



ASSOCIATI!

di Enzo Toffanin

Impegno di fondi del budget aziendale; per sottoscrivere la quota annuale AIEA; euro 180 per un nuovo associato e 155 per il rinnovo; motivazioni Vediamole con ordine. L'Associazione, con questa cifra individuale che ricorda il prezzo di un abbonamento ad una rivista o meno di un caffè al giorno, ma non per questo da non giustificare, mi permette di ricevere pubblicazioni tecniche di buona fattura (l'Information System Control Journal, il periodico Global Communiqué, da gennaio 2003 i notiziari Express Line di fonte ISACA; InfoAIEA, Newsletter di fonte AIEA). Mi tiene aggiornato sulle novità del Book Store ISACA, mi

mette a disposizione gli studi dell'IT Governance Institute e della Fondazione. Mi consente di partecipare ai Gruppi di Ricerca italiani, a Comitati e Gruppi di lavoro Internazionali per elaborare standard, procedure di audit e di controllo. Mi dà accesso ai siti web ISACA e AIEA, incluse le aree riservate ai soci con tutto il patrimonio di conoscenze che ISACA mette a disposizione on line. Direi che le 180/155 euro sono ben spese. Ma forse vi sono anche altre motivazioni.

Una storia comune. Qualche anno fa, mi chiamano in azienda e mi dicono "... tu sei il nostro esperto di

EDP audit" (si diceva così allora). Mi ritrovo un nuovo ufficio, un lavoro da inventare, quesiti insoliti sui sistemi IT, molta buona volontà, poca tecnica, un po' di disorientamento.

L'idea: esisterà pure qualcuno che si occupa di queste cose? Cerco, scartabello e trovo l'Associazione Italiana EDP Auditors, l'AIEA. Il gioco è fatto; subito una sottoscrizione, l'incontro con un bel drappello di colleghi di altre aziende, il contatto che mi mancava, la formazione, le letture giuste. E si comincia a navigare (remare direbbe qualcuno).

Qualche anno dopo il mio
(Continua a pagina 2)



Sommario:

<i>Associati! di E. Toffanin</i>	1
<i>AIEA—I numeri del 2002</i>	1
Gruppo di Ricerca: 'Sistemi di Gestione della Sicurezza delle Informazioni'	3
<i>EU Task Force Bancaforte CISM</i>	4
<i>Impressioni di un socio di L. Carrozzi</i>	10
<i>COBIT NEWS</i>	11
<i>Sessioni di studio</i>	12 15
<i>Lecture</i>	16
<i>Indice</i>	18

Primi in EUROPA

Conoscere la propria storia rende consapevoli dei traguardi raggiunti e dell'impegno profuso. In questo mese ricorre il nostro compleanno!

Il nostro capitolo è il **43°** della storia di ISACA.

E' stato il **primo** capitolo dell'Europa (prima degli anglosassoni e dei nordici).

Siamo nati esattamente il **20 dicembre 1979!**

Grazie a tutti i Presidenti, Consiglieri, Soci e Volontari che hanno contribuito in questi 23 anni di sviluppo e progresso professionale.



ASSOCIATI!

di Enzo Toffanin

(Continua da pagina 1)

lavoro è strutturato, altri colleghi più giovani mi affiancano, li indirizzo, li faccio associare e do loro le possibilità che io ebbi a suo tempo.

Il tempo passa. Il mio ruolo è un po' cambiato. L'ufficio è cresciuto. Rispondo all'Alta Direzione, nel senso stretto del termine: ricevo quesiti a cui devo dare risposte tempestive, di alta qualità, allineate alla migliore prassi internazionale. Ancora scopro che la formula più efficiente è il confronto con quei colleghi che erano giovani quando entrai in Associazione e che ora condividono con me la soddisfazione e la fatica di un ruolo consolidato in azienda e di uno standing riconosciuto.

Lo standing. Non mi riferisco solo al prestigio: quando c'è, aiuta a vivere meglio. Mi riferisco alla posizione raggiunta, alla sua prospettiva di promozione e cambiamento. A qual cosa che riguarda le mie aspettative, la mia possibilità di confrontarmi con il mercato, i miei deside-

rata (sono realistici?!), le mie relazioni personali. Certo la mia azienda può sentire meno questi valori. Ma essi investono il mio essere e il mio futuro e per me significano appartenere ad una comunità che mi riconosce per il ruolo che ho in azienda, per la mia professionalità, per la mia storia.

In questa comunità impostata al contributo personale volontario l'unica gerarchia possibile è l'autorevolezza; e come si sa l'autorevolezza non la si acquisisce per nomina.

In questa comunità c'è chi è più giovane e cerca il supporto e la formazione che quelli come me riescono a dare. Qualche capello grigio in più fa capire che la concorrenza è sacrosanta, ma il business cerca anche riferimenti tecnici e etici a cui si arriva solo dal confronto aperto di opinioni e posizioni; l'associazione professionale può essere un luogo ideale ove convergere per far valere le proprie esperienze, ottenendone una adesione che è frutto di compromesso positivo tra le diverse parti e interessi in gioco.

E il tempo continua a passare. Ci sono tempi d'oro e tempi meno esaltanti. Qualche volta cambiare lavoro è motivo di grande entusiasmo e soddisfazione e qualche volta lo è di meno. E anche qui quando si recide un laccio, contare su legami che rimangono intatti è senza dubbio un valore apprezzato. Quando poi si riparte nella nuova realtà, ricostruire metodi, procedure, approcci non è così semplice, così copiabile dalla passata esperienza. Mentre valersi legittimamente di metodi e standard dell'Associazione, a cui magari si è pure contribuito nella elaborazione, è motivo di sicurezza, orgoglio ed efficienza.

Non so se queste considerazioni tutte assieme mi permetteranno di sostenere con dovizia di ragioni anche quest'anno la mia richiesta di fondi del budget aziendale per sottoscrivere la quota annuale AIEA, ma forse, riflettendo, le motivazioni e le ragioni sono anche le mie ragioni, che certo non sono in contrasto con quelle della mia azienda, ma possono rimanere assai importanti per me; anche quando le altre priorità aziendali minacciano di sacrificare il budget per la mia quota AIEA; non foss'altro perché magari in azienda mi occupo di qualche cosa di diverso dall'EDP Audit di buona memoria. Non posso certo spiegare che nel frattempo l'AIEA ha vissuto quasi 24 anni e l'ISACA di più, è nato l'ICT Governance, la sicurezza non è più teoria, né goliardica sfida ai sistemi.

