

COBIT 4.0[©]

Dalla sua iniziale apparizione nel 1992, COBIT si è sviluppato in un modello di controllo per la *governance* dell'IT. Ormai universalmente accettato, COBIT e i suoi prodotti di supporto forniscono una guida ad ampio spettro e un supporto a molte imprese ed istituzioni in tutto il mondo.

Nel 2002, 10 anni dopo l'inizio del progetto COBIT e avendo alle spalle la produzione di tre versioni, fu concepita una strategia per assicurare la sostenibilità degli ulteriori sviluppi di COBIT. Uno degli obiettivi chiave di questa strategia era quello di fornire un quadro di riferimento che fosse mantenuto ed aggiornato con continuità in modo da soddisfare le esigenze di un IT in rapido cambiamento, di un agevole ritorno da parte degli utenti e di un miglioramento continuo.

Questa strategia ha portato nel 2005 alla pubblicazione della quarta versione di di COBIT.

(da pagina 2 la descrizione delle innovazioni contenute in COBIT 4.0)

FAQ: COBIT 4.0[©]

1. Qual è la storia del modello COBIT?
2. Quali cambiamenti sono avvenuti nel business per stimolare un aggiornamento di COBIT?
3. Quali componenti di COBIT sono stati modificati nella nuova versione 4.0?
4. Dove posso trovare COBIT 4.0?

Le risposte a queste e altre domande frequenti per conoscere meglio COBIT 4.0 a pagina 10.

ITGI: Val IT series

Creare valore per le aziende. Una delle priorità è la governance degli investimenti. L'IT Governance Institute ha appena pubblicato tre fascicoli su questo argomento.

*Enterprise Value: Governance of IT Investments,
The Val IT Framework*

Puoi consultare queste pubblicazioni sul sito www.itgi.org

In questo numero

Uno dei punti di forza di ISACA e ITGI è COBIT: il modello per l'IT Governance. Lo scorso autunno è stata pubblicata la versione 4.0. In questo numero vi presentiamo le principali innovazioni attraverso l'articolo di Hardy e Guldentops tradotto da Marchiori. Altri chiarimenti ve li forniamo attraverso la traduzione delle faq. La comprensione degli adeguamenti e delle novità consentirà alle organizzazioni che usano questo modello di dare continuità all'investimento effettuato e di sfruttare le nuove potenzialità.

E' oggi possibile frequentare un corso online su COBIT e sostenere un esame che certifichi la conoscenza di base del modello. A pagina 26 trovate i riferimenti a questo corso e alle pubblicazioni dell'ITGI sulla governance degli investimenti IT.

L'audit dei Sistemi di Gestione della Qualità si occupa del sistema informativo che lo supporta? Ce ne parla Bianconi del SINCERT.

Share your knowledge. (O.N.)



Sommario: numero 1 del 2006

COBIT 4.0: The New Face of COBIT [©] <i>di G. Hardy e E. Guldentops</i>	2
Le FAQ di COBIT 4.0	10
L'Audit del Sistema di Gestione per la Qualità: un grande assente il Sistema Informativo <i>di R. Bianconi</i>	18
Recensione di "OS/390—z/OS: Security, Audit and Control Features" <i>a cura di E. Dona' e F. Gozzi</i>	24
COBIT [©] Foundation Course	26
Val IT	26
Sessioni di Studio	27

25 e 26 maggio 2006
XX Convegno
Nazionale AIEA
Verona

COBIT 4.0: The New Face of COBIT®

By Gary Hardy and Erik Guldentops, CISA, CISM
 INFORMATION SYSTEMS CONTROL JOURNAL,
 VOLUME 6, 2005

traduzione di Francesco Marchiori

Nel marzo 2005 la Commissione della Comunità Europea (CE) ha scelto il *Control Objectives for Information and related Technology (COBIT)* dell'IT Governance Institute (ITGI) come uno dei tre standard internazionali che le agenzie di pagamento connesse con il fondo monetario di garanzia agricolo europeo (FEAOG) devono utilizzare in materia di sicurezza informatica e di controllo.

