ISACA Roma

NEWS

Email: isacaroma@isacaroma.it. Web: www.isacaroma.it/newsletter Giugno 2004, numero 3

Sommario

Messaggio del Presidente

L'importanza di chiamarsi CISA

Parafrasando Oscar Wilde, il titolo del mio editoriale di questo mese si riferisce all'esame di certificazione CISA che ha avuto luogo, in contemporanea in tutto il mondo, lo scorso 12 giugno. Lascio i dettagli su come si è svolto l'esame ai gentili associati che ci hanno inviato le loro riflessioni che pubblichiamo in altra parte della newsletter. Vorrei invece, in queste poche righe, offrire qualche spunto per la riflessione sull'importanza che le certificazioni CISA e CISM stanno assumendo a livello mondiale. In primo luogo alcuni dati: i candidati sono stati ben 14.000 per l'esame CISA e 700 per l'esame CISM (che, ricordiamolo, è giunto solo al secondo anno di vita); in Italia i candidati CISA 2004 sono stati più di 100 di cui circa la metà si sono presentati a Roma; le persone che hanno già ottenuto la certificazione negli scorsi anni sono circa 35.000 per il CISA e circa 5.000 per il CISM. Come si vede numeri di tutto rispetto che indicano l'importanza di "chiamarsi" CISA (e CISM) per chi opera in questo settore.

Proprio in ragione dell'importanza e delle specificità di ciascuna certificazione, il nostro Capitolo, sulla base delle indicazioni ricevute dall'Isaca International, dividerà le sue attività in quelle specifiche di Assurance, per i CISA, e Security, per i CISM, con l'organizzazione di giornate di studio specifiche, progetti di ricerca, ecc.
Infine alcune note di servizio:

- ricordo a tutti gli associati certificati che occorre "mantenere" la certificazione sia con il pagamento della relativa fee che con l'effettuazione delle ore di Continuing Professional Education (CPE);
- i nuovi associati che si iscrivono ad ISACA dopo il primo giugno (ma entro il 31 agosto) hanno uno sconto del 50% sulla quota dovuta ad Isaca International.

Un ringraziamento, infine, a tutti gli associati (e non) che hanno partecipato al convegno del Capitolo dello scorso 3 giugno (sul quale riferiamo in altra parte della newsletter) ed in particolare agli amici che hanno contribuito all'organizzazione dell'evento.

A tutti un cordiale saluto.

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

President's corner - The importance of being CISA - President's Message

By quoting Oscar Wilde, the title of this month column refers to the CISA exam which was offered, anywhere in the world, on June 12th. I leave comments and impressions regarding how the examination was conducted to our kind members, published elsewhere in this newsletter. Instead, I would in these few lines discuss the importance that the CISA and CISM designations are continuous acquiring at global level. First some data: candidates for this year exam were about 14.000 for the CISA exam and 700 for CISM (which is only two years old). Candidates for CISA 2004 in Italy were over 100, half of them sat in Rome;

persons who gained the designation in the previous years are about 35.000 for CISA and 5.000 for CISM. Because of the importance and specificity of each certification, our Chapter, following the directives received from Isaca International, will split its activities in those specific of Assurance, for CISAs, and IS Security, for CISMs, by organising session of study, research projects, etc

Last some reminders:

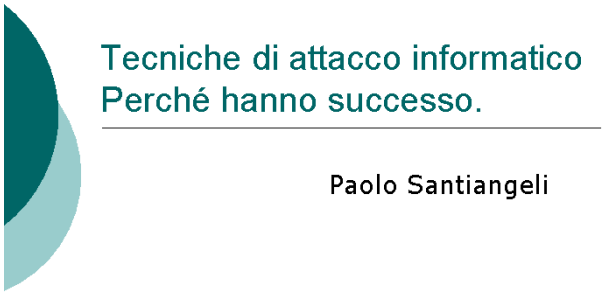
- The certification must maintained both paying the maintenance fee and by submitting the Continuing Professional Education (CPE) hours;
- People who decide to become members after June 1st and before August 31st receive 50% discount of Isaca International fee.