In conclusione, buoni motivi per sostenere la richiesta fondi del budget in azienda ce ne sono; ma se per qualche ragione non bastasse, credo che per meno del prezzo di un caffè al giorno, valga sicuramente la pena di fare questa spesa anche di tasca propria.

AIEA—I numeri del 2002

Convegno Nazionale	1
Gruppi di Ricerca attivati	4
Sessioni di studio	11
CPE hours accumulabili	50
Aziende rappresentate	100
Aderenti	300
Accessi sito Web da aprile 2001	10.200



Gruppo di Ricerca: *‘Sistemi di Gestione della Sicurezza delle Informazioni’*



Presentazione del progetto

Gli standard e i riferimenti metodologici degli Information Security Management System (ISMS) di cui disponiamo (es.: BS7799/ISO17799) trovano ancora ridotti livelli di adozione da parte delle aziende nonostante offrano autorevoli modelli di governance della sicurezza ICT e siano in grado di influire in maniera profonda sulla protezione e sullo sviluppo del business aziendale.

La comunità professionale degli Information System Auditors non può che trarre vantaggio dalla loro diffusione.

L'adozione di tali sistemi consente infatti non solo di praticare le relative attività di audit ma anche di offrire servizi di supporto al management aziendale per le attività di disegno e implementazione degli ISMS. Vengono quindi a crearsi nuove opportunità di coinvolgimento degli auditor, fermo restando il doveroso rispetto della separazione di ruoli tra chi progetta il sistema gestionale e chi lo verifi-

ca. Obiettivo del GdL è quello di identificare i percorsi di promozione degli ISMS focalizzando le nuove opportunità per gli Information System Auditors.

Le attività verranno svolte secondo i seguenti tre passi.

1. Gli ISMS: strumenti per la qualità e continuità del business aziendale

Enunciare importanza e vantaggi degli approcci strutturati e integrati per la gestione della sicurezza delle informazioni.

L'obiettivo è quello di presentare con chiarezza ed efficacia quali potenti strumenti di coordinamento e controllo tali sistemi rendono disponibili al management.

In tale contesto diviene preziosa la competenza ed il ruolo degli auditor che possono divenire 'interpreti e garanti' del modello manageriale di riferimento.

2. Comprendere le barriere all'adozione degli ISMS

Condurre un'analisi delle barriere (non ulti-

me quelle culturali) alla introduzione degli ISMS nelle aziende.

L'obiettivo è quello di comprendere cosa blocchi o rallenti l'adozione di tali strumenti facendo riferimento, laddove possibile, anche alle caratteristiche di filiera e dimensione aziendale. Le modalità di analisi saranno definite dal gruppo nel corso dei lavori. E' comunque prevedibile l'utilizzo di questionari specifici da proporre ad aziende e/o manager di riferimento.

3. Sugerimeti /Action list

Si tratta di formulare delle possibili soluzioni agli ostacoli identificati al punto precedente. L'obiettivo è quello di fornire al management suggerimenti e possibili percorsi soluzione (es.: action list: to-do/not-to-do) per superare i fattori limitanti individuati. I risultati saranno raccolti in un 'Manuale di facilitazione all'introduzione degli ISMS' a disposizione dell'associazione.

Componenti del Gruppo di Ricerca:

Bianco Tcube

Carrozzi TIN

Cheyne Fondspa

Tomassi GRTN

Vollono Poste

Zambon BNL

NEW CISM™ Certification

(fonte ISACA)

Hot News

→ Toffanin nella "EU Task Force"

Il Presidente Internazionale di ISACA, Robert Roussey, ha chiamato il nostro segretario Enzo Toffanin a far parte della commissione "2002-03 European Union Task Force". E' una commissione importante che definirà il profilo della nostra professione in ambito europeo per i prossimi anni, ne abbiamo parlato in InfoAIEA di settembre 2002. Ci congratuliamo con Enzo per l'ulteriore riconoscimento della sua professionalità e gli auguriamo buon lavoro.

→ Ongetta nel Comitato Tecnico di Bancaforte

Il nostro Presidente, Silvano Ongetta, è stato chiamato a far parte del Comitato Tecnico della rivista BancaForte. E' una pubblicazione dell'ABI che si occupa in modo ampio e articolato della sicurezza in ambito bancario e finanziario. Per avere la propria copia gratis rivolgersi ad aiea@aiea.it. Auguri e congratulazioni a Silvano.

CISM characteristics

"CISM differs from the others by virtue of its experience requirements and focus exclusively on the job performed by an information security manager.

Other security certifications are characterized by a focus on technical skills or platform- or product-specific knowledge, or they are aimed at the practitioner in the earlier years of their career. Only CISM targets the information security manager-the individual who has progressed beyond the practitioner focus, whose emphasis is no longer technical or specialist skills, and who has moved on to the management of an enterprise's information security program. CISM is for the individual who must manage and oversee the enterprise's information security effort, including the practitioners, many of whom may hold the other certifications the field offers".

CISM Job Practice Analysis Completed

The CISM job practice analysis survey was recently sent to more than 2,300 information security directors, managers and officers who were

asked to validate the work and to determine the relative frequency and criticality associated with CISM task and knowledge statements. The results of this survey were evaluated and the final job practice analysis was approved and will be used for CISM exam content. The development of the CISM job practice analysis included the use of prominent industry leaders, subject matter experts and industry practitioners, all of which played a key role.

CISM Grand-fathering Period

The CISM Certification Board has begun to review applications for CISM under the grandfathering provision. Nearly 100 applications already have been received and are being scrutinized to ensure individuals have the proper and appropriate information security management experience. The program allows professionals with extensive information security management experience an opportunity to qualify for and obtain the CISM credential without taking the CISM exam. The grandfathering period will run through 31 December 2003.



NEW CISM™ Certification CISM FAQ'S

Why has ISACA developed an information security certification?

ISACA's name reflects its obligation to offer products, services and benefits not only to the information systems audit profession, but to those who play a vital role in information systems control as well. More than 20 years ago ISACA pioneered the Certified Information Systems Auditor (CISA) credential and has developed and offered training programs to information systems auditors, information security practitioners and those involved in information technology governance. Most recognized in the industry are a series of ISACA conferences that are known as CACS (computer audit, control and security). These programs are held each year worldwide and meet the educational needs of a wide variety of information systems professionals. In recent years, ISACA has undertaken other information security and IT control activities: increased focus on security in the *Information Systems Control Journal*, creation of the IT Governance Institute, and development of research in the privacy area. The maturity of ISACA membership and CISAs and their requested need for an information security credential that goes beyond the practitioner level has led ISACA to the development the CISM credential.

