



Gli Standard ISACA e IIA per l'audit IT

di A. Rodaro

Recentemente è stato incluso nel *corpus* delle Guide Interpretative degli Standard IIA un insieme di documenti tratti direttamente dalle corrispondenti Guide dell'Associazione Mondiale degli Auditor Informatici, l'ISACA, che può vantare decenni di esperienza e leadership nel settore informatico.

L'introduzione di queste nuove Guide è un evento che va portato all'attenzione di tutti quei professionisti che possano essere coinvolti in interventi di audit con valenza informatica. Esse costituiscono pertanto un vademecum prezioso in tutte le fasi dell'audit, dalla pianificazione, alla esecuzione, all'evidenza nelle carte di lavoro, alla stesura del report, e forniscono elementi utili a massimizzare l'efficienza ed evitare errori di fondo, sempre possibili quando si affrontano argomenti che la letteratura presenta con un linguaggio spesso troppo tecnico.

Delle sette nuove Guide emesse cinque riguardano problematiche specifiche dell'audit informatico, le rimanenti trattano i CAAT (*Computer Assisted Audit Tools*) e il campionamento.

(>>>> articolo a pagina 2)



*Un sincero augurio per un sereno Natale e un anno ricco di soddisfazioni personali e professionali.
Il Consiglio Direttivo AIEA.*

In questo numero

Soddisfazioni per ISACA e per la comunità degli IS Auditor:

- alcune delle best practice promosse da ISACA sono state adottate dalla Associazione degli Internal Auditor (IIA),

- le certificazioni di ISACA, CISA e CISM, hanno ottenuto il riconoscimento dell'ANSI.

Con l'occasione ricordiamo che l'attività professionale dell'IS Auditor deve essere conforme agli standard pubblicati da ISACA e vi presentiamo l'esperienza di due professionisti che hanno conseguito la certificazione CISA e CISM nel corso del 2005.

Negli ultimi anni la normativa per la certificazione dei sistemi di gestione della sicurezza ha avuto continui aggiornamenti, è indispensabile mantenersi aggiornati, vi aiutiamo con un approfondimento su ISO 17799 e su ISO 27001.

Segnaliamo l'articolo sugli incidenti informatici e il riepilogo delle nostre Sessioni di Studio, occasioni di aggiornamento e scambio di conoscenze.

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



Sommario: numero 3 del 2005

La nuova serie di Guide Interpretative degli Standard IIA facilita l'audit IT <i>di A. Rodaro</i>	1 e 2
Evoluzione delle normative di riferimento della Information Security ed analisi delle principali novità introdotte <i>di C. Gallotti</i>	5
ISO17799:2005 ISO 27001:2005	5 9
Il ruolo dell'IS Auditor nella gestione degli incidenti informatici <i>di D. Forte</i>	11
CISA and CISM Certifications receive ANSI accreditation	13
Ho conseguito la certificazione CISM <i>di S. Bove</i>	14
Ho conseguito la certificazione CISA <i>di A. Pasquinucci</i>	17
Sessioni di Studio	20

Nel prossimo numero:
COBIT 4.0



La nuova serie di Guide Interpretative degli Standard IIA facilita l'audit IT

di Angelo Rodaro

Questo articolo è stato scritto dal Consigliere AIEA Angelo Rodaro e pubblicato su Italia Oggi.

Riteniamo sia particolarmente utile anche per i nostri associati e quindi lo riproporriamo, ringraziando: Angelo Rodaro, AIIA e Italia Oggi per la gentile concessione.

Le Guide Interpretative dell'Institute of Internal Auditors (IIA) sono documenti assai significativi, in quanto costituiscono indicazioni operative autorevoli, frutto della conoscenza ed esperienza di professionisti di internal auditing di tutto il mondo, e rappresentano uno strumento chiave ai fini della concreta applicazione degli Standard Internazionali della Professione. Come tali, la loro applicazione, pur non essendo obbligatoria, è fortemente consigliata.

Recentemente è stato incluso nel *corpus* delle Guide Interpretative un insieme di documenti tratti direttamente dalle corrispondenti Guide dell'Associazione Mondiale degli Auditor Informatici, l'ISACA, che può vantare decenni di esperienza e leadership nel settore informatico.

L'introduzione di queste nuove Guide è un evento che va portato all'attenzione di tutti quei professionisti che possano essere coinvolti in interventi di audit con valenza informatica. Esse costituiscono pertanto un vademecum prezioso in tutte le fasi dell'audit, dalla pianificazione, alla esecuzione, all'evidenza nelle carte di lavoro, alla stesura del report, e forniscono elementi utili a massimizzare l'efficienza ed evitare errori di fondo, sempre possibili quando si affrontano argomenti che la letteratura presenta con un linguaggio spesso troppo tecnico.

Un punto importante è quello riportato nell'introduzione di ciascuna guida: i suggerimenti in essa contenuti non intendono essere esaustivi di tutte le procedure necessarie per svolgere bene un incarico di audit, ma delineano piuttosto un nucleo di principi di responsabilità specifiche dell'auditor.

Delle sette nuove Guide emesse cinque riguardano problematiche specifiche dell'audit informatico, quali l'*outsourcing*, l'impatto di controlli IT pervasivi e di quelli attuati in autonomia da prestatori di servizi terzi, nonché la verifica delle applicazioni automatizzate. Le rimanenti trattano invece l'utilizzo di due tipologie di strumenti tecnici, i CAAT (*Computer Assisted Audit Tools*) e il campionamento, il cui interesse non si limita al campo informatico.

Le Guide si completano e integrano tra loro, nel senso che i contenuti di alcune di esse vengono spiegati od integrati dalle altre.

Vediamo ora brevemente il contenuto delle Guide e in che modo possono essere d'aiuto, a partire da quelle riguardanti gli strumenti tecnici, che per diversi aspetti sono quelle di uso più corrente.

Computer Assisted Audit Techniques - CAAT (Codice 1220-2)

Indica alcuni principi sulle possibilità d'uso, lo scopo, il modo di scegliere, di applicare e di valutare gli strumenti automatizzati di supporto all'audit. In particolare evidenzia le necessarie cautele da adottare. Fornisce regole per la documentazione del procedimento e delle evidenze di audit nelle carte di lavoro ed è completata da un piccolo glossario per facilitarne la comprensione oltre che il dialogo con i tecnici informatici.

(Continua a pagina 3)

Gli Standard IIA e l'audit IT

(Continua da pagina 2)

Campionamento dell'audit (Codice 2100-10)

Contiene alcune definizioni e concetti di base del campionamento. Riassume le classi e i tipi di campionamento, il concetto di popolazione e l'uso delle unità, i requisiti del campione e i rischi di campionamento. Tratta brevemente i principi da seguire nella valutazione, analisi e proiezione degli errori evidenziati sull'intera popolazione. E' utile ricordare che le principali applicazioni di audit per uso generalizzato (tra cui ACL) contengono funzioni apposite di supporto che facilitano molto e rendono immediato l'uso del campionamento, nel caso i dati sulla popolazione siano disponibili in forma automatizzata. La Guida individua quegli elementi e quei concetti di fondo che permettono di eseguire di persona i campionamenti ed estrarre i risultati, ma ricorda anche assai opportunamente che estrarre un campione appropriato è un'attività critica che può richiedere l'intervento di un esperto.