I would also thank all members and non-members who participated to the Chapter meeting held in Rome on June 3rd, and in particular to those who contributed to event organisation.

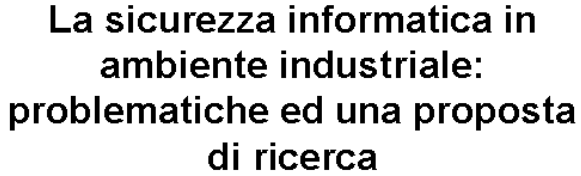
Iniziative del capitolo

Convegno del 3 giugno

Il 3 giugno si è tenuto, presso il centro Vojta, via Pincherle 186, il secondo convegno nazionale del Capitolo di Roma di ISACA.
Le slide delle presentazioni sono disponibili presso il sito del Capitolo. Di seguito una breve sintesi degli interventi.
Il primo intervento, a cura di Paolo Santiangeli, ha riguardato gli attacchi informatici e si è soffermato sull'importanza del "fattore umano"; la maggior parte degli attacchi sfruttano debolezze imputabili al comportamento non corretto degli utilizzatori dei SI; in particolar modo spesso le password sono troppo deboli e facilmente individuabili. Interessante la proposte per costruire una password robusta sfruttando versi poetici e sostituendo alcune lettere con numeri per cui, ad esempio, da "O Luce Etterna Che Sola In Te Sidi" si ottiene 0lEcS1Ts.



Il secondo intervento è stato di Glauco Bertocchi ed ha riguardato le problematiche della sicurezza informatica in ambiente industriale. È stata presentata, a cura di ISPELS - Istituto Superiore per la Prevenzione e la Sicurezza del Lavoro, una ricerca per l'individuazione di una metodologia per l'analisi del rischio dei sistemi informatici utilizzati per monitoraggio e controllo di impianti industriali(SIMC) e per la classificazione dei relativi criteri di sicurezza informatica.



L'ultimo intervento ha avuto come oggetto la presentazione del "Centro Ricerche sulla Sicurezza", un punto di riferimento indipendente da prodotti e fornitori per la valutazione dei sistemi e dei prodotti informatici, e per lo sviluppo e analisi delle metodologie di realizzazione dei piani di sicurezza e di valutazione.

Il Centro nasce in collaborazione con l'Information Systems Audit and Control Association (ISACA), The Institute of Internal Auditors (IIA), Università ed altri Centri di ricerche.

ISACA Roma SPQR

SPQR (Speciale Quaderni di Ricerca) è la nuova iniziativa di ISACA Roma; essa consiste nella pubblicazione, ogni sei mesi circa, di un numero

speciale della newsletter dedicata ad approfondimenti verticali sui temi della assurance e security.
Il primo quaderno SPQR è dedicato al tema "protezione delle infrastrutture critiche informatiche", un argomento ormai di attualità anche in Italia dopo che il Ministero dell'Innovazione Tecnologia ha costituito uno specifico gruppo di lavoro in tale senso.
La stessa Assemblea generale dell'ONU ha approvato una risoluzione (58/199) che incoraggia le iniziativa nazionali ed internazionali di ricerca e sviluppo per la "creazione di una cultura diffusa della sicurezza informatica e sulla protezione delle infrastrutture informatiche critiche".
"Molte delle reti essenziali per la vita del Paese, come quelle idriche, energetiche, dei trasporti e delle telecomunicazioni, ma anche quelle finanziarie, nonché la stessa Pubblica Amministrazione hanno sofisticati apparati informatici per il loro controllo e la loro gestione", ha detto il Ministro Stanca, "e la distruzione o temporanea indisponibilità di tali risorse strategiche può avere effetti negativi sull'economia, sulla vita quotidiana dei cittadini e sulle capacità di difesa del Paese. Per questo l'incremento della loro protezione, nel momento di grave incertezza internazionale che stiamo attraversando, è una priorità non più differibile".