What will the CISM exam cover?

The CISM exam will cover five information security management areas, each of which is further defined and detailed through task and knowledge statements. The five areas are:

[Information Security Governance](http://www.isaca.org/cismcont1.htm) (www.isaca.org/cismcont1.htm) Establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations.

[Risk Management](http://www.isaca.org/cismcont2.htm) (www.isaca.org/cismcont2.htm) Identify and manage information security risks to achieve business objectives.

[Information Security Program\(me\) Management](http://www.isaca.org/cismcont3.htm) (www.isaca.org/cismcont3.htm) Design, develop and manage an information security program to implement the information security governance framework.

[Information Security Management](http://www.isaca.org/cismcont4.htm) (www.isaca.org/cismcont4.htm) Oversee and direct information security activities to execute the information security program.

[Response Management](http://www.isaca.org/cismcont5.htm) (www.isaca.org/cismcont5.htm) Develop and manage a capability to respond to and recover from disruptive and destructive information security events.

Clicking on the title of any of these five areas will take you to a list of specific task and knowledge statements that represent a current market perspective of what is performed and what should be known by information security managers and provides the basis for the CISM exam.

NEW CISM™ Certification CISM FAQ'S

(Continua da pagina 5)

What is the CISM job practice analysis and how was it developed?

ISACA's philosophy toward certification is to measure individuals' ability and knowledge as it pertains to the performance of their job. As such, ISACA approached the creation of the CISM job practice analysis with the same care and rigor it always has devoted to CISA. To ensure the job practice analysis is reflective of the work performed by information security managers, ISACA appointed a working committee of information security experts to develop and validate a series of task and knowledge statements that properly describe this role. The work included the use of prominent industry leaders, subject matter experts and industry practitioners, all of which played a key role in the development of the CISM job practice analysis.

What are the qualifications to earn the CISM credential?

Qualifying for CISM requires a combination of four "e's": experience, ethics, education and examination. Specifically, the requirements are:

- Successful completion of the Certified Information Security Manager (CISM) exam
- Adherence to a code of professional conduct
- Commitment to continuing professional education
- Submission of verified evidence of a minimum of five years of information security work experience, with a minimum of three years of information security management work experience in three or more of the job practice areas. Waivers for general information security work experience are available, if certain education or certification requirements are met.

For further details, click here. (www.isaca.org/cismrequire.htm)

Who is eligible to become CISM certified and what makes CISM unique?

CISM is unique in the information security credential marketplace because it is designed specifically and exclusively for individuals who have experience managing an information security program. Experience requirements and the CISM exam are based on the experience required to competently perform the duties and responsibilities of an information security manager. These requirements and the tasks and knowledge that are tested were developed by information security leaders and later validated by subject matter experts and information security managers. The requirements are designed to measure an individual's *management* experience in information security situations, not general practitioner skills.

Will CISAs qualify for CISM?

The CISM certification program recognizes the achievement of the CISA credential as a baseline representation that an individual has gained general information security skill and knowledge. As such, CISAs receive a two-year general information security waiver. However, CISAs will not be eligible to earn a CISM unless they have the required experience and can demonstrate proficiency and practical knowledge in the role of an information security manager.

(www.isaca.org/cismrequire.htm#experience) Click here to learn how to earn CISM both through exam and through grandfathering.

(Continua a pagina 7)



NEW CISM™ Certification CISM FAQ'S

(Continua da pagina 6)

Will CISSPs and other security credential holders qualify for CISM?

The CISM certification program recognizes the achievement of the CISSP credential as a baseline representation that an individual has gained general information security skill and knowledge, just as it does with individuals who have earned a CISA. As such, CISSPs receive a two-year general information security experience waiver. However, CISSPs will not be eligible to earn a CISM unless they have the required experience and can demonstrate proficiency and practical knowledge in the role of an information security manager. Holders of other, more specialized credentials, such as the SANS Global Information Assurance Certification (GIAC), Microsoft Security Systems Engineer (MCSE), CompTIA Security + Credential and the Disaster Recovery Institute Certified Business Continuity Professional (CBCP) also can receive a one-year general information security experience waiver.

How is CISM different from the other security certifications?

CISM differs from the many other security certifications by virtue of its experience requirements and focus on the job performed by an information security manager. Other security certifications are characterized by a focus on technical skills or platform- or product-specific knowledge, or they are aimed at the practitioner in the earlier years of their career. Only CISM targets the information security *manager* the individual who has progressed beyond the practitioner focus, whose emphasis is no longer technical or specialist skills, and who has moved on to the management of an enterprise's information security program. CISM is for the individual who must manage and oversee the enterprise's information security effort, including the practitioners, many of whom may hold other certifications the field offers.

The focus on management that makes CISM unique is demonstrated in its experience requirement, which calls for a minimum of *three* years in information security management, and in its exam focus that is based on the job practices performed by information security managers.

How is CISM different from the Certified Information Systems Security Practitioner (CISSP)?

Although there are many differences between the CISSP common body of knowledge and the CISM job practice areas, the most obvious difference is in the experience requirements. Only CISM requires information security management experience, in addition to general information security experience. CISSP has no such management requirement.

Earning the CISSP and/or the CISA credential is complementary to the attainment of the CISM credential and is encouraged.

What is CISM's grandfathering provision?

The grandfathering provision allows individuals who have an advanced number of years of experience managing an information security program to earn the CISM certification without taking the CISM exam. The grandfathering provision period is available only for a limited time that ends on 31 December 2003. After that, all CISM candidates, regardless of experience level, will be required to pass the CISM exam to qualify for CISM certification. The experience requirements are more stringent than for candidates taking the exam. Whereas the individual taking the exam must have *five* years of information security work experience, with at least *three* of those years in information security management experience in *three* or more of the job practice analysis areas, the grandfathering applicant must have a minimum of *eight* years of information security work experience, with at least *five* of those years in information security manage-

(Continua a pagina 8)

NEW CISM™ Certification CISM FAQ'S

(Continua da pagina 7)

ment work experience in *four* or more of the job practice analysis areas. Waivers for general information security work experience are available, if certain education or certification requirements are met.

For details, click here. (www.isaca.org/cismrequire.htm#grandfather)

When will the first CISM exam be held?

The first CISM exam will be in June 2003, at the same time and in the same worldwide locations where the CISA exam is held. The CISM exam will consist of 200 multiple-choice questions that cover the CISM job practice areas. In 2003, the exam will be offered in English only, however, future plans include the translation of the CISM exam into other languages based on demand and interest.

Can I take the CISM exam and CISA exam on the same day?