Outsourcing di attività informatiche ad altre organizzazioni (Codice 2100-12)

Tratta l'attualissimo e a volte scottante problema dell'auditing dei Sistemi Informatici in presenza di *outsourcing*; richiama le principali caratteristiche e i requisiti del contratto di servizio, come pure i tipi di verifiche da condurre sulle clausole contrattuali. Evidenzia l'importanza del diritto di audit e dei controlli interni del fornitore del servizio e stabilisce un criterio base: l'intervento deve essere condotto come se il servizio informatico non fosse fornito da terzi, ma da un Servizio interno all'organizzazione. Chiarisce alcuni principi di condivisione dei risultati di audit, da seguire nella discussione e nella distribuzione del rapporto.

Effetto dell'attività di terzi sui controlli IT dell'organizzazione (Codice 2100-13)

Cataloga le varie tipologie di servizio IT reso da prestatori esterni e, in presenza di punti deboli nei controlli informatici, tratta brevemente le possibili cause / ripercussioni rilevanti per il controllo interno. La Guida inoltre stabilisce principi in tema di *Governance* e di come valutare il peso relativo dei controlli IT ad opera di interni e di esterni ("Quanto sono o dovrebbero essere importanti per noi i controlli IT dei prestatori di servizio esterni? Come va ricostruito il mosaico dei nostri e dei loro controlli?"). Infine la Guida tocca altri temi critici, come le relazioni con le strutture di controllo interno del fornitore e la presenza di sub-fornitori.

Effetto dei controlli pervasivi sui sistemi informativi (Codice 2100-11)

Differenziando i controlli informatici "pervasivi" da quelli specifici, la Guida stabilisce una gerarchia dei controlli stessi in modo da facilitare la valutazione della loro portata ed efficacia ("Questo controllo non funziona bene: ciò è grave oppure no?"). La Guida introduce l'utilizzo della Metodologia CobIT ("*Control Objectives for Information and related Technology*") per il ciclo di vita delle applicazioni informatiche. Il CobIT include aspetti informatici e di *best practice*, introduce metriche utili alla valutazione comparativa della situazione rilevata, ma è anche costruito per "ritagliare" nel modo più appropriato il programma di audit, in funzione degli obiettivi e dell'ambito prescelto.

Verifica dei sistemi applicativi (Codice 2100-9)

Individua le tipologie di rischio legate all'uso di applicazioni informatiche, nonché i momenti critici della vita delle applicazioni, durante i quali è opportuno eseguire le valutazioni; definisce inoltre alcune regole da seguire nelle verifiche.

(Continua a pagina 4)



Gli Standard IIA e l'audit IT

(Continua da pagina 3)

Requisiti delle evidenze di audit (Codice 2100-14)

Elenca le varie tipologie di "evidenza" in ambito di audit informatico, indica alcuni principi e dà esempi su come scegliere il tipo di evidenza da utilizzare e su come documentare queste evidenze. I requisiti di materialità e rilevanza sono così anche proiettati nell'ambito informatico.

L'auditor che utilizzi queste Guide deve comunque essere cauto. Alcune delle attività elencate e la parte preponderante dei giudizi di adeguatezza non possono prescindere da un nucleo adeguato di conoscenze informatiche, che d'altro canto devono fare sempre più parte integrante del nostro bagaglio professionale standard. Un po' come un ciclista che deve orientarsi sulla cartina che gli indica il percorso da seguire: per leggere la carta deve saper interpretare correttamente i simboli, e deve saper collegare i luoghi reali ai simboli.

Un ultimo punto importante: la formulazione sintetica delle Guide si adatta particolarmente ad un impiego pratico per finalità di supervisione degli interventi di audit. Pertanto esse costituiscono un indispensabile strumento per gli audit manager nelle attività di controllo sulla completezza e qualità degli interventi di audit in ambito informatico.

Angelo Rodaro, Consigliere AIEA
Responsabile IS Auditing—Edison SpA

Notizie AIEA - Notizie AIEA
Notizie AIEA - Notizie AIEA

Il 10 e 11 novembre 2005 si è svolto il corso di preparazione alla sessione di esame CISA di dicembre.

Il 27 e 28 ottobre 2005 si è svolto il corso di preparazione alla sessione di esame

Notizie ISACA - Notizie ISACA
Notizie ISACA - Notizie ISACA

ISACA Cosponsor del Computer Security Day

ISACA è lo sponsor principale del 18° Computer Security Day organizzato dalla Association for Computer Security Day (ACSD). L'evento si è svolto il 30 novembre 2005 e sono intervenuti partecipanti provenienti da più di 50 Paesi. Ulteriori informazioni, tra cui come richiedere il poster gratuito della manifestazione, sono disponibili all'indirizzo www.computersecurityday.org.

***Evoluzione
delle normative di riferimento
della Information Security
ed analisi delle principali
novità introdotte***

di Cesare Gallotti

**Dalle BS 7799-2:2002 e ISO 17799:2005
alle ISO 17799:2005 e ISO 27001:2005**

Il 15 giugno e il 15 ottobre 2005 sono state emesse rispettivamente la nuova versione dell'ISO 17799, che sostituisce quella del 2000, e la norma ISO 27001:2005, che sostituirà la BS 7799-2:2002. In seguito saranno stabilite le regole di transizione dalla BS 7799-2:2002 all'ISO 27001:2005.

L'ISO 17799 è una *linea guida* o "*code of practice*" (usa il verbo "should") che presenta in modo approfondito alcune misure per garantire la sicurezza delle informazioni. L'ISO 27001:2005 è, invece, la "*specific*" (usa il verbo "shall") ovvero lo standard di riferimento per le certificazioni dei Sistemi di Gestione per la Sicurezza delle Informazioni.

Le due norme sono correlate e infatti la norma 27001 riporta, nell'Allegato A, i *controlli* indicati nell'ISO 17799:2005 e che dovranno essere utilizzati nello Statement of Applicability per descrivere le decisioni prese in merito al trattamento del rischio.

Per il 2006 è prevista la rinumerazione dell'ISO 17799:2005 in ISO 27002:2006 e verrà emessa l'ISO 27000 dedicata a "Terminologia e definizioni", seguendo così il modello già usato per le norme della serie ISO 9000 e ISO 14000.

Nel futuro si prevede l'emissione di nuove norme della serie 27000, dedicate alla gestione dei rischi, alle metriche e misurazioni dei processi di un Sistema di Gestione per la Sicurezza delle Informazioni, oltre a una guida per la loro implementazione.

Analisi dell'ISO 17799:2005

La nuova norma ISO 17799:2005 presenta una breve descrizione per ciascuna misura proposta, detta *controllo* di sicurezza, seguita da una descrizione più approfondita (*Implementation Guidance*) e da eventuali ulteriori considerazioni, riferimenti ad altri standard o richiami a possibili aspetti legali (nel paragrafo *Other information*).

(Continua a pagina 6)



Normative della Information Security: ISO 17799:2005 e ISO 27001:2005

(Continua da pagina 5)

La precedente versione della ISO 17799:2000 indicava come "controllo" sia la breve descrizione che la Implementation Guidance, lasciando agli estensori della BS 7799-2:2002 il compito di redigere una sintesi da riportare nell'Allegato A. In questo modo alcune misure importanti (come, per esempio, la definizione di *Ownership of assets*), non erano riportate per quelli che potremmo definire *errori di sintesi*.

I controlli attualmente proposti sono 134, contro i 127 precedenti. Molti sono stati riformulati per aggiornare della terminologia, renderla omogenea e per garantire la completezza delle descrizioni. Altri controlli sono stati aggiunti per evitare *errori di sintesi*.