MINISTRO PER L'INNOVAZIONE

Chiunque volesse proporre un articolo per SPQR è pregato di inviare i propri contributi a isacaroma@isacaroma.it (soggetto: SPQR) entro il prossimo 31 agosto.
Il primo SPQR sarà reso pubblico entro il 30 settembre.

C(ertification)-DAY resoconto, semiserio, dell'esame CISA del 12 giugno

Abbiamo chiesto ai colleghi che hanno sostenuto l'esame CISA del 12 giugno scorso ci mandarci le loro osservazioni sull'evento su temi quali l'atmosfera che si respirava, la difficoltà delle domande, la qualità della traduzione, eccetera.
Ecco una breve sintesi dei commenti ricevuti (ci scusiamo in anticipo per aver dovuto sintetizzare i contributi).

CISA® CERTIFIED INFORMATION SYSTEMS AUDITOR

Tutti si sono lamentati dell'aspetto logistico inteso come sedia e banco:

- i posti erano costituiti da una specie di trespoli; problematico tenere in equilibrio il fascicolo delle domande ed il foglio delle risposte (Ugo);
- le sedie erano scomode, per gli esaminandi sarebbe preferibile disporre di banchi normali, ove appoggiare due fogli (Enrico).

Tutto sommato, la qualità delle traduzione e delle domande è stato buono:

- le domande mi sono sembrate piuttosto difficili, alcune per il senso generale della domanda, altre perché le risposte erano molto simili; solamente 5-6 domande erano quasi uguali a quelle dei test (Fabrizio);
- la traduzione, tutto sommato è stata molto buona (Gian Luca);
- i timori sulla traduzione si sono rivelati infondati (Enrico);
- La preparazione delle domande sembra sia fatta veramente da persone estranee alle problematiche (Ugo)

Critiche varie e consigli:

- tutto l'esame è fortemente orientato ad una metodologia operativa molto "americana"; non sempre è facile l' individuazione puntuale dei ruoli e dei compiti assegnati ai vari ruoli in un contesto lavorativo "italiano" (Ugo);
- conviene imparare a memoria (o quasi) il libro (Ugo);

A tutti in bocca al lupo!

ISACA International News

Webcast

Le webcast sono presentazioni online (dal sito www.ISACA.org/webcasts) sui principali temi di Assurance e Security. Frequentare (virtualmente) le webcast permette, inoltre, di guadagnare punti CPE.
Al momento sono disponibili, le seguenti webcast:

- Auditors and Quality Assurance: Achieving Enterprise Security through Collaboration

- Introduction to Information Security Architecture
- How to Carry Out a Strategic COBIT Based IT Risk Assessment
- An Overview of Threat and Vulnerability Analysis
- IT Risk Management: A Case Study of E-commerce Availability
- The IT Balanced Scorecard

IT Control Objectives for Sarbanes-Oxley

È disponibile la nuova versione degli "IT Control Objectives for Sarbanes-Oxley"
Download:
http://www.isaca.org/Template.cfm?Section=home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=12406

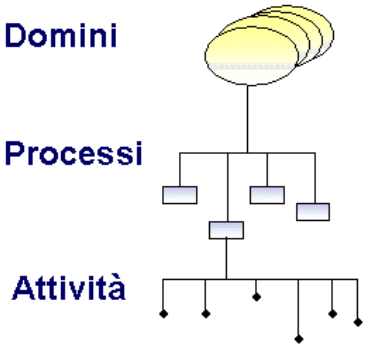
Approfondimenti: Introduzione a COBIT

(a cura di Agatino Grillo)

(versione ridotta di un articolo pubblicato da "*Upgrade: The European Journal for the Informatics Professional*", http://www.upgrade-cepis.org, Vol. IV, No. 6, December 2003; versione in inglese in: http://www.upgrade-cepis.org/issues/2003/6/up4-6Grillo.pdf , versione in italiano in: http://apache.tecnoteca.it/upgradepdf/it-up4-6Grillo.pdf)