Since the CISM and CISA exams are geared to information systems professionals at different points in their career, the 2003 CISM and CISA exams will be held simultaneously. This means that an individual will not be able to sit for both exams. Individuals who are not currently practicing as an information security manager, but aspire to in the future, are encouraged first to earn the CISA designation.

What CISM exam study materials will be available and when?

A CISM Review Manual will be available in January 2003 to assist individuals to prepare for the CISM exam. The manual will feature detailed descriptions and explanations of task and knowledge statements and provide applicable information security management principles, practices and strategies with references to where additional guidance can be found. This manual will assist with exam preparation, but since the exam is based on information security management practices it must be used as a guide and not considered as an all-inclusive study source. CISM review courses also will be conducted by ISACA chapters on a limited basis.

What does the CISM continuing professional education program require?

In order to become and remain a CISM an individual must agree to comply with the CISM continuing professional education program. This program requires an individual to earn a minimum of twenty (20) hours annually and one hundred and twenty (120) hours every three years of continuing professional education. Specific activities and requirements are currently under development and will be published in January 2003. In addition, an annual maintenance fee of US \$35 ISACA member and US \$50 non-member will be required beginning in 2003. Individuals holding both a CISM and a CISA will receive a discount.

What if we as a chapter cooperate locally with the ISSA chapter or promote CISSP?

ISACA chapters are encouraged to maintain their relationships with ISSA/ISC(2). ISACA does not view CISM and CISSP as competitive, but rather complementary. We are all trying to serve the security market, but at different levels and in different ways; therefore it is in the best interests of all concerned to work together.

What are the grandfathering fees to be used for?

The CISM Certification Board determined that the fee charged for application as a CISM under the grandfathering provision should be set at an appropriate level above the cost of exam in order to generate the funds needed to initiate the certification program and to ensure that only serious candidates apply. These funds are, and will continue to be, used to fund the various start-up activities and expenses relating to the certification, including the development and validation of the job practice, program marketing and promotion, hiring administrative personnel to handle applications and inquiries, legal expenses, initial exam item and study guide development and funding CISM Certification Board meetings.



COBIT™ NEWS

COBIT e l'Università

The Information Systems Audit and Control Association (ISACA) is organizing, hosting and delivering workshops to:

Develop a better understanding of the academic needs in building up courses using COBIT.

Determine the components required for good COBIT case studies.
Determine how COBIT components can be leveraged to create comprehensive cases for the classroom

ISACA is providing a grant opportunity for academics to attend a workshop.

You are requested to invite your local academics to view the grant proposal and download the application posted to the ISACA web site at <http://www.isaca.org/cobitacadem.htm> and urge them to submit their application for consideration by 31 January 2003. The European workshop will be held either pre- or post-European Accounting Conference in April 2003. The North American workshop will be held either pre- or post-American Accounting Conference in August 2003.

Please feel free to contact me at <research@isaca.org> if I can be of Any further assistance to you.

Sincerely,
Linda Wogelius
Research Assistant

E' una opportunità per i professori universitari che conosciamo; potrebbe essere l'inizio di un filone di ricerca accademica con tesi e relazioni di sicuro interesse professionale. Passa la notizia.

COBIT: versione italiana, I complimenti di ISACA

Orillo,
Silvano,
and Aureliana,

Thank you for the translated sections of CobiT, the publications have arrived at International in good condition and look very professional.

I have forwarded the publications to Patty Handchetz who oversees our bookstore, and also informed Tom Lamm in the research department of the publications arrival. In addition, we have now been notified that the funds referenced below have been received by our financial institution.

Thank you for your efforts in the translation of CobiT.

Scott Artman

Uniamo ai complimenti di ISACA quelli del Direttivo e li indirizziamo a tutti i componenti del gruppo. Il tempo dedicato è sttao tanto ma ne è valsa la pena. Presto la versione Italiana, della quale abbiamo il copyright e un contratto in esclusiva con ISACA, sarà disponibile sul Bookstore.

COBIT: per aggiungere una nuova dimensione

L'IT Governance Institute® ha pubblicato le prime "IT control practice statements", i soci possono scaricarle dal sito www.isaca.org/@member.

Tutti i soci sono invitati ad utilizzare e provare questi standard e far pervenire ad ITGI le loro osservazioni.

Complessivamente saranno disponibili 29 control practice statements entro il primo semestre del 2003.

La metodologia COBIT 3rd Edition® può essere ordinata al Bookstore del sito www.isaca.org/bookstore.htm. Inoltre alla COBIT home page si possono trovare esempi di utilizzo presso diverse aziende.

Segnalaci tutte le esperienze di utilizzo di COBIT che conoscete, invia alla redazione aiea@aiea.it i seguenti dati:

- Azienda,
- Riferimenti (responsabile, auditor, ufficio, tel.,ecc.),
- E-mail,
- Consulente (eventuale),
- Titolo dell'attività,
- Anno di realizzazione,
- Autorizzazione alla pubblicazione o non autorizzazione alla pubblicazione (in questo caso i dati saranno usati solo per fini statistici),
- Breve descrizione.



La giornata di studio del 2.10.2002 a Roma: le impressioni di un nuovo socio.

La mia partecipazione alla giornata AIEA del 2 ottobre è stata per me come aver incontrato un vecchio amico, uno di quelli che conosci da tempo, ma che poi per un motivo o l'altro perdi di vista.

Più di qualche anno fa (era il 1995, se non ricordo male) quando in Telecom Italia seguivo, tra l'altro, gli aspetti di *performance management* dei sistemi informatici nel gruppo 'metrologia' del CMG (Computer Measurement Group), partecipai all'avvio di un neonato Gruppo di lavoro AIEA sulle tematiche del 'Monitoraggio'.

Ciò avveniva nell'ambito di quegli scambi avviati tra associazioni che, con profili e finalità diverse, si cimentano su materie affini per attivare, come diremmo oggi, un po' di 'cross-fertilization'.

Ricordo positivamente quell'esperienza perché l'approccio culturale e metodologico era sostanzialmente lo stesso e le riunioni filavano lisce, con profitto per tutti i partecipanti.

Da qualche anno mi occupo di Risk Analysis e Security management e visto l'interesse che AIEA mostra sul tema, ho presentato domanda di adesione all'associazione e

seguito la sessione di studio del 2 Ottobre a Roma.

Veniamo alle impressioni di 'primo impatto' dell'associazione.

Il taglio del sito web, le procedure interne (es.: vaglio nuove adesioni), l'attività di formazione e informazione dei soci, e le altre numerose attività presentate nella sessione di studio, mi confermano l'opinione di una associazione dinamica e protesa nella difesa e promozione del profilo, delle competenze e delle esperienze professionali (manageriali e tecniche) degli auditor ICT.