L'esame e l'adozione da parte di un'istituzione così grande ed autorevole come la CE è l'evidenza tangibile di quanto COBIT è diffuso e di quanta strada ha fatto dai tempi del suo debutto più di dieci anni fa. Il quarto trimestre 2005 segnerà l'ultima evoluzione per questa importante metodologia, in quanto vedrà la luce l'ultima edizione, COBIT 4.0. Questo articolo sintetizza il contenuto attuale di COBIT e descrive in particolare le modifiche inserite nella nuova versione, i motivi per i quali sono state apportate e i benefici per gli utenti attuali e futuri.



Articolo tratto dal volume 6 del 2005 di Control Journal.

La necessità di un aggiornamento

Dalla sua iniziale apparizione nel 1992, COBIT si è sviluppato in una metodologia di controllo *de facto* per la *governance* dell'IT. Ormai universalmente accettato, COBIT e i suoi prodotti di supporto forniscono una guida ad ampio spettro e un supporto a molte imprese ed istituzioni in tutto il mondo. Poiché l'IT e la guida richiesta per gestirla efficacemente non stanno ferme, gli utenti di COBIT, specialmente quelli che hanno impegnato le loro organizzazioni ad adottare come quadro di riferimento il COBIT, si aspettano un supporto e un miglioramento continuo.

Nel 2002, 10 anni dopo l'inizio del progetto COBIT e avendo alle spalle la produzione di tre versioni, fu concepita una strategia per assicurare la sostenibilità degli ulteriori sviluppi di COBIT. Uno degli obiettivi chiave di questa strategia era quello di fornire un quadro di riferimento che fosse mantenuto ed aggiornato con continuità in modo da soddisfare le esigenze di un IT in rapido cambiamento, di un agevole ritorno da parte degli utenti e di un miglioramento continuo.

Nel 2003, con la funzione di *repository sempre aggiornato* di COBIT fu lanciato COBIT Online®, fornendo in tal modo un prodotto che poteva essere aggiornato con immediatezza e continuità ed era facilmente accessibile a tutti gli utenti di COBIT. Di volta in volta, in corrispondenza alla realizzazione degli aggiornamenti più importanti per rispondere ad evoluzioni significative, saranno prodotte anche nuove versioni PDF di COBIT stampabili e scaricabili da internet.

(Continua a pagina 3)

COBIT 4.0: The New Face of COBIT

(Continua da pagina 2)

Nei cinque anni da quando nel 2000 fu lanciata COBIT 3a edizione, ITGI ha condotto ricerche ad ampio raggio sulla governance dell'IT ed ha analizzato le osservazioni di chi utilizza COBIT in modo massiccio. Tutto ciò ha costituito la base per il progetto di aggiornamento di COBIT 4.0, iniziato nel 2004 e pronto per il rilascio a novembre 2005.

Modalità di sviluppo e manutenzione

Per un'organizzazione no profit come ITGI, trovare ed organizzare le risorse per supportare COBIT è una sfida immensa. Lo status indipendente di ITGI e il desiderio di promuovere una guida utile e disponibile senza vincoli sono anch'essi fattori unici che influenzano il modo in cui sono portati avanti i lavori.

