tutto;
- l'humus aziendale deve essere adatto o adattabile;
- l'impegno per l'implementazione (integrazione in azienda, formazione ecc.) non è da sottovalutare (è forse l'aspetto più importante);
- il settore informatico aziendale dovrebbe pure adottare CobiT; l'ideale sarebbe forse di organizzare la funzione informatica sulla base della struttura di CobiT (troppo bello: faciliterebbe il lavoro ai revisori);
- la comunicazione risulta facilitata solo quando tutti gli attori sono a loro agio con CobiT;
- indisponibilità del materiale CobiT in italiano, ora (parzialmente) risolta grazie all'impegno dell'AIEA (ISACA Milano) e ISACA Roma
- una certa macchinosità della metodologia, ossia poco adatto a interventi minimi "alla buona": aspetto probabilmente risolto da CobiT Online e Quickstart.

Ulteriori informazioni:

La Scuola Universitaria Professionale della Svizzera Italiana (SUPSI) è una delle 7 scuole universitarie professionali svizzere (*Fachhochschule, Haute école specialisée, University of applied sciences*). Ha statuto universitario, orientato alla formazione professionale e alla ricerca applicata. Con l'Università della Svizzera italiana (USI), fondata nel 1996, costituisce il principale polo universitario di lingua italiana in Svizzera, raggruppante oggi circa 3000 studenti nella regione di Lugano.

Il MACS è un Executive Master in Advanced Computer Science o Studio Postdiploma in Informatica Avanzata della SUPSI - la Scuola Universitaria Professionale della Svizzera Italiana - e rappresenta un'offerta di formazione continua destinata a tutti i professionisti dell'informatica, con l'obiettivo di mantenere e sviluppare le conoscenze professionali e la competitività del singolo nel mercato delle nuove tecnologie.
http://www.macs.supsi.ch/

Il responsabile del corso è: Eugenio Corti, Controllo delle finanze del Cantone Ticino, eugenio.corti@ti.ch

Università "La Sapienza" di Roma, facoltà di scienze M.F.N.

Presso la prima Università di Roma, è attivo l'insegnamento di "Sistemi Informativi" per i Corsi di Laurea in Informatica e Tecnologie Informatiche (facoltà di Scienze Matematiche Fisiche e Naturali); COBIT è trattato nell'ambito delle lezioni dedicate all'Audit dei Sistemi Informativi e viene messo a confronto con i diversi standard applicabili per la "governance" e l'audit dei SI per fornire una utile base di riferimento per gli specialisti che operano nel settore. Il responsabile del corso è il prof Federico Minelle che viene coadiuvato, per gli approfondimenti sull'IS Auditing e COBIT, dal prof Romano Boni, CISA; quest'ultimo ha gentilmente risposto ad alcune nostre domande sull'argomento.

Da quanti anni viene utilizzato COBIT in questo corso?
Dall'anno accademico 2003-2004.

Che tipo di materiale didattico viene utilizzato?
Il materiale didattico è stato elaborato sulla base dell'esperienza professionale maturata ed è basato, per quanto riguarda COBIT, sulla documentazione ufficiale ISACA.

Utilizzate lo strumento Cobit-on-line e siete a conoscenza dell'iniziativa "Cobit in Academia Program"?
No ad entrambe le domande.

Qual è il grado di interesse verso Cobit da parte degli studenti?
Le lezioni sull'Audit dei SI sono state finalizzate a fornire le conoscenze di base su questo argomento, di cui è stata messa in evidenza la rilevanza, data l'inevitabilità di interazioni e la possibilità di coinvolgimento diretto nella futura attività professionale degli studenti. Il loro interesse, in particolare verso il COBIT non è comunque, al momento, misurabile.

In futuro pensate di continuare ad utilizzare Cobit nei vostri corsi?
Sì.

Conoscete altre iniziative accademiche che utilizzano Cobit nei propri corsi?
Non sono a conoscenza di altre iniziative accademiche relative a Cobit in Università italiane, mentre mi risulta che negli USA costituisce oggetto di alcuni corsi universitari.

Ulteriori informazioni e contatti:
Professor Federico Minelle, minelle@di.uniroma1.it
Professor Romano Boni, boni@di.uniroma1.it
La pagina web del corso:
http://cesare.dsi.uniroma1.it/~sistinf/index.html

IT Governance: COSO Enterprise Risk Management Framework

Introduzione

Il *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) ha pubblicato, lo scorso 29 settembre, l'aggiornamento del framework *Enterprise Risk Management* (ERM), in collaborazione con PricewaterhouseCoopers. Il framework descrive i principi, le componenti ed i concetti più importanti della gestione del rischio aziendale e fornisce una roadmap precisa per identificare e gestire i rischi.
L'ERM si basa sull' *Internal Control — Integrated Framework*, pubblicato nel 1992 dallo stesso COSO, cioè sullo standard internazionale più noto e diffuso per il sistema di controlli interni; tale standard, negli USA, è stato indicato come *guidaline* per la conformità al Sarbanes-Oxley Act dal SEC, l'organo di controllo della borsa; recentemente anche l'ISACA ha pubblicato un proprio documento che fa numerosi riferimenti al modello COSO (si veda: *IT Control Objectives for Sarbanes-Oxley* di ISACA, disponibile in: http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=13923 pdf 435 k).