Ritengo prezioso il servizio in tal senso reso dall'associazione, particolarmente nell'attuale contingenza di mercato.

La massiccia fase di implosione del mercato ICT se da una parte ha frantumato e ridotto il volume complessivo di attività, dall'altra sta favorendo la razionalizzazione dei processi ed il ripensamento dei modi di creare e gestire i servizi di ICT recuperando efficienza e qualità erogata. Taluni strumenti metodologici a nostra disposizione (es.: COBIT, BS7799) e le relative best practices consentono di supportare le aziende clienti proprio in tal senso, agendo sui si-

stemi di coordinamento e controllo dell'ICT.

Le mie aspettative dall'associazione? Che diffonda sempre più la cultura e le professionalità dell'IT Audit. E' importante, forse oggi più che mai, far conoscere il contributo che queste portano alla generazione di 'business value' aziendali.

Potrebbe essere interessante a tal riguardo avviare uno specifico gruppo di lavoro sul tema. Penso ad esempio ad un gruppo teso ad individuare i fattori chiave necessari a promuovere presso le aziende l'adozione di un 'Information Security Management System'. E' importante capire cioè quali siano al momento le 'barriere d'accesso' all'introduzione di tali sistemi e per quanto possibile, individuare delle strategie per superarle a fronte dell'opportunità che tali sistemi offrono di trasformare la sicurezza ICT da 'problema' a 'valore' sia per l'azienda che lo adotta che per i suoi clienti.

**Luigi Carrozzì –
ICT Security Analyst**



Alcuni statements relativi al primo dominio per la certificazione CISM

Knowledge Statements

- 1.01 Knowledge (K. after) of information security concepts.
 - 1.02 K. of the relationship between information security and business operations.
 - 1.03 K. of techniques used to secure senior management commitment and support of information security management.
 - 1.04 K. of methods of integrating information security governance into the overall enterprise governance framework.
 - 1.05 K. of practices associated with an overall policy directive that captures senior management level direction and expectations for information security in laying the foundation for information security management within and organization.
 - 1.06 K. of an information security steering group function.
 - 1.07 K. of information security management roles, responsibilities, and organizational structure.
 - 1.08 K. of areas of governance: (for example, risk management, data classification management, network security, system access...).
 - 1.09 K. of centralized and decentralized approaches to coordinating information security.
- (continua nel prossimo numero)*

ISACA: Bookstore

Attraverso una iniziativa congiunta ISACA e Deloitte & Touche è stata sviluppata una serie monografica dal titolo "e-Commerce Security Series".

I sei libri della serie sono:

- *e-Commerce Security—Global Status Report*
- *e-Commerce Security—Enterprise Best Practices*
- *e-Commerce Security—Trading Partner Identification, Registration and Enrollment*
- *e-Commerce Security—Public Key Infrastructure*
- *e-Commerce Security—Business Continuity Planning*
- *e-Commerce Security—Securing the Network Perimeter*

I libri possono essere ordinati a ISACA (www.isaca.org).

CISM™ REVIEW MANUAL 2003

ISACA

The *Certified Information Security Manager (CISM) Review Manual 2003* is a reference guide designed to assist individuals in preparing for the Certified Information Security Manager (CISM) examination and for individuals who wish to learn more about the role and responsibility of an information security manager.

The manual also provides definitions and practical examples.

(Available January 2003)

CISA: Esame 2003, Corsi, Materiale

CORSI

Anche nel 2003 effettueremo i corsi di preparazione all'esame CISA, sia a Roma sia a Milano. I corsi avranno inizio a febbraio; informazioni di dettaglio su sedi e calendario saranno comunicate in gennaio. Se non sei CISA valuta l'opportunità di sostenere l'esame nel 2003 e iscriviti ai corsi di preparazione.

Se hai i requisiti per richiedere la certificazione CISM nell'ambito della qualificazione Grandfathering, considera che essere CISA vale come due anni di esperienza.

2003 CISA Study Materials

2003 CISA study materials are now available through the ISACA Bookstore. The *2003 CISA Review Manual*, *2003 CISA Questions, Answers and Explanations Manual* (500 study questions) and *2003 CISA Questions, Answers and Explanations Manual Supplement* (100 questions) are excellent sources for candidate preparation for the 2003 CISA exam. The *CISA Questions, Answers and Explanations* CD-ROM (600 questions) and the CISA Study Course (currently under development) will be available this month for chapter download and use.

CISA Mentor

Ogni CISA dovrebbe diffondere la propria certificazione individuando nuovi candidati all'esame.

Le informazioni possono essere fornite direttamente o attraverso il materiale consultabile o scaricabile dal sito www.isaca.org.

Security Management



Sessione di studio di Torino— 7.11.2002

Auditorium di Telecom Italia
Corso Bramante, 20 - Torino

PROGRAMMA

- 14.00 Registrazione dei partecipanti
 14.15 Benvenuto a cura del Presidente AIEA **Silvano Ongetta**
 14.20 **Giorgio Gallina**
 Saluto da parte di Telecom Italia e breve presentazione del consorzio INTEL.AUDIT
 14.30 **Adamo Bove** - Telecom Italia Mobile
Il Security Management nelle strategie di sviluppo competitivo delle imprese
 15.15 **Marco Terragno** - Reale Mutua
La progettazione del Sistema di gestione della Sicurezza in Reale Mutua
 16.00 Pausa Caffè
 16.15 **Ada Di Sario** - FIAT
La protezione delle informazioni in un contesto aziendale tecnologicamente complesso: analisi del rischio e sicurezza delle infrastrutture di rete.
 17.00 Dibattito con gli oratori
 17.30 Conclusione dell'incontro a cura del chairman
 17.45 Termine dei lavori

A margine dei programmi delle sessioni vi diamo alcuni spunti estratti tra quelli più interessanti, le presentazioni complete le potete trovare sul sito www.aiea.it.

RISK ASSESSMENT: Riferimenti Normativi

RIFORMA CORPORATE GOVERNANCE
D. Lgs. N. 58/1998 - c.d. decreto Draghi



IL SISTEMA DI CONTROLLO INTERNO ASSUME AUTONOMO
RILIEVO NELLA LEGISLAZIONE SOCIETARIA

PRIMA

Il piano di audit per la copertura dei rischi era stabilito dal Management anche sulla base dei suggerimenti dell'Internal Audit.