Non sono da segnalare modifiche tali da compromettere il lavoro svolto sin qui dalle aziende che hanno redatto uno Statement of Applicability conforme al BS 7799-2:2002, a parte la nuova numerazione e la maggiore attenzione ad alcuni argomenti, come verrà analizzato di seguito.

I capitoli iniziali ricalcano quanto già previsto dalla norma del 2000, con un'estensione del secondo capitolo dedicato alle definizioni, l'aggiunta di un breve capitolo (il quarto) dedicato alla valutazione e trattamento del rischio e uno (il terzo) di descrizione della struttura dello standard.

Agli *starting point* già proposti dall'ISO 17799:2000 ne viene aggiunto uno riguardante la correttezza di esecuzione delle applicazioni.

Per la successiva analisi, i capitoli saranno presentati secondo l'ordine della versione del 2000. Questo per facilitare chi ha lavorato sino ad oggi con questa.

Quasi tutti i titoli e descrizioni dei controlli sono stati modificati. Saranno di seguito segnalate le sole modifiche di rilievo agli scopi di questo articolo.

3 Security Policy

Una maggiore attenzione viene posta alle terze parti: l'ISO 17799:2005 richiede di comunicare la politica di sicurezza, oltre che al personale interno, anche alle "entità esterne rilevanti".

Questo aspetto era già presente nella norma del 2000, ma poco evidenziato dalla BS 7799-2:2002. La nuova organizzazione dei controlli e le relative descrizioni (anche se non saranno segnalate nel prosieguo dell'articolo) sottolineano questo argomento talmente importante da non richiedere ulteriori commenti.

4 Organizational Security

Al primo controllo è presente una novità: viene eliminato il "Security forum", entità organizzativa amatissima da quanti sino ad oggi si sono occupati di sicurezza delle informazioni.

Le responsabilità gestionali sono ora date alla Direzione Aziendale, uniformemente a quanto già previsto dalle attuali versioni di standard come l'ISO 9001 e l'ISO 14000. Il Security Forum veniva delegato dalla Direzione per fornire supporto alle attività di sicurezza, definire la politica di sicurezza e approvare gli investimenti di maggior portata: attività ora di competenza della stessa Direzione.

Viene comunque lasciata la possibilità di costituire un gruppo con competenze più specifiche e mag-

(Continua a pagina 7)

Normative della Information Security: ISO 17799:2005 e ISO 27001:2005

(Continua da pagina 6)

giore orientamento verso le tematiche di sicurezza.

Il controllo sugli accordi di riservatezza (6.1.3, per la ISO 17799:2000) non è più collocato nel capitolo dedicato alla gestione del personale, ma in questo sull'organizzazione della sicurezza perché riconducibile anche alla gestione delle "terze parti".

I controlli 4.1.5 e 4.1.6 della versione del 2000, ora numerati come 6.1.7 e 6.1.6, relativi al supporto di specialisti esterni e all'attivazione di contatti con altre organizzazioni, sono stati modificati e resi più chiari.

I controlli successivi, a cui è dedicata la Sezione 6.2, sono relativi alla gestione delle terze parti e sono stati riorganizzati. Viene chiarito meglio il concetto di outsourcing e le sue differenze rispetto ad altre tipologie di rapporti con terzi. Per questo motivo non è possibile trovare un corrispondente diretto del controllo 4.3.1 della precedente versione dell'ISO 17799.

Il nuovo controllo 6.2.2 esplicita la necessità di considerare, tra le terze parti, non solo i fornitori, ma anche i clienti.

5 Asset classification and control

Questo capitolo è stato rinominato "Asset management" e ha due controlli in più.

Il nuovo controllo 7.1.2 è dedicato alla "proprietà" degli asset (*Ownership of assets*). Tale argomento, benché presente nel controllo 4.1.3 dell'ISO 17799:2000, non era riportato nella BS 7799-2:2002 per *errore di sintesi*.

6 Personnel Security

La nuova norma dedica 3 nuovi controlli (8.3.1, 8.3.2, 8.3.3) alla gestione del personale interno o esterno in occasione della fine del rapporto con un'organizzazione. Queste misure, per *errori di sintesi*, non sono richiamate dall'Allegato A della BS 7799-2:2002.

Viene anche aggiunta la nuova misura 8.2.1, in cui viene specificato che è responsabilità della Direzione comunicare al personale, sia interno che esterno, l'obbligo di applicazione delle politiche e procedure di sicurezza.

Gestione degli incidenti

Le misure della ISO 17799:2000 da 6.3.1 a 6.3.4 riguardano la gestione degli incidenti, a cui la nuova norma del 2005 dedica un capitolo in più: il 13.

Per *errore di sintesi*, i controlli dell'Allegato A della BS 7799-2:2002 richiedevano di segnalare e analizzare gli incidenti, ma non contemplavano la gestione degli stessi. Una parziale eccezione a ciò è rappresentata dal controllo 8.1.3, limitato però ai soli incidenti informatici. Il controllo 13.2.1 della nuova norma richiede la gestione degli incidenti per tutti gli ambienti.

(Continua a pagina 8)



Normative della Information Security: ISO 17799:2005 e ISO 27001:2005

(Continua da pagina 7)

Il controllo della vecchia norma 6.3.3 sulle vulnerabilità software è collocato nel capitolo dedicato allo sviluppo e gestione dei sistemi.

Il controllo relativo alla raccolta di prove a scopi legali, precedentemente collocato nel capitolo "Compliance", è stato ora più propriamente accorpato agli altri controlli di gestione degli incidenti.

7 Physical and environmental security

Si segnala l'aggiunta del controllo 9.1.4, che specifica meglio le misure da intraprendere contro le minacce ambientali, non riportate dall'Allegato A della BS 7799-2:2002 per *errore di sintesi*.

Il controllo 7.2.2, precedentemente dedicato alla protezione delle infrastrutture di erogazione di energia, è stato esteso a tutte le infrastrutture

Il controllo sulla Clear Desk Policy è stato ricollocato tra le "User responsibilities".

8 Communication and operations management

Per la nuova norma del 2005 sono stati ampiamente riscritti e aggiornati i controlli del 2000. In particolare, si nota una maggiore attenzione agli strumenti informatici esterni all'azienda, alle terze parti, al commercio elettronico (a cui è stata dedicata la nuova sezione 10.9) e all'evoluzione degli strumenti di automazione per l'ufficio.

E' stato aggiunto il controllo 10.8.1 relativo allo scambio di informazioni, mentre è interessante la riformulazione del vecchio controllo 8.7.7 sulla posta elettronica, che viene ora fatta rientrare come caso particolare di "Electronic messaging".

Una nuova sezione 10.10 è stata dedicata al monitoraggio dei sistemi (logging e auditing), raggruppando ed estendendo alcuni controlli precedentemente dedicati al solo monitoraggio dei sistemi o degli accessi. Alla protezione dei log, considerata precedentemente come caso particolare di sicurezza dei record aziendali, è ora dedicato il controllo 10.10.3.

9 Access Control

Le misure di controllo degli accessi sono in larga parte rimaste invariate o adeguate alle nuove tecnologie.

L'aggiornamento consiste nell'ammodernamento del linguaggio e nell'eliminazione di controlli specifici del solo mondo mainframe.