Overview

COBIT (Control Objectives for Information and related Technology) giunto alla terza edizione, è un approccio alla verifica dei sistemi informativi sviluppato per permettere la comprensione all'Alta Direzione, all'audit interno e alle funzioni di controllo della natura dei controlli e delle potenziali criticità esistenti.
COBIT si basa su un framework process-based basato su tre livelli logici di classificazione (Attività, Processi e Domini) così da permettere l'individuazione per ciascuno livello delle risorse IT da sottoporre a controllo e dei "proprietari" di tali risorse.



(figura: fonte ISACA)

La metodologia si compone di un insieme di 34 obiettivi di controllo di alto livello, uno per ciascuno dei principali processi dell'IT, e di circa 300 obiettivi di controllo dettagliati; gli obiettivi di controllo sono raggruppati in quattro domini:

- Organizzazione e pianificazione (*Planning & Organisation*);
- Acquisizione e realizzazione (*Acquisition & Implementation*);
- Erogazione del servizio e assistenza (*Delivery & Support*);
- Monitoraggio (*Monitoring*).

CMM

La determinazione del livello di rispetto degli obiettivi di controllo può essere effettuato mediante un self-assessment o un review indipendente (IS Auditing), utilizzando una scala di valutazione dei controlli IT previsti che si rifà al Capability Maturity Model (CMM) con valori che vanno tra 0 (non esistente) a 5 (ottimizzato).
Il CMM è un modello per la valutazione della "maturità" dei processi IT aziendali sviluppato dal SEI (Software Engineering Institute), www.sei.cmu.edu
COBIT fornisce, inoltre, tool specifici quali:

- Misuratori di performance;
- List dei fattori critici di successo comprese le principali best practices per ogni processo IT;
- Maturity models per assistere nel benchmarking e decision-making per le successive attività di capability improvements.

Si noti che la versione inglese di COBIT è liberamente scaricabile (ad esclusione delle Audit Guidelines) dal sito ISACA in: http://www.isaca.org/Template.cfm?Section=Obtain_COBIT previa registrazione gratuita. E' inoltre possibile acquistare da ISACA la versione cartacea anche in

italiano (traduzione a cura di AIEA, capitolo di Milano di Isaca, www.aiea.it).

Obiettivi di controllo

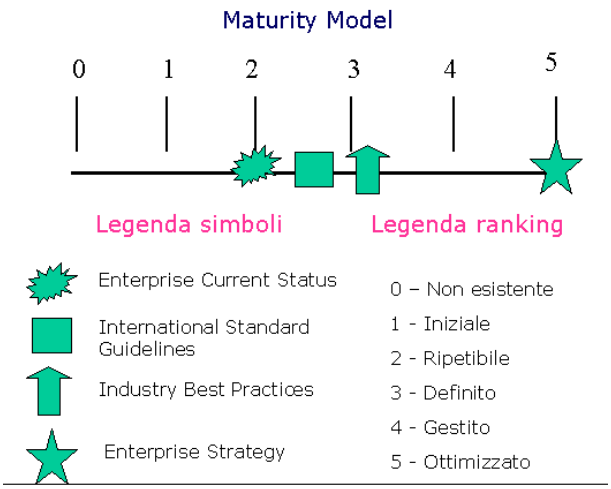
Di seguito sono riepilogati i 34 Obiettivi di controllo di alto livello di COBIT (traduzione italiana a cura dell'autore).