Cos'è il COSO?
COSO è un'organismo privato che si occupa di controlli interni e *corporate governance*. Tra i membri di COSO vi sono l'American Institute of Certified Public Accountants, l'American Accounting Association, Financial Executives International, l'Institute of Management Accountants l' Institute of Internal Auditors.
www.coso.org

Documenti disponibili

La precedente versione del 2002 dell'ERM era, in quanto draft, liberamente scaricabile. La nuova edizione viene distribuita a pagamento; nel sito del COSO è disponibile, gratuitamente, oltre ad una faq sintetica sulle novità, un executive summary dell'ERM, (http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf, 195 k) ed è possibile ordinare i documenti ufficiali, cioè il Framework ERM completo e le Application Techniques.
Il Framework illustra i concetti fondamentali della gestione del rischio ed enfatizza il ruolo dei comitati direttivi e del top management aziendale. Le Application Techniques descrivono i concetti fondamentali per un enterprise risk management efficace anche in un'ottica di business.

IIA *paper position* su ERM
L' *Institute of Internal Auditors*, IIA, ha pubblicato la sua posizione ufficiale (*position paper*) relativa al ruolo dell' Internal Auditor rispetto all'enterprise risk management di COSO. Il paper sottolinea le

modalità con le quali gli auditor devono mantenere la propria indipendenza ed obiettività ed i passi da compiere per garantire valore ed efficacia all' organizzazione. Il documento può essere scaricato da http://www.theiia.org/iia/download.cfm?file=283,pdf 397 kB.

The Institute of Internal Auditors
Progress Through Sharing

Definizioni

L'Enterprise Risk Management è un processo aziendale strategico e trasversale che deve essere gestito dal top management aziendale; il suo scopo è identificare gli eventi che possono generare danni o perdite e gestirli coerentemente con la propensione al rischio aziendale e con il raggiungimento degli obiettivi di business.
I rischi, di conseguenza, sono definiti come quegli eventi che possono produrre impatti negativi, cioè impedire la creazione di valore o ridurlo; viceversa le opportunità di business sono gli eventi che producono "impatti positivi". Cioè vuol dire che la gestione degli eventi, potenzialmente positivi e negativi, è un compito del management e, di conseguenza, un elemento fondamentale della *governance* aziendale.

Componenti dell'ERM

L'Enterprise risk management si compone di otto componenti correlati:

- Internal Environment: comprende i valori aziendali, le competenze, lo stile manageriale, le responsabilità;
- Objective Setting: gli obiettivi aziendali devono essere chiari e condivisi e possono essere classificati come:
  - strategici, che si riferiscono, cioè, alla *mission* aziedale;
  - operativi, che si riferiscono, cioè, all'efficacia ed efficienza;
  - di reporting, che si riferiscono, cioè, alla qualità e correttezza delle informazioni finanziarie o meno, che l'azienda offre al mercato, agli azionisti, ai dipendenti, ai fornitori;
  - di conformità, che si riferiscono, cioè, al rispetto delle leggi e dei regolamenti di mercato;
- Event Identification: è la corretta identificazione di rischi ed opportunità, come precedentemente indicato;
- Risk Assessment: i rischi devono essere analizzati e classificati dal punto di vista della probabilità di accadimento e del danno o impatto ipotizzabile al fine di decidere come gestirli; i rischi, inoltre, devono essere gestiti sia come rischi potenziali che come rischi effettivi;
- Risk Response: dopo aver classificato i rischi, devono essere decise le possibili azioni di contenimento o contrasto (evitare, accettare, ridurre o condividere il rischio) sulla base della tolleranza accettabile e della propensione al rischio dell'azienda;
- Control Activities: occorre stabilire e rendere pubbliche le opportune politiche e procedure per far si che il "risk response" sia effettivo;
- Information and Communication: le informazioni più importanti devono essere identificate, registrate e communicate nei modi e nei tempi necessari per rendere il personale cosciente e responsabile dei propri compiti;
- Monitoring: l'intero processo di ERM deve essere continuamente monitorato al fine di permettere, se necessario, di operare delle correzioni.