Sono stati eliminati i controlli 9.4.2 sull'*enforced path* (raramente applicato e meglio espresso come caso particolare di controllo delle trasmissioni), 9.5.1 sull'autenticazione automatica dei terminali (più specifico per ambienti mainframe e ora caso particolare della 11.6.1), 9.5.6 sulla segnalazione automatica di transazioni effettuate sotto coercizione (ora caso particolare di segnalazione di incidenti).

(Continua a pagina 9)

Normative della Information Security: ISO 17799:2005 e ISO 27001:2005

(Continua da pagina 8)

10 System development and maintenance

In questo capitolo i controlli dedicati alla crittografia (quelli della sezione 10.3 della ISO 17799:2000) sono passati da cinque a due. Nella nuova versione, la crittografia è da intendersi più come tecnologia particolare che come controllo a sé stante. Rimangono i due controlli relativi alle politiche e alla gestione delle chiavi crittografiche.

Il vecchio controllo 10.2.3 è stato riformulato considerando l'autenticazione delle trasmissioni come caso particolare di integrità. I restanti controlli sono stati resi più chiari e aggiornati.

11 Business continuity management

Capitolo largamente rimasto invariato. Da segnalare solo qualche aggiunta e precisazione.

12 Compliance

Anche questo Capitolo non ha subito variazioni di rilievo se non qualche aggiunta e precisazione.

Analisi della ISO 27001

La 27001:2005 riprende in larga parte la BS 7799-2:2002.

In particolare, i requisiti per la valutazione di un ISMS sono descritti nei primi capitoli da 4 a 8 (un capitolo è stato aggiunto perché il punto 6.4 è diventato il capitolo 6) e nell'Allegato A che riporta i controlli della ISO 17799:2005.

Tra le cose rilevanti si segnalano:

La descrizione dello Statement of Applicability: viene detto che il SoA "deve fornire un riassunto delle decisioni relative al trattamento del rischio" e viene anche richiesto di "dimostrare, per ciascun controllo, la sua relazione con i risultati del risk assessment e del risk treatment, con la politica e con gli obiettivi"; questo documento, quindi, non dovrà più riportare solo riferimenti a procedure o documenti di descrizione in dettaglio del controllo, ma anche una descrizione dei rischi che va a contrastare;

Misurazione dell'efficacia dei controlli di sicurezza: In più punti si fa riferimento alla richiesta di misurare l'efficacia dei controlli o di gruppi di controlli. Questo aspetto è sicuramente quello che rappresenta la maggiore innovazione della nuova norma e il maggiore impegno per chi implementa un ISMS. In particolare si potrà fare riferimento alla disponibilità dei sistemi e a statistiche sugli incidenti rilevati e gestiti, ma altri indicatori dovranno essere individuati dalle singole aziende sulla base dei dati e dei sistemi di monitoraggio che hanno a disposizione o compatibili con quelli già esistenti.

(Continua a pagina 10)



Normative della Information Security: ISO 17799:2005 e ISO 27001:2005

(Continua da pagina 9)

Come elementi di minor rilievo si segnalano:

- * viene esplicitato che la metodologia di valutazione del rischio deve garantire risultati comparabili e riproducibili, ossia che i risultati di valutazioni del rischio in momenti diversi dell'azienda diano evidenza delle modificazioni eventualmente avvenute, e che la stessa metodologia applicata in condizioni simili dia gli stessi risultati
- * viene esplicitata la necessità di rivedere periodicamente il risk assessment, mentre prima si chiedeva di rivedere il solo rischio accettabile
- * viene esplicitamente richiesto un documento che descriva la metodologia di risk assessment.

Purtroppo i capitoli non sono allineati con l'ISO 9001:2000, e questo può rendere l'integrazione dei sistemi di gestione più laborioso di quanto auspicato.

Conclusioni

Le nuove ISO 17799:2005 e ISO 27001:2005 risultano essere più vicine alle esigenze del mercato e degli utilizzatori, grazie ai controlli più dettagliati, alla loro organizzazione più coerente e al loro aggiornamento.

Sicuramente, anche a fronte della richiesta di misurazione dell'efficacia dei controlli, la norma non perde la sua caratteristica di essere applicabile in tutte le realtà e sarà compito di ciascuna azienda individuare le modalità più adeguate per avere a disposizione dati utili al miglioramento continuo.

Queste norme, poi, dimostrano sempre più di migliorarsi tenendo conto dell'esperienza di quanti ne hanno utilizzato le precedenti versioni, in modo da renderle sempre più punto di riferimento per coloro che si occupano di sicurezza delle informazioni e dei sistemi di gestione ad essa dedicati.

Cesare Gallotti, CISA, è Lead Auditor BS 7799-2 e ISO 9001 presso Det Norske Veritas (www.dnv.it).

È autore del libro *Sicurezza delle Informazioni - Analisi e gestione del rischio* (ed. Franco Angeli, 2003).

Si ringrazia DNV Italia per l'autorizzazione alla pubblicazione.

Il ruolo dell'IS Auditor nella gestione degli incidenti informatici

di Dario Forte



In tutte le strutture ove sia presente questa funzione, l'IS auditor ha un ruolo sempre più importante nell'incident management.

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

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

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

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

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

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

Il ruolo dell'IS auditor

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

- Preparazione agli incidenti: A prescindere dal ruolo ovvio di ownership ricoperto, nella fase di esercizio e in quella operativa, dalla funzione sicurezza (inclusa quella informatica), l'Audit viene di solito chiamato a

(Continua a pagina 12)



Il ruolo dell'IS Auditor nella gestione degli incidenti informatici

(Continua da pagina 11)

discutere l'incidenza delle politiche e delle procedure di gestione dell'incidente nei confronti del Top Management e della Polizia/autorità Giudiziaria. Può, in alcuni casi estremi, avere potere di veto (succede soprattutto nell'ambiente finance) ed è un anello infungibile nella catena di gestione.

- **Notifica:** a seconda delle procedure che sono state stabilite nella fase di cui al punto precedente, l'Audit riceve (anche in cc) una comunicazione dell'avvenuto incidente. Con notifica, in questo caso, alcuni intendono anche l'avvenuta notifica, da parte dell'Autorità Giudiziaria, di un qualsivoglia Decreto, per l'acquisizione di eventuali log e/o ulteriori informazioni eventualmente disponibili.
- **PostMortem/Digital Forensic.** Come più volte chiarito in letteratura, la produzione di potenziali fonti di prova deve seguire determinati criteri tecnico/legali. Per esperienza personale mi capita sempre più spesso di assistere all'intervento diretto degli IS auditor in attività di Digital Investigation correlate a violazioni di tipo interno (per esempio causate da impiegati infedeli). Alcuni IS auditor (esperienza diretta su cliente inglese operante in Italia), inoltre, operano congiuntamente all'IT security al fine di reperire eventuali falle replicate sui sistemi e porvi rimedio.
- **Reportistica e Lessons Learned.** L'audit, per definizione, ha una linea diretta con il Top Management. E' quindi evidente come, in molti casi, sia questa categoria di operatori a dover stilare il rapporto finale relativo all'incidente, ferma restando l'infungibile attività dell'IT security.

I problemi di tutti i giorni

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

Le soluzioni e le sfide del futuro

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

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

Dario Forte, CISM, CFE, dopo un lungo trascorso nelle Forze di Polizia ha fondato DFLabs (www.dflabs.com). Docente di Gestione degli Incidenti Informatici all'Università di Milano. E' socio AIEA.