REVISIONE PER ECCEZIONI

DOPO

L'entità e la priorità dei rischi è identificata attraverso il processo di Risk Assessment basato su criteri di valutazione del rischio coerenti e costanti nel tempo.

PIANO DI AUDIT

Risk Assessment Area IT: Introduzione

Il **Risk Assessment** per l'Information Technology è uno strumento di lavoro che ha come obiettivo la valutazione del livello di rischio potenziale dei sistemi aziendali mediante criteri

standard, al fine di definire il **piano degli interventi di audit** in termini di: obiettivi, priorità, frequenza e risorse da impegnare.

La fase iniziale del lavoro prevede l'individuazione, in collaborazione con i responsabili IT, dei Sistemi Informativi più rilevanti per dimensione, impatto sul business e normativa vigente, in quanto procedure poco rilevanti possono rendere più difficile l'individuazione delle reali aree di rischio, su cui indirizzare il controllo.

Vengono quindi definite le **"unità di rischio"** che raggruppano più sistemi omogenei per



IS Auditing delle Architetture Open Source

Sessione di studio di Roma— 03.12.2002

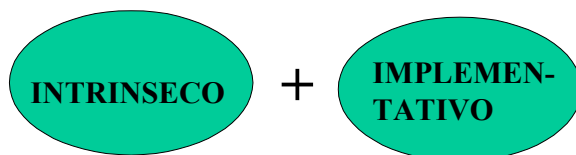


Palazzo Barberini—Circolo Ufficiali FF. AA. d'Italia—Sala Millevoi
Via delle 4 fontane - Roma

PROGRAMMA

- 9.30 Registrazione dei partecipanti
 10.00 Introduzione dei lavori da parte di **Donatella Rosa** (Vicepresidente AIEA)
 10.15 **Agatino Grillo** - Euros Consulting
Gruppo di ricerca: IS Auditing delle Architetture Open Source
 Consuntivo e prospettive
 10.30 **Renato Alessandrini** - ICCREA Holding
Linee guida per l'IS Auditing delle architetture Open Source
 11.00 **Francesco Blanco** – Ernst&Young
Audit Program per l'IS Auditing delle architetture Open Source
 11.30 Pausa Caffè
 11.45 **Claudio Telmon** - Università di Pisa
Peculiarità del Software OpenSource (OSS) dal punto di vista della sicurezza
 12.15 **Gabriele Giulimondi** - Pontificia Università S.Tommaso,
Total cost of ownership (TCO) delle architetture Opensource
 12.45 Dibattito con gli oratori
 13.00 Conclusione dell'incontro a cura del chairman

RISCHIO =



Dipende dalla natura
delle informazioni trattate
Controllabile con monitoraggi
periodici ed interventi sulla
sicurezza

Dipende dalla realizzazione
ed uso del sistema
Riducibile con interventi
organizzativi e/o
tecnologici

Visita il nostro sito

www.aiea.it

Le presentazioni degli inter-
venti delle sessioni sono
scaricabili dal sito.

In queste pagine alcune
slide con alcuni interessanti
spunti di riflessione, gli ar-
gomenti completi sul sito.

COBIT: traduzione e diffusione

Sessione di studio di Roma— 03.12.2002



Palazzo Barberini—Circolo Ufficiali FF. AA. d'Italia—Sala Millevoi
Via delle 4 fontane - Roma

PROGRAMMA

- 14.15 Introduzione dei lavori da parte di **Silvano Ongetta** (Presidente AIEA)
- 14.30 **Orillo Narduzzo** - SEC SERVIZI
Gruppo di ricerca: COBIT 3 — Traduzione e diffusione
Consuntivo e prospettive
- 14.45 **Gianpaolo Marcolongo** – Banca Popolare dell'Emilia Romagna
COBIT: sviluppo di software affidabile
- 15.15 **Francesco Mariani** – Selesta
Maturity Model: strumento di autoverifica dell'auditor
- 15.45 Pausa Caffè
- 16.00 **Francesco Santiloni** - Banca Monte Paschi
Andrea Pederiva – Deloitte Business Consulting
COBIT: base di conoscenza per il sistema dei controlli interni nelle Banche
- 16.30 **Bruno Ghisu** – Banco di Sardegna
COBIT e Disaster Recovery
- 17.00 Dibattito con gli oratori
- 17.30 Conclusione dell'incontro a cura del chairman
- 17.45 Termine dei lavori

Le presentazioni complete si trovano
sul sito www.aiea.it

Controlli Interni sui Sistemi Informativi

1. Le strategie IT devono essere approvate dal CDA
2. Le politiche, gli standard e i controlli sull'IT devono essere definiti e documentati
3. Le procedure di approvazione e acquisizione (su hw, sw e servizi anche in outsourcing) devono essere formalizzate; l'acquisizione deve assicurare la continuità del servizio
4. L'Internal Audit deve essere in grado di verificare l'adeguatezza dei controlli sull'IT
5. Gli ambienti di sviluppo e produzione devono essere separati

Controlli Interni sui Sistemi Informativi

6. Gli accessi ai diversi ambienti devono essere disegnati tenuto conto di rischi di frode e infedeltà del dipendente
7. L'Internal Audit deve controllare le violazioni alla sicurezza logica
8. Deve essere assicurata la sicurezza fisica dei dati e la protezione dei sistemi da eventi esterni
9. Un piano di emergenza deve assicurare la continuità delle operazioni vitali e il ritorno alla normalità in tempi ragionevoli



Auditing con lo standard BS7799

Sessione di studio di Milano— 06.12.2002



Starhotel Rosa — Sala “Rossini”
Via Pattari, 5 - Milano

PROGRAMMA

- 14.00 Introduzione dei lavori da parte di **Arturo Salvatici** (Consigliere AIEA)
- 14.15 **Emanuele Boati** - UniCredito Italiano
Gruppo di ricerca: Auditing con lo standard BS7799
Consuntivo e prospettive
- 15.00 **Angelo Piazzolla** – DNV
Dalla sicurezza informatica alla sicurezza delle informazioni: lo standard BS7799
- 16.00 Pausa Caffè
- 16.00 **Eugenio Marogna** – SIA
Certificazione BS7799 - L'esperienza della prima società italiana certificata: SIA
- 17.00 Dibattito con gli oratori
- 17.30 Conclusione dell'incontro a cura del chairman
- 17.45 Termine dei lavori

Il Gruppo di Ricerca: Auditing con lo standard BS7799:
Massimiliano Rinalducci, Claudio Bacchieri, Emanuele Boati