Il Comitato Guida di COBIT, costituito da membri volontari di ISACA e da un gruppo di direzione con un piccolo budget, definisce e guida la strategia di COBIT e il processo di sviluppo. Esperti, provenienti dall'associazione ISACA da tutto il mondo e da imprese leader, costituiscono l'unico gruppo di supporto volontario a COBIT, che ora è cresciuto contando oltre cento esperti e sette gruppi di volontari sparsi in varie zone geografiche. Questa struttura pone COBIT su un livello privilegiato in quanto risorsa mantenuta in modo attivo da utenti esperti di tutte le parti del mondo. Operando con efficienza ed obiettività in sessioni di lavoro focalizzate allo sviluppo senza pressioni od orientamenti commerciali, ITGI può sviluppare COBIT con grande efficacia. Di volta in volta, specifici lavori di sviluppo sono finanziati ed eseguiti da consulenti o istituzioni accademiche. Il Quartiere Generale di ISACA fornisce i servizi di supporto per trasformare il materiale grezzo in prodotti finiti e si occupa della loro diffusione una volta nati.

COBIT 4.0 è un programma complesso costituito da molti progetti interconnessi. E' stato un impegno di due anni con numerose sessioni di lavoro e specifiche attività di sviluppo, con la supervisione di un gruppo di coordinamento. E' ora all'opera un superbo e crescente insieme di persone dedicate, impegnate a sostenere l'evoluzione di COBIT anche per il futuro.

La risposta ad un ambiente e ad un'utenza che cambia

Enormi cambiamenti sono occorsi nell'IT dal 1992, con l'espansione di internet e la globalizzazione che determinano la totale dipendenza dall'IT per l'operatività aziendale e il raggiungimento degli obiettivi strategici. Nei cinque anni passati, c'è stato anche un focus senza eguali su corporate governance, sistema di regole più stretto e nuove responsabilità per i dirigenti delle società. L'impatto sull'IT è stato un focus molto più concentrato su direzione e performance dell'IT e accresciuto interesse per la governance dell'IT. L'interesse per COBIT è evoluto dal suo uso iniziale come strumento per l'auditor a quadro di riferimento per la governance dell'IT e per il miglioramento della gestione e dei controlli dell'IT.

Queste evoluzioni hanno rappresentato nuove sfide cui COBIT 4.0 ha tentato di rispondere:

Focus crescente sulla gestione dell'IT – Fornire una guida per la gestione ed il controllo dell'IT utile per l'ordinario ambiente operativo IT.

Un'utenza impegnata nell'assurance che è sempre più diversificata – Soddisfare le esigenze di auditor, legislatori, esperti di sicurezza ed altri coinvolti nel fornire garanzia sulle prestazioni dell'IT in molte differenti circostanze.

Focus maggiore sulla governance al livello del consiglio d'amministrazione – Assicurare che c'è un sufficiente focus sull'azienda e meccanismi per allineare la gestione ed il controllo degli obiettivi IT alle necessità dell'impresa.

Accresciuta maturità delle best practice e degli standard IT – Assicurare che, anche se le imprese adottano

(Continua a pagina 4)

COBIT 4.0: The New Face of COBIT

(Continua da pagina 3)

sempre più metodologie specialistiche come ITIL® e ISO 17799, COBIT può essere usato come integratore e quadro di riferimento che fa da ampio ombrello superiore e continua ad essere considerato una guida altamente credibile e pratica per il controllo generale dell'IT.

Utilizzo integrato da parte di tre categorie principali: direzione, personale IT e auditor – Assicurare che la struttura, la presentazione e il linguaggio usati offrano una più facile comprensione ed applicazione da parte dei manager come pure dei tecnici e dei professionisti.

Attenzione alle regole e alla conformità – Garantire che COBIT copra l'intero ambito della governance IT e mostrare come esso si mappa sui domini della governance IT e sul riferimento COSO. Assicurare che esso possa continuare ad essere visto come la metodologia *de facto* del controllo dell'IT per la governance dell'IT.