CISA and CISM Certifications Receive ANSI Accreditation

Comunicato ISACA

ISACA is extremely proud that the American National Standards Institute (ANSI) has accredited the CISA and CISM certifications under ISO/IEC 17024:2003, General Requirements for Bodies Operating Certification Systems of Persons. ANSI, a private, nonprofit organization, accredits other organizations to serve as third-party product, system and personnel certifiers.

ISO/IEC 17024 specifies the requirements to be followed by organizations certifying individual against specific requirements. ANSI describes ISO/IEC 17024 as "expected to play a prominent role in facilitating global standardization of the certification community, increasing mobility among countries, enhancing public safety, and protecting consumers."

ANSI's accreditation:

- Promotes the unique qualifications and expertise ISACA's certifications provide
- Protects the integrity of the certifications and provides legal defensibility
- Enhances consumer and public confidence in the certifications and the people who hold them
- Facilitates mobility across borders or industries

Accreditation by ANSI signifies that ISACA's procedures meet ANSI's essential requirements for openness, balance, consensus and due process in accordance with the ISO 17024 standard. To maintain ANSI accreditation, certification bodies such as ISACA are required to consistently adhere to a set of requirements or procedures related to quality, openness and due process.

With this accreditation, ISACA anticipates that significant opportunities for CISAs and CISM's will continue to open in the US and around the world. The accreditation is both an international and US accreditation: it is based on an international standard but implemented by ANSI to be recognized in the US and by other countries that enter into an arrangement with ANSI. This is in keeping with the purpose of 17024: to begin standardization of accreditation of personnel certification agencies around the world.

ISACA NEW LOGO AND NEW TAGLINE

Comunicato ISACA

To convey its broadened scope of professional expertise, the Information Systems Audit and Control Association will use only its acronym—ISACA—after 1 January 2006. The association has also adopted a new tagline to further define and explain its acronym: ISACA: Serving IT Governance Professionals.

"ISACA is changing its logo to reflect the expanded professional niche we serve. We have seen an increasing number of information security professionals in our membership, and we are committed to providing pertinent programming and research to our constituents," said Everett Johnson, CPA, international president of ISACA. "In addition, we find that our members are eager for information on IT governance, privacy, control, risk management, and the entire gamut of IT control and governance-related activities."

ISACA remains committed to serving the fields of assurance and control, which, along with information security, are included under the broader, encompassing umbrella of IT governance.

"We realized that all of the professions we serve fall under the IT governance banner," said Johnson. "Each one of those professions has an important role to play in ensuring that organizations exercise effective governance."



Ho conseguito la certificazione CISM

di Stefania Bove

Un importante riconoscimento approda in una Pubblica Amministrazione Italiana: dopo aver trapiantato il CIA e il CISA, si supera l'esame di certificazione CISM

Sul numero di Settembre 2003 di InfoAIEA, veniva pubblicata una breve recensione su un Convegno organizzato dagli organismi pagatori della Regione Toscana e del Veneto, dal titolo: "E-government per lo sviluppo dei servizi amministrativi nel settore dei finanziamenti in agricoltura-Auditing e sicurezza informatica degli organismi pagatori regionali", molto è cominciato in quella occasione.

A quel convegno, infatti, partecipavo anch'io per raccontare l'esperienza maturata da ARTEA ⁽¹⁾ nel settore. Dopo aver rivisto i rapporti di audit eseguiti, riguardate le normative specifiche di settore, trascorso i fine settimana a cercare su Internet le "best practices", sono arrivata per caso sul sito dell'ISACA.

Ho scaricato COBIT e letto di filato tutti i volumi pubblicati gratuitamente: poteva essere uno standard che ben si adattava alla realtà della nostra organizzazione, quella di una agenzia di nuova istituzione che stava avviando il servizio di controllo interno, prestando particolare attenzione alla sicurezza informatica. Il supporto del Responsabile del Servizio e della Direzione è presto trovato: si decide di procedere.

Tra i relatori al convegno, a nome dell'AIEA, interveniva il Consigliere Orillo Narduzzo, esperto di COBIT...era il 12/06/2003⁽²⁾. E' così che ho conosciuto l'AIEA, ed è lì che ho sentito per la prima volta nominare le certificazioni internazionali CISA e CISM. Vi confesso che quei titoli mi hanno fatto, ed ancora mi fanno, "impressione" ma potevano rappresentare un segnale forte, un modo per dimostrare che anche nelle pubbliche amministrazioni si stava sviluppando un serio interesse nei confronti dell'auditing e della sicurezza informatica.

Trovati gli spunti, bisognava rimboccarsi le maniche e lavorare.

Quanti sacrifici fatti per superare in due anni gli esami CIA (Certified Internal Auditor), CISA (Certified Information Systems Auditor) e CISM (Certified Information Security Manager)? Tanti.

Un ricordo significativo? mio figlio Antonio, tre anni, che chiede <<Mamma, che fai dormi? Mamma, dormi, dormi ??...>> svegliandomi scuotendo il letto con salti energici a mo' di Tigro, dopo una notte passata a studiare.

Ho dovuto sfruttare tutti i momenti possibili per ritagliare il tempo per prepararmi: la notte, i viaggi in treno, i fine settimana ed anche le ore trascorse sulla spiaggia, sotto l'ombrellone: per la gioia di tutti la prima borsa che preparavo prima della partenza conteneva i testi dell'ISACA.

Eppure ancora oggi ho lo stesso entusiasmo e lo stesso desiderio di apprendere e di cogliere de-

(Continua a pagina 15)

Ho conseguito la certificazione CISM

(Continua da pagina 14)

gli spunti da introdurre nella quotidiana attività lavorativa, già perché il fine ultimo non era l'ottenimento delle certificazioni, una meta sicuramente ambita, ma "crescere" professionalmente e far sviluppare l'organizzazione.

Energia ed entusiasmo riscontrati anche nelle persone che mi hanno circondato, che mi hanno aiutato con consigli ed incoraggiamenti: la famiglia, l'organizzazione, i colleghi d'ufficio el'AIEA.

Cos'è l'esame CISM? Un esame che certifica la professionalità acquisita in qualità di responsabile della sicurezza informatica. Quattro ore di lavoro in totale concentrazione, 200 domande impegnative racchiuse in un "book" pieno di simulazioni, emblema di ciò che credo la professione possa riservare; in sintesi quello che può scaturire dalla fervida immaginazione e dalla esperienza di un team internazionale di esperti.

Un grosso handicap nell'affrontare l'esame è stato, come previsto, la mancanza di esperienza in qualità di responsabile della sicurezza informatica e solo una grande determinazione supportata da un' idonea preparazione teorica mi hanno aiutato a superare una prova mirata a premiare l'esperienza acquisita sul campo.

Mentre sostenevo l'esame qualche volta mi sono fermata ed ho pensato: "vorrei avere maggiore esperienza per poter rispondere con più sicurezza a questa domanda", ma il tempo era poco anche per fare queste digressioni!

La sera del 28 luglio ero piuttosto inquieta, l'organizzazione mi aveva appena fornito, tramite VPN, l'accesso da remoto alla LAN aziendale e volevo eseguire dei test... effettuo il log-in al sito personale dell'ISACA (my ISACA) dopo circa 20 giorni dall'ultimo accesso e, meraviglia delle meraviglie, scopro che avevano pubblicato i risultati: ce l'avevo fatta!!!