Organizzazione e pianificazione		
PO1	Definizione di un piano IT strategico	*Define a strategic IT plan*
PO2	Definizione delle architecture informatiche	*Define the information architecture*
PO3	Determinazione delle direzioni tecnologiche	*Determine technological direction*
PO4	Definizione dell'organizzazione IT	*Define the IT organisation and relationships*
PO5	Gestione degli investmenti IT	*Manage the IT investment*
PO6	Comunicazione al management degli obiettivi strategici	*Communicate management aims and direction*
PO7	Gestione delle risorse umane	*Manage human resources*
PO8	Assicurare il rispetto dei requisiti esterni	*Ensure compliance with external requirements*
PO9	Risk Assessment	*Assess risks*
PO10	Project Management	*Manage projects*
PO11	Gestione della qualità	*Manage quality*

Acquisizione e realizzazione		
AI1	Identificazione delle soluzioni automatizzate	*Identify automated solutions*
AI2	Acquisizione e manutenzione delle applicazioni software	*Acquire and maintain application software*
AI3	Acquisizione e manutenzione della infrastruttura tecnologica	*Acquire and maintain technology infrastructure*
AI4	Sviluppo e manutenzione delle procedure	*Develop and maintain procedures*
AI5	Installazione e certificazione dei sistemi	*Install and accredit systems*
AI6	Ch'ange Management	*Manage changes*

Erogazione del servizio e assistenza		
DS1	Definizione e gestione dei Service Level Agreement (SLA)	*Define and manage service levels*
DS2	Gestione delle terze parti	*Manage third-party services*
DS3	Gestione delle performance e capacità	*Manage performance and capacity*
DS4	Assicurare la continuità del servizio	*Ensure continuous service*
DS5	Assicurare la sicurezza dei sistemi	*Ensure systems security*
DS6	Identificare ed attribuire i costi	*Identify and allocate costs*
DS7	Training e formazione degli utenti	*Educate and train users*
DS8	Assistenza e informazione dei clienti	*Assist and advise customers*
DS9	Gestione delle configurazioni	*Manage the configuration*
DS10	Gestione degli incidenti	*Manage problems and incidents*
DS11	Gestione dei dati	*Manage data*
DS12	Gestione delle facility	*Manage facilities*
DS13	Gestione delle operazioni	*Manage operations*

Monitoraggio		
M1	Monitoraggio dei processi	*Monitor the processes*
M2	Assessment dell'adeguatezza dei controlli interni	*Assess internal control adequacy*
M3	Ottenere una assurance indipendente	*Obtain independent assurance*
M4	Fornire un audit indipendente	*Provide for independent audit*



(figura: fonte ISACA)

English abstract

Control Objectives for Information and related Technology (COBIT), now in its 3rd edition, is a framework developed by ISACA that helps organizations balance their risks vs. returns in an IT environment and ensure alignment of business needs with overall IT processes.

The COBIT mission is to research, develop, publicise and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors.

Most of the components of COBIT are available in open standard format, available for complimentary download by the public.

COBIT is a business orientated framework that identifies 34 information technology processes, grouped in 4 domains, and is supported by 318 detailed control objectives.

Each one of the 34 processes references IT resources, and the quality, fiduciary and security requirements for information.

Further, the COBIT Management Guidelines are generic and action orientated for the purpose of addressing the following types of management concerns:

1) Performance measurement – What are the indicators of good performance?
2) IT control profiling – What is important? What are the critical success factors for control?
3) Awareness – What are the risks of not achieving our objectives?
4) Benchmarking – What do others do? How do we measure and compare?

For each of the 34 COBIT IT processes, there is an incremental measurement scale based on a rating of 0 through 5. The scale is associated with generic qualitative maturity model descriptions ranging from "Non Existent" to "Optimised" derived by the "Capability Maturity Models®" of the Software Engineering Institute – SEI.

Whatever the model, the scales should not be too granular as that would render the system difficult to use and suggest a precision that is not justifiable.

In contrast, one should concentrate on maturity levels based on a set of conditions that can be unambiguously met.

Against levels developed for each of CobiT's 34 IT processes, management can map:

1) The current status of the organisation – where the organization is today;
2) The current status of (best-in-class in) the industry – the comparison;
3) The current status of international standard guidelines –additional comparison;
4) The organisation's strategy for improvement – where the organisation wants to be.