Mario Grasso

SCRIVERE PER IL WEB

Franco Angeli, pagg. 137, 14€
 Segnalato da Bancaforte

Lettere

“Sotto molti punti di vista la scrittura è la competenza di base, trasversale ad ogni altra attività. Essa ha un ruolo fondamentale nel processo di comunicazione, reso più articolato dall'avvento di Internet. Essere in grado di comunicare via web può essere un obiettivo di lavoro, un obbligo scolastico, una necessità per affari o un interesse personale. Qualunque sia la motivazione che spinge a comunicare via Internet, la scrittura on line richiede un adeguamento delle competenze che non è solo tecnico. Questo vale soprattutto per la scrittura funzionale, in uso negli ambienti di lavoro. Non vi è imprenditore, manager, professionista o funzionario che possa permettersi di sapere comunicare per iscritto. Oggi il modo di scrivere fa i conti con il verbo “ciccare”, con lo schermo che ha regole diverse dalla carta stampata. Scrivere sul web e per il web significa due cose diverse, sono necessarie due diverse cassette degli attrezzi, anche se questa distinzione non durerà ancora per molto. Attenzione però a non lasciarsi ingannare dalla lusinga tecnologica e ricordarsi che il mezzo non è il messaggio. Con la multimedialità, la comunicazione si fa più scoppiettante, più godibile ma anche più

pericoloso perché c'è il rischio di confondere lo strumento con il contenuto che esso è chiamato a veicolare”.

(recensione apparsa su Bancaforte)

Un libro gradevole, di veloce lettura sia perché le pagine non sono molte sia perché l'autore scrive in modo semplice e non indulge in esibizioni culturali di chi se la racconta addosso. Il fluire del messaggio è piano e ben articolato e lo si può intuire dai titoli dei principali capitoli: Costruire un testo, Vestire un testo, Valorizzare il testo, Anche l'occhio vuole la sua parte, Animare il testo, La cassetta degli attrezzi...

In verità il libro è rivolto ai web master ma molto può essere apprezzato da un normale utilizzatore di e-mail.

A tale riguardo alcune annotazioni sulle regole grammaticali, sull'uso dei termini inglesi, sull'utilizzo appropriato dei segni d'interpunzione e sulle netiquette mi sono apparse pregevoli.

Il libro forse non vincerà il premio Strega, probabilmente ci sarà in giro di meglio e di più approfondito e quindi non mi sento di sollecitarvi a correre senza perdere tempo dal libraio per acquistarne due copie (la seconda per il backup), volevo solo condividere con voi le mie impressioni.

Silvano Ongetta

Larry Hubbard, CIA, CPA, CCSA

CONTROL SELF ASSESSMENT: A PRACTICAL GUIDE

Institute of Internal Auditor,
 pagg. 105, 64sterline ingl., 2000

Tra i testi consigliati per approfondire il Control self Assessment primo fra tutti vi è questo libro scritto da uno dei più esperti conoscitori della materia. Larry Hubbard ha lavorato sia come consulente che come dipendente di società di produzione, ha potuto quindi studiare e utilizzare operativamente queste tecniche che continua a divulgare nell'ambito dell'IIA dove è frequentemente sia relatore che leader di corsi di formazione. Ha un vasto background in contabilità, auditing e finanza; le sue specializzazioni sono sul control self-assessment, sul pensiero creativo, sulla tecnologia informatica, sull'operational auditing, sul risk assessment.

Un autore eccezionale per un testo semplice e completo che passa in rassegna i diversi approcci al CSA. Mantenendosi più a livello generale che tecnico fornisce una visione d'insieme del CSA e si focalizza sui fattori che influenzano un CSA di successo. Partendo dal presupposto che il metodo del CSA sarà il principale approccio dei prossimi anni sponsorizzato dall'IIA, l'autore nell'esposizione privilegia questo approccio.

Riportiamo subito alcune conclusioni alle quali perviene l'autore:

1. l'implementazione del CSA è differente caso per caso anche nella stessa organizzazione,
2. non c'è una sola “best practice” che deve essere seguita nell'applicazione del CSA,
3. non c'è una sola strada, una unica modalità, per utilizzare con successo il CSA,
4. a mano a mano che le organizzazioni crescono, da un punto di vista di cultura aziendale, il CSA diviene sempre più utile e a volte l'indispensabile strumento di auditing.

I capitoli del libro approfondiscono la definizione di CSA, i diversi approcci al CSA, gli elementi centrali della metodo-

CONTROL SELF ASSESSMENT: A PRACTICAL GUIDE

(Continua da pagina 16)

logia (obiettivi aziendali, rischi di non raggiungerli, controlli che mitigano questi rischi), l'approccio del "workshop facilitato" che è considerato tra i più efficaci, le due fasi più critiche della realizzazione dell'intervento e della raccolta e presentazione dei risultati.

Hubbard affronta un argomento importante che ripropongo quale esempio della concretezza ed utilità del libro. Si tratta della validazione dei risultati del Control Self Assessment gestito dall'auditor-facilitatore. Il "workshop" permette di raccogliere molte informazioni, la maggior parte comunicate verbalmente, e pertanto con una validità generalmente inferiore ad altre evidenze quali il test, l'osservazione o la conferma indipendente. Di norma, ed in particolare se le informazioni debbono essere usate per un audit, l'auditor deve decidere il metodo e l'ampiezza dell'attività di test obbligatoriamente richiesta per confermare le affermazioni individuate attraverso il workshop.

Questo è solo un esempio di come l'autore coniuga il rigore del metodo con la guida pratica alla applicazione di questa metodologia. Buona lettura, o buon studio.

Orillo Narduzzo



Auguri di Buon Natale e di importanti traguardi professionali nel Nuovo Anno a tutti gli amici soci e alle loro famiglie dal Consiglio Direttivo dell'AIEA.

Stiamo aggiornando l'anagrafe dei soci, avete ricevuto un modulo con i dati e la richiesta di segnalare eventuali variazioni; se non lo avete vi ricordiamo di mandarci un fax o un e-mail con i dati aggiornati per potervi meglio servire.

I dati richiesti sono:

CODICE SOCIO AIEA, CODICE SOCIO ISACA,
COGNOME, NOME, DATA DI NASCITA

TITOLO, CERTIF. CISA, DATA CERTIF

TELEFONO, FAX, CELLULARE, E-MAIL

AZIENDA, SERVIZIO, INDIRIZZO, C.A.P., CITTÀ

RICORDATI DI COMUNICARCI GLI ESTREMI DEL BONIFICO RELATIVO AL RINNOVO DELLA TUA ISCRIZIONE.