Ci tengo a rivolgere pubblicamente i ringraziamenti all'AIEA, che spero possa trovare nelle pubbliche amministrazioni un ambito di crescita. Ringrazio in particolare il Presidente Silvano Ongetta che mi ha dato la possibilità di raccontarvi questa esperienza ed il Consigliere Angelo Rodaro, che ha organizzato in modo eccezionale il corso di preparazione all'esame: grazie per il supporto e l'incoraggiamento fornito fino ad un minuto prima dell'esame.

Ringrazio i docenti del corso di preparazione all'esame che mi hanno aiutato a superare la prova, mostrando grande professionalità, preparazione specifica ed hanno condiviso la loro personale esperienza lavorativa.

Ringrazio ancora l'amministrazione, ed in particolare il Direttore dell'Agenzia Giuseppe Cortese, che ha da sempre sostenuto l'attività di Auditing, incoraggiando i progressi ed i progetti formativi del personale del Servizio di Controllo Interno.

Ringrazio infine mio marito, per tutta la comprensione manifestata e mio figlio che dopo aver ascoltato questa storia ha esclamato: "sei tu? ...tutta tu?...un pochino anche io!".

(Continua a pagina 16)



Ho conseguito la certificazione CISM

(Continua da pagina 15)

(1) ARTEA

ARTEA (Agenzia Regionale Toscana Erogazioni Agricoltura) è l'organismo pagatore della Regione Toscana istituito con legge regionale n.60/99. Svolge le funzioni di autorizzazione, esecuzione e rendicontazione dei pagamenti di aiuti, contributi e premi previsti da disposizioni comunitarie, nazionali e regionali nel settore dell' Agricoltura www.artea.toscana.it.

(2) Il Regolamento (CE) numero 465/05 e COBIT

Con il Regolamento (CE) numero 465/05 è stato modificato il Regolamento CE numero 1663/95, includendo tra gli standard internazionali cui fare riferimento per la sicurezza dei sistemi d'informazione COBIT:

“la sicurezza dei sistemi d'informazione si basa su criteri definiti in una versione applicabile, nell'esercizio finanziario di cui trattasi, di una delle seguenti norme internazionalmente riconosciute:

- norma ISO 17799 dell'Organizzazione internazionale per la standardizzazione/norma britannica 7799: Code of Practice for Information Security Management (BS ISO/IEC 17799),
- Bundesamt für Sicherheit in der Informationstechnik (Ufficio federale per la sicurezza delle tecniche dell'informazione): IT Grundschutzhandbuch/IT manuale di sicurezza informatica di base (BSI),
- Information Systems Audit and Control Foundation: Control Objectives for Information and related Technology - COBIT (obiettivi di controllo nel campo dell'informazione e delle tecnologie correlate).

L'organismo pagatore sceglie una delle norme internazionali di cui al primo comma quale base della sicurezza dei propri sistemi d'informazione.

Occorre che le misure di sicurezza siano adeguate alla struttura amministrativa, al personale e all'ambiente tecnologico di ciascun organismo pagatore. Lo sforzo finanziario e tecnologico deve inoltre essere proporzionale ai rischi effettivi”.

Stefania Bove, CIA, CISA, CISM è Auditor presso ARTEA Toscana.

Ho conseguito la certificazione CISA

di Andrea Pasquinucci



Il nostro Presidente mi ha chiesto di raccontarvi le mie personali impressioni sul corso e l'esame CISA 2005. Vi dico subito che alla fine ho passato l'esame e quindi spero tra poco di poter ottenere la certificazione CISA. Ma prima di fare qualche commento sull'esame è meglio che riparta dall'inizio.

Prima di tutto, la mia principale attività non è quella di IS Auditor, io mi occupo di sicurezza informatica come libero professionista. Nel mio lavoro però mi capita di partecipare a Audit informatici oppure di svolgere in prima persona delle *valutazioni* di sistemi informatici per piccole e medie aziende che altro non sono se non piccoli IS Audit. Visto che la mia formazione nel campo dell'Audit non era completa, il corso CISA mi è interessato molto per dare un inquadramento generale alla mia attività come Auditor, ovvero tappare tutti i buchi e fornirmi una base generale solida. A differenza della maggior parte di coloro che hanno seguito il corso, Auditor di professione, il mio interesse era quindi prima nel corso e poi nella certificazione.

Devo subito dire che il corso mi ha soddisfatto, fornendomi le informazioni e quel panorama sull'attività di Audit che mi mancavano. La collocazione delle lezioni nelle giornate di venerdì e sabato per me è risultata ottima, anche se all'inizio temevo di perdere alcuni venerdì, alla fine sono riuscito a seguire tutte le lezioni.

Per quanto riguarda le lezioni, personalmente ritengo che il modo migliore per affrontarle sia quello di prima leggersi il capitolo nel manuale, e poi seguire la lezione. (Sarebbe utile quindi che il manuale arrivasse prima dell'inizio delle lezioni, cosa che non è capitata per problemi tra corriere e dogana, da quel che abbiamo capito.) Purtroppo non sono riuscito a farlo se non per un paio di capitoli/lezioni, ovviamente perché non è facile leggersi un centinaio o più di pagine nel corso di una settimana lavorativa. Trovare il tempo per studiare mentre si lavora non è mai facile, neppure di sera perché si è stanchi e si preferirebbe giustamente fare qualche cosa di più rilassante. I momenti per me più interessanti delle lezioni sono state le discussioni aperte con i docenti, gli esempi teorici o veramente vissuti, insomma tutte le discussioni che ci coinvolgevano in prima persona. Personalmente suggerirei ai docenti di cercare di limitare le presentazioni di infinite slide con elencazioni di casi e classificazioni, tanto ci sono sul manuale, cercando invece di ampliare per quanto possibile gli esempi ed i casi da discutere insieme. Ho trovato che questi momenti erano quelli più istruttivi, nei quali sono riuscito a capire la logica di certe affermazioni, procedimenti o punti di vista. E' stato anche molto utile il confronto fra le esperienze diverse dei partecipanti al corso, tra gli Auditor interni ed esterni e quelli, come me, provenienti da campi diversi. Questo è stato possibile grazie anche al fatto che si è formato un bel gruppo tra noi studenti, e l'atmosfera in aula è sempre stata molto positiva.

Devo ovviamente fare anche un commento sul manuale. E' onnicomprensivo, c'è di tutto e di più. E' ovviamente scritto a molte mani, con ripetizioni, contraddizioni, balzi in avanti e refusi del passato. In altre parole è una specie di Bibbia, difficile da navigare ma nella quale c'è tutto quello di cui si ha bisogno, alle volte formulato in modo chiaro, altre volte un po' meno ed altre in modo del tutto confuso. Malgrado tutto ciò, devo dire che vi ho trovato molte informazioni utili ed interessanti, ovvero il manuale mi è servito per imparare, cosa che non posso dire di alcuni manuali di altri corsi/certificazioni che ho fatto.

(Continua a pagina 18)



Ho conseguito la certificazione CISA

(Continua da pagina 17)

Arrivo finalmente all'esame. Premetto che ho un po' di esperienza in esami e certificazioni informatiche, con domande multiple-choice (una risposta scelta fra quattro date) eccetera. Il primo problema che mi si è posto è stato quello della lingua: fare l'esame in inglese o italiano? Benché abbia fatto tutti i miei altri esami per certificazioni in inglese, questa volta ho scelto italiano. Ho fatto questa scelta prima ancora dell'inizio del corso e basandomi fondamentalmente sul fatto che sia il corso che il manuale sarebbero stati in italiano. Ovviamente i rischi erano di trovare domande tradotte in modo errato, o che la traduzione avrebbe reso incomprensibili domande a trabocchetto, quelle in cui una sola parolina quasi nascosta cambia il significato della domanda stessa.