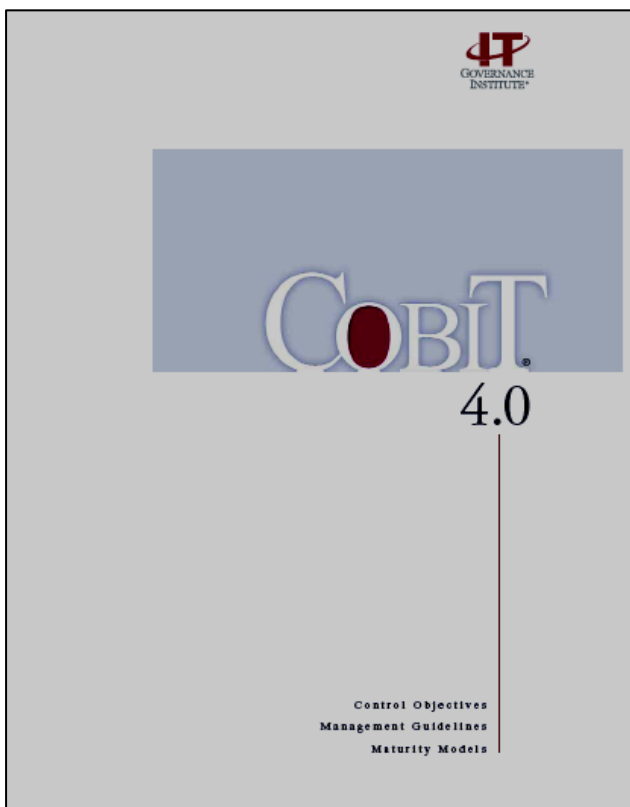
I punti focali del progetto CobiT 4.0

La strategia di sviluppo di COBIT 4.0 si è concentrata sulle aree seguenti:

... omissis ... (vedi FAQ n.4 in una pagina successiva)

Le principali modifiche in CobiT 4.0

Il capitolo seguente descrive le principali aree di COBIT oggetto di variazioni e miglioramenti.



Framework

Sono state introdotte modifiche all'ambito di ogni dominio e di alcuni processi, sebbene i domini siano ancora 4 e i processi 34 come prima:

Pianificazione ed Organizzazione

PO4 *Definire l'organizzazione e le relazioni IT* è stato esteso per coprire i processi e le relazioni IT al pari dell'organizzazione.

PO5 *Gestire gli investimenti in IT* è stato migliorato per coprire più pienamente la creazione del valore.

PO8 *Assicurare la conformità ai requisiti esterni* è stato eliminato e il suo contenuto è stato spostato in un nuovo ME4.

PO10 *Gestire la qualità* è diventato PO8. Ora ci sono solo 10 processi nel dominio PO.

Acquisizione e Realizzazione

A14 *Sviluppare le procedure* è stato espanso ed ora si chiama *Abilitare l'operatività e l'utilizzo*.

Un nuovo processo *Procurare le risorse IT* è stato aggiunto come A15 (il vecchio A15 è diventato A17,

(Continua a pagina 5)

COBIT 4.0: The New Face of COBIT

(Continua da pagina 4)

una collocazione più logica nel ciclo di vita).

AI6 *Gestire le modifiche* e AI7 *Installare e accreditare soluzioni e modifiche* (in precedenza sistemi) sono stati maggiormente allineati ai principi ITIL.

Erogazione e Assistenza

DS8 è stato ribattezzato *Gestire il service desk e gli incidenti*, mentre DS10, ora ribattezzato *Gestire i problemi*, copre solo la gestione dei problemi. Ciò è in linea con la guida ITIL.

DS11 *Gestire i dati* ora contiene solo obiettivi di gestione dei dati mentre gli obiettivi correlati al controllo delle applicazioni sono stati spostati in un capitolo all'interno del quadro di riferimento. Questo perché solitamente i controlli delle applicazioni sono integrati nei processi di business, non nei processi di IT.

Monitoraggio e Valutazione

ME1 è stato ribattezzato *Monitorare e valutare le prestazioni IT*, per andare incontro in primo luogo alle esigenze dei responsabili di processo.

ME2 è stato ribattezzato *Monitorare e valutare il controllo interno*, per andare incontro in primo luogo alle esigenze di quanti hanno responsabilità globali sull'IT.