Rapporti fra gli obiettivi aziendali e le componenti

Vi è uno stretto rapporto fra gli obiettivi aziendali e le componenti ERM precedentemente indicate.
Tali rapporti possono essere evidenziati attraverso l'immagine tridimensionale di un cubo, ove le colonne verticali rappresentano le quattro categorie di obiettivi, le righe orizzontali rappresentano le otto componenti e la terza dimensione è rappresentata dall'organizzazione aziendale.

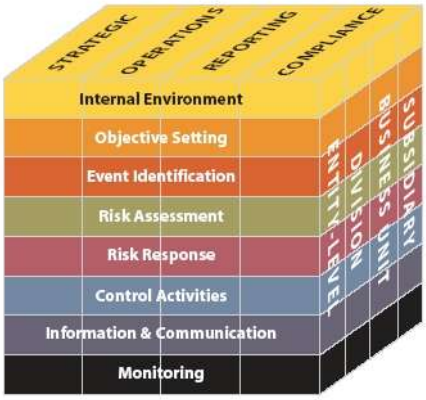

Figura fonte: COSO

ERM e controlli interni

Il sistema di controllo interno è una parte fondamentale dell'ERM; attraverso i controlli è infatti possibile gestire i rischi. I due più importanti framework di COSO, ERM e "Controlli interni" del 1992, sono dunque coerenti e compatibili.
Occorre chiarire, però, che secondo la *vision* di COSO, non basta un buon sistema di controlli interni per gestire i rischi aziendali: da questo punto di vista l'

Enterprise Risk Management è più ampio e include il sistema dei controlli interni.

Risk Assessment

La fase di risk assessment può utilizzare approcci di misurazione del rischio di tipo quantitativo o qualitativo.
Gli approcci di tipo quantitativo privilegiano indicatori per lo più di tipo economico, ad esempio i valori a bilancio dei beni analizzati; gli approcci di tipo qualitativo si basano sui molteplici fattori che potrebbero rappresentare un rischio aziendale (importanza per il business degli asset, requisiti normativi, problemi di immagine ed altro).
Per chi volesse approfondire l'argomento, consiglio la lettura di un interessante documento della *Research Foundation dell'Institute of Internal Auditors* sul Risk Assessment disponibile in:
http://www.theiia.org/iia/download.cfm?file=1778 (pdf, 214 k) che presenta e commenta alcuni casi di valutazione del rischio aziendale usando l'ERM (si riferisce alla versione 2002 dell'ERM).

Conclusioni

I cambiamenti prodotti dalle nuovi modelli di business e tecnologie richiedono nuovi approcci metodologici anche nel campo dell' enterprise risk management; sinteticamente si può dire che si passa concettualmente da un approccio basato sul *Risk Avoidance* (evitare, ridurre i rischi) ad un approccio basato sul *Continuous Risk Management* (gestire i rischi).
Ciò richiede di valutare l'esposizione al rischio mediante un periodico e rapido assessment che permetta di posizionare continuamente gli asset critici rispetto ai parametri di riferimento.
Il Rapid Risk Assessment deve garantire una serie di funzionalità, quali:

- strumenti per la *Risk Gap Analysis (As-Is versus To-Be)* al fine permette il confronto fra la propria esposizione al rischio (*As-Is*) rispetto ad un modello di riferimento (*To-Be*);
- strumenti per il *Tracking* al fine di evidenziare l'evoluzione nel tempo della esposizione al rischio indicando e quantificando i miglioramenti;
- strumenti di simulazione per permettere l'analisi *What-If*;
- strumenti di *Benchmarking* per confrontare la propria situazione rispetto ad aziende simili.

Risorse web:

Le faq di COSO su ERM 2004:
http://www.coso.org/Publications/ERM/erm_faq.htm
La precedente versione di ERM (2002):
http://www.erm.coso.org/Coso/coserm.nsf/vwWebResources/PDF_Manuscript/$file/COSO_Manuscript.pdf (pdf, 2,5 MB)

Agatino Grillo, CISA, CISSP, CISM. Lavora in OASI SpA. Ha pubblicato numerosi articoli e white paper sui temi dell' IS Auditing e della IT Security. Può essere contattato al seguente indirizzo: web@agatinogrillo.it

Ringraziamenti

Si ringraziano per aver collaborato a questo numero della newsletter:

- Boni Romano
- Carducci Giulio
- Cilli Claudio
- Corti Eugenio
- Di Stefano Gian Luca
- Fusaro Marco
- Giustozzi Corrado
- Grillo Agatino
- Minelle Federico
- Roncato Alessandro
- Spaziani Ugo

Information Systems Audit and Control Association®

A recognized global leader in IT governance, control and assurance