D'altra parte, il fatto peculiare dell'esame CISA è di concedere in media solo poco più di un minuto per rispondere ad ogni domanda, e benché il mio inglese non sia male, sono sicuramente più veloce a leggere e comprendere in italiano. L'esame CISA si differenzia infatti da tutti gli altri esami per certificazioni che ho fatto proprio per il fattore tempo. Negli altri esami non ho mai avuto problemi di tempo, finendo sempre in buon anticipo senza dovermi preoccupare. L'esame CISA è invece basato diciamo sui riflessi, il candidato deve conoscere l'argomento a sufficienza per poter rispondere quasi senza dover pensare: una volta capita la domanda, la risposta giusta deve essere evidente altrimenti non c'è tempo per ragionarci su.

Per prepararmi all'esame ho adottato la mia procedura di sempre, prima studio tutta la teoria e poi faccio un po' di esercizi. So bene che questa non è la procedura adottata da tutti, anzi tra i miei compagni di corso molti si sono dedicati subito agli esercizi tornando alla teoria a seconda dei risultati degli esercizi, ovvero usando le risposte sbagliate come indicatore degli argomenti da studiarli meglio. Malgrado i miei sforzi, sono arrivato alla fine del corso, a due settimane dall'esame, avendo visto tutta la teoria almeno una volta e fatto pochi esercizi. Negli ultimi giorni di preparazione ho dedicato due ore al giorno allo studio della teoria e fatto 100 domande di fila con il limite temporale di due ore. In tutto ho fatto per esercizio poco meno di mille domande, di cui la maggior parte in inglese, ed alcune veramente vecchie ed obsolete. Il punto però non era tanto nelle domande in se, ma nell'abituarmi a rispondere nei tempi richiesti.

Arriviamo finalmente all'esame. Cosa dire? Malgrado la preparazione e tutto quanto ci era stato detto al corso e da colleghi che l'avevano già fatto, è stato una sorpresa. Mi aspettavo di trovare un 20% o 30% di domande già viste, ma così non è stato, le domande che avevo già fatto sono state molto poche. Inoltre buona parte delle domande non assomigliava a quelle che avevo fatto negli esercizi e che mi aspettavo di trovare. Questo ha creato in me, e dai commenti dei compagni di esame anche in altri, un senso di insoddisfazione che unito alla stanchezza delle 4 ore di esame ha fatto sì che ogni proposito di pranzo insieme post-esame è stato tacitamente abbandonato. Credo che il sentimento di insoddisfazione sia nato dal fatto che dopo aver fatto esercizi sino alla nausea, si era creata in me una quasi certezza di sapere a cosa andavo in contro. L'aver trovato domande diverse da quelle che mi aspettavo, mi ha fatto pensare in prima battuta che tutto il tempo e la fatica che avevo messo nella preparazione dell'esame erano stati inutili.

Ovviamente non è stato così, anche solo per il fatto che sono riuscito a finire tutte le domande a cinque minuti dal termine, e questo grazie al fatto che mi ero esercitato sulla tempistica. Comunque, terminato l'esame anche se insoddisfatto, ho atteso il risultato che è arrivato con un buon mese di anticipo sui tempi previsti.

Andrea Pasquinucci, CISA, professionista in ambito IT Security.

Siena - 8 luglio 2005

Monte Dei Paschi di Siena
 Centro di Formazione di Gruppo, Villa Isabella,
 V.le Camillo Benso di Cavour, 24

PROGRAMMA

- 10,00 Saluti di benvenuto da parte del Monte dei Paschi di Siena
- 10,15 **Anthony Cecil Wright, Presidente ANSSAIF, Responsabile del progetto di Business Continuity, Banca Nazionale del Lavoro**
Da luglio 2005 a Dicembre 2006: cosa ci attende? Che priorità? Che rischi di progetto?
- 11,00 **Andrea Beretta, Associate Partner, KPMG - Nolan & Norton**
*Il progetto di Business Continuity: le fasi di "implementation" e "maintenance".
 Quali riferimenti e "best practices"*
- 11,30 Pausa caffè
- 11,45 **Vincenzo Giardina, Responsabile del Progetto Continuità Operativa del Consorzio Operativo MPS.**
Dal Design all'Implementation: problematiche realizzative del BCP
- 12,30 **Giovanni Oldani, IBM Italia**
Disaster Recovery: aspetti tecnico – organizzativi
- 13,00 Colazione
- 14,00 **Stefano Cesarini, Senior Manager, KPMG.**
*L'auditing del progetto di business continuity:
 alcune riflessioni*
- 14,30 **Marco Recchia, Banca Antonveneta**
L'auditing del BCP: problematiche.
- 15,15 **Francesco Santiloni, Area Controlli Interni – Corporate Center Monte dei Paschi di Siena, Servizio Metodi e Attività Specialistiche.**
L'attività di Auditing sul BCP/DR del Gruppo MPS
- 16,00 **Tavola rotonda – coordinatori:**
Anthony Cecil Wright, ANSSAIF;
Francesco Santiloni, Consigliere AIEA;
Massimiliano Magi Spinetti, dirigente responsabile della Commissione Tecnologie e Sicurezza, ASSOCIAZIONE BANCARIA ITALIANA
- 17,00 Chiusura dei lavori





Sessioni di studio

Torino - 22 settembre 2005

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

PROGRAMMA

- 9.15 Introduzione dei lavori da parte del Chairman
- 9.30 **Alberto Carnevale (Protiviti)**
Introduzione all'Enterprise Risk Management
- 10.15 **Marco Marengo (Toro Assicurazioni)**
Modelli ed esperienze di Risk Management
- 11.00 Pausa caffè
- 11.15 **Tiziana Rossi (Ersel Sim)**
Risk Assessment : l'esperienza Ersel
- 12.00 **Pietro Ranieri (Fondiarria-Sai)**
Risk Assessment del Sistema Informativo Aziendale
- 12.45 Dibattito con gli oratori e conclusione dell'incontro a cura del Chairman
- 13.15 Termine dei lavori



Sessioni di studio

Roma - 28 settembre 2005

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

PROGRAMMA

- 14.15 Introduzione dei lavori da parte del Chairman (Donatella Rosa Vicepresidente AIEA)
- 14.30 **Michele Barbi (Etnoteam)**
IT Governance – modello di gestione
- 15.20 **Luigi Brusamolino (Symantec)**
I nuovi fenomeni di frodi online: strategie e contromisure di sicurezza
- 16.10 Pausa caffè
- 16.25 **Stefano Silvestri (PricewaterhouseCoopers)**
Gruppo di lavoro "Penetration test": obiettivi e risultati
- 17.00 **Pietro Brunati (Nest)**
Gruppo di lavoro "Penetration test": organizzazione e modalità operative
- 17.50 Dibattito con i relatori
- 18.30 Termine dei lavori