INDICE GENERALE

2001-2002



TITOLO	AUTORE	NUMERO
ISACA/AIEA		
ASSOCIATI!	E. Toffanin	2002/12
New CISM Certification	Redazione	2002/12
COBIT News	Redazione	2002/12
Impressioni di un associato	L. Carrozzi	2002/12
ISACA e la Commissione Europea	E. Toffanin	2002/09
Consuntivo 2002	S. Ongetta	2002/09
New CISM certification	Redazione	2002/09
Adding a dimension to CobIT	Redazione	2002/09
Two New IT Governance publications	Redazione	2002/09
Continuing Education Policy	ISACA/AIEA	2002/09
CISA 2002	L. Pertile	2002/09
XVI Convegno: IT Governance	S. Ongetta	2002/06
Assemblea Annuale	S. Ongetta	2002/06
XVI Convegno: IT Governance – Presentazione	Redazione	2002/06
Cisa Exam	A. Rodaro	2002/06
Stiamo lavorando per voi e con voi!	D. Rosa	2002/03
Leadership professionale	Redazione	2002/03
Convegno Nazionale – Programma	Redazione	2002/03
Il Codice Etico ISACA	AIEA	2002/03
Assemblea 2	S. Ongetta	2001/12
Risultati dell'esame CISA 2001	A. Rodaro	2001/12
Assemblea degli associati	Redazione	2001/12
Conferenza Internazionale di Parigi	C. De Santis	2001/12
10° Anniversario esame CISA in Italia	Redazione	2001/12
Indirizzato ai soci presenti al Convegno e non	S. Ongetta	2001/07
Proposta di un nuovo statuto	Ongetta, Toffanin	2001/07
Nuovo Consiglio Direttivo dell'Associazione	Redazione	2001/07
SPECIALE XV Convegno Nazionale	Redazione	2001/07
SPECIALE STATUTO	Redazione	2001/07
CISA: qualifica professionale prestigiosa	A, Rodaro	2001/07
Articoli		
La sicurezza del settore pubblico negli Stati Uniti	A. Salvatici	2002/09
IT Governance – Linee guida	P. Schiavon	2002/06
Documenti e firme elettroniche	A. Salvatici	2002/06
Sicurezza informatica	A. Salvatici	2001/12
Una nuova sfida: l'IT Governance	O. Narduzzo	2001/12
Gruppi di ricerca		
Sistemi di Gestione della Sicurezza delle Informazioni	L. Carrozzi	2002/12
Penetration test dal punto di vista dell'auditor	GL. Moxedano	2002/09
COBIT 3: traduzione e diffusione	O. Narduzzo	2002/03
Gruppi di ricerca	Redazione	2001/12



INDICE GENERALE 2001-2002

(Continua da pagina 18)

TITOLO	AUTORE	NUMERO
Sessioni di studio		
Milano 6.12.2002 - Auditing con lo standard BS7799		2002/12
Roma 3.12.2002 - COBIT 3: traduzione e diffusione		2002/12
Roma 3.12.2002 - IS Auditing delle architetture Open Source		2002/12
Torino 7.11.2002 - Security Management		2002/12
Milano 26.9.2002 - Rischio e Organizzazione		2002/09
Roma 2.10.2002 - Auditing e Sicurezza		2002/09
Milano 14.6.2002 - La continuità del business		2002/06
Roma 2.7.2002 - ICT security, l'analisi del rischio, il Disaster Recovery		2002/06
Roma 21.11.2001 - Frodi aziendali: l'auditing, la sicurezza, il forensics		2001/12 2002/03
Milano 12.12.2001 - Come trovare un approccio metodologico a nuovi e vecchi problemi		2001/12 2002/03
Padova 15.2.2002 - Auditing: evoluzione dei sistemi di controllo per l'IT Governance		2002/03
Roma 20.3.2002 - Il trattamento dei dati personali nuove norme, nuove opportunità		2002/03
Milano 12.10.2001 - L'auditing di sicurezza. Esperienze di CobiT		2001/12
Standard ISACA		
Internet Banking	R. Griselli	2002/06
Task Force a supporto	S. Silvestri	2002/06
Audit dei sistemi ERP	A. Schiavi	2002/06
Control Risk Self Assessment	O. Narduzzo	2002/06
Letture		
CONTROL SELF ASSESSMENT: A PRACTICAL GUIDE di Larry Hubbard, recensione O. Narduzzo		2002/12
SCRIVERE PER IL WEB di Mario Grasso, recensione S. Ongetta		2002/12
CONTROL FRAMEWORKS and SELF ASSESSMENT di David McNamee, recensione O. Narduzzo		2002/09
ON-LINE BANKING - Soluzioni tecnologiche multicanale di A. Carignani e M. Sorrentino, recensione O. Narduzzo		2002/03
IL RISCHIO E LE BANCHE - La revisione dell'Accordo di Basilea: implicazioni per banche e imprese di Rainer Masera, recensione O. Narduzzo		2002/03
COPERNICO - Un approccio innovativo per la Direzione dei Sistemi Informativi in azienda di Claudio Antonelli, recensione O. Narduzzo		2002/03
Tesi		
L'auditing dei sistemi informativi con la metodologia COBIT 3. Il Caso Olivetti.	G. Saitta	2002/06
Sistemi di sicurezza e auditing delle basi dati nelle tecnologie dell'informazione.	E. Beato	2002/03

AIEA**Associazione Italiana Information Systems Auditors****ISACA****Information Systems Audit and Control Association****Capitolo di Milano**

20131 Milano

Via Accademia, 19

Tel. +39.02.70608405

Fax +39.02.700507644

E-mail: aiea@aiea.it

P.IVA 10899720154

InfoAIEADicembre 2002,
numero in attesa di registrazione

Responsabile: Silvano Ongetta

Redazione: Orillo Narduzzo

Hanno collaborato:

Luigi Carrozzi, Orillo Narduzzo,
Silvano Ongetta, Enzo Toffanin

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,

SCRIVETEICI!!E-mail : infoaiea@aiea.it, aiea@aiea.it

Sede: AIEA,

Redazione InfoAIEA

Via Accademia, 19

20131 Milano

Consiglio Nazionale 2001-2003

Presidente: Silvano Ongetta
Vice presidenti: Donatella Rosa,
Francesco Galli
Segretario: Enzo Toffanin
Tesoriere: Aureliana Radaelli

Consiglieri

Emanuele Boati , Agatino Grillo
Gianluigi Moxedano, Orillo Narduzzo
Angelo Rodaro , Arturo Salvatici

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 Continuing Education.

Gli articoli scientifici o le comunicazioni di esperienze saranno premiati con una pubblicazione tecnica.