Sessioni di studio

Roma - 3 novembre 2005

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

PROGRAMMA

- 14.15 Introduzione dei lavori da parte del Chairman (Donatella Rosa Vicepresidente AIEA)
- 14.30 **Raoul Savastano (KPMG)**
Digital accounting: rischi e opportunità del documento elettronico
- 15.20 **Giacomo Aimasso (Exo Service)**
Auditing dei Servizi di Outsourcing: approccio basato sulla Gestione del Rischio
- 16.10 Pausa caffè
- 16.25 **Flavio Riciniello (Eidos Consulting)**
Quattro passi ... tra le frodi
- 17.20 Dibattito con i relatori
- 18.30 Termine dei lavori



Sessioni di studio

Milano - 11 novembre 2005

Unicredit Servizi Informativi
Via Livio Cambi, 1

PROGRAMMA

- 14.15 Introduzione dei lavori da parte del Chairman
- 14.20 **Francesco Perna (ENEL)**
Realizzazione in azienda di un Security Operation Center
- 15.15 **Giovanni Pietrabissa (PWC)**
XBRL – eXtensible Business Reporting Language – nasce un nuovo standard europeo. Nuove opportunità?
- 16.00 Pausa caffè
- 16.15 **Miam Rizzo (Fasternet)**
Il controllo: la seconda anima della tecnologia
- 17.00 Domande e dibattito finale con i relatori
- 17.45 Conclusione dell'incontro a cura del Chairman
- 18.00 Termine dei lavori





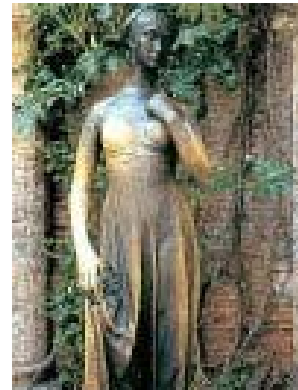
Sessioni di studio

Verona - 25 novembre 2005

Banco Popolare di Verona e Novara
Sala Convegni - Viale delle Nazioni, 4

PROGRAMMA ITIL e CMMI per l'IT Governance

- 9.00 Apertura dei lavori e saluto da parte di **Silvano Ongetta, Presidente AIEA**
- 9.10 Saluto da parte di **Giovanni Pietrobelli, Direttore Generale Società Gestione Servizi—BPVN**
- 9.20 Introduzione dei lavori da parte del Chairman, **Orillo Narduzzo, Vicepresidente AIEA**
- 9.30 **Stefania Renna (Computer Associates)**
ITIL: cos'è e di cosa tratta
- 10.00 **Stefania Renna, Elio Molteni (Computer Associates)**
Una architettura tecnologica conforme ad ITIL
- 10.30 Pausa caffè
- 10.45 **Giovanni Motta (BMC)**
Centralità del CMDB nei processi ITIL
- 11.15 **Giovanni Motta (BMC)**
Atrium CMDB: tecnologia abilitante per ITIL
- 11.45 **Federico Corradi (Cogitek)**
Il percorso di realizzazione di ITIL: l'esperienza di CSI Piemonte
- 12.15 Domande e dibattito con i relatori
- 12.30 Buffet offerto da BMC, Compuware, AIEA
- 14.00 **Marco Salvato (KPMG)**
ITIL e altre metodologie a supporto dell'IT Governance: una visione integrata
- 14.30 **Claudio Sangiorgi (Compuware)**
L'evoluzione nella gestione dei Processi: l'IIM (Integrated IT Management)
- 15.00 **Paola Pizzi (Poste Italiane SpA)**
Poste Italiane Best Practice e Metodologie coabitazione ed evoluzione
- 15.30 **Ezio Miozzo (Studio di Consulenza Aziendale)**
Il CMM© e CMMI© una metodica che ha fatto strada
- 16.15 Domande e dibattito con i relatori
- 17.00 Termine dei lavori



Sessioni di studio

Roma - 13 dicembre 2005

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

PROGRAMMA

- 14.15 Introduzione dei lavori da parte del Chairman (Donatella Rosa Vicepresidente AIEA)
- 14.30 **Alessandro Lega (Traicon – Gruppo DAB)**
Social Engineering: ovvero l'arte dell'inganno
- 15.20 **Marinella Marzo (PWC) e Giovanni Pietrabissa (PWC)**
*XBRL – eXtensible Business Reporting Language
nasce un nuovo standard europeo, nuove opportunità?*
- 16.10 Pausa caffè
- 16.25 **James Cheyne (NCR)**
Business Continuity Plan: Guida alla stesura
- 17.20 Dibattito con i relatori
- 18.30 Termine dei lavori



Sessioni di studio

Milano - 16 dicembre 2005

Unicredit Servizi Informativi
Via Livio Cambi, 1

PROGRAMMA

- 14.15 Introduzione dei lavori da parte del Chairman
- 14.30 **Siro Tasca (Protiviti)**
Adeguamento al Sarbanes-Oxley Act: requisiti normativi ed impatti per le imprese italiane
- 15.20 **Andrea Pasquinucci (AIPSI)**
Algoritmi crittografici oggi: sopravvivere tra 'rotture' e novità
- 16.10 Pausa caffè
- 16.25 **Stefano Niccolini (Federazione BCC)**
L'Information System Auditing in accordo con la metodologia Cobit e la certificazione ISO 9001:2000
- 17.30 Dibattito con i relatori
- 18.15 Conclusione dell'incontro a cura del Chairman
- 18.20 Termine dei lavori





AIEA
Associazione Italiana
Information Systems Auditors

ISACA
Information Systems Audit and
Control Association

AIEA capitolo di Milano di ISACA

20141 Milano— Via Valla, 16
Tel 02 84742.365- Fax 02 84742212
E-mail: aiea@aiea.it
P.IVA 10899720154

InfoAIEA

2005, Volume 3 n.3
Registrazione al Tribunale di Milano
n. 372 del 9.6.2003

Direttore Responsabile **Silvano Ongetta**
Editore: AIEA, via Valla, 16
20141 MILANO

Redazione: **Orillo Narduzzo**
Hanno collaborato: **Stefania Bove,**
Dario Forte, Cesare Gallotti, Orillo
Narduzzo, Andrea Pasquinucci,
Angelo Rodaro.

Tutti i diritti sono riservati. Il testo e le immagini non possono essere riprodotti senza autorizzazione. Le opinioni espresse dagli autori non rappresentano necessariamente le posizioni dell'AIEA. Ogni contributo sarà subordinato al vaglio di un Comitato Scientifico.

Siamo su Internet:
www.aiea.it

COLLABORATE!!

InfoAIEA ha bisogno della collaborazione di tutti gli associati: articoli, segnalazioni, quesiti, opinioni, vignette,

SCRIVETECCI!!

E-mail : infoaiea@aiea.it, aiea@aiea.it
Sede: AIEA, Redazione InfoAIEA
Via Valla, 16 - 20141 Milano

Consiglio Nazionale 2004-2006

Presidente: **Silvano Ongetta**
Vice presidenti: **Donatella Rosa,**
Orillo Narduzzo
Segretario: **Enzo Toffanin**
Tesoriere: **Daniela Cellino**

Consiglieri:

Mario Ballerini, Emanuele Boati,
Francesco Ceccarelli, Francesco Galli,
Angelo Rodaro.

Probiviri:

Francesco Blanco, Daniela Landini,
Enrico Schiocchet



ISACA

Information Systems Audit and Control Association

Nota per i collaboratori.

Gli articoli scientifici pubblicati costituiscono una opportunità per guadagnare ore di credito nell'ambito del CISA e CISM Continuing Education.

I documenti debbono essere inoltrati in formato testo o word, le figure debbono essere inserite come immagini.