ME3 *Supervisionare la governance IT* sostituisce il precedente *Ottenere una certificazione indipendente*, per andare incontro in primo luogo a quanti hanno nell'impresa responsabilità generali per quanto attiene agli aspetti IT.

ME4 *Assicurare conformità alle regole* sostituisce il precedente M4 *Condurre un audit indipendente* che è stato considerato non essere un processo IT. ME4 risponde ai requisiti di regolamenti esterni, legali e contrattuali ed è derivato dal vecchio PO8.

Il numero delle tipologie di risorse implicate nei processi IT è stato ridotto da cinque a quattro:

Risorse umane

Informazioni, al posto dei dati

Applicazioni

Infrastrutture, categoria che sostituisce tecnologia e servizi di supporto.

Control Objectives & Management Guidelines

La presentazione dell'obiettivo di controllo di alto livello è ancora in forma di cascata, ma è stata modificata nel seguente formato:

***Il controllo sul processo IT di ...
che soddisfa il requisito aziendale per l'IT di ...
è raggiunto con ...
è gestito da ...
ed è misurato da ...***

(Continua a pagina 6)

COBIT 4.0: The New Face of COBIT

(Continua da pagina 5)

Gli obiettivi di controllo e le linee guida per la gestione sono stati integrati in un solo documento, con il loro contenuto che è riportato di seguito all'interno di ogni processo. In questo modo è disponibile un libro singolo e facile da navigare per tutti i tipi di utenza.

Gli obiettivi di controllo di dettaglio sono stati migliorati per aumentare il grado di copertura della governance dell'IT e l'armonizzazione con altre pratiche e per accogliere le osservazioni ricevute. Il numero di obiettivi e il volume di materiale è stato ridotto di circa il 20% e la loro presentazione è stata resa più pratica e concisa. Si era trovato che molti obiettivi di controllo della 3a edizione erano di natura generale, così sono stati eliminati e sostituiti da una breve lista generale nel Quadro di riferimento.

Ogni processo IT ha ora una descrizione con la definizione degli input ed output primari che evidenziano da quale processo derivano o a quale processo sono orientati, oppure se il percorso è esterno a COBIT. Questi collegamenti di input e output permettono di identificare i flussi dei processi chiave all'interno di COBIT.

Per ogni processo IT sono state inserite nuove informazioni aggiuntive che descrivono le attività di processo (in modo esemplificativo e non esaustivo) e la proprietà e le responsabilità del processo stesso. Ciò è presentato come una lista di attività chiave incrociate con uno schema RACI che usa una lista di ruoli standard dell'impresa e dell'IT.

In appendice è fornita una matrice che mostra il legame tra gli scopi generali dell'impresa e gli scopi dell'IT e come questi sono mappati sui processi IT (definiti da COBIT). Questo materiale è stato usato per migliorare scopi e metodi di misura in COBIT 4.0 e per supportare la dimostrazione dell'ampia copertura di COBIT anche da una prospettiva aziendale.

Gli scopi e i metodi di misura (KGI e KPI) sono stati revisionati e migliorati per fornire un migliore orientamento al business e un maggiore focus sugli scopi di ogni processo e sugli scopi generali dell'IT. KPI e KGI sono stati migliorati in modo significativo: in struttura e contenuto. I metodi di misura sono in numero minore ma più concretamente utilizzabili per le attività principali di ogni processo, per il processo in sé e per l'IT in generale. Ciò consente agli utenti di distinguere tra indicatori di performance per il processo, indicatori di scopo per il processo e indicatori di scopo per l'IT. Tutti queste misure si collegano direttamente agli scopi generali dell'impresa e dell'IT individuati nel Quadro di riferimento.

I fattori critici di successo della 3a Edizione sono stati sostituiti da due nuove entità: gli input di processo sono i fattori di successo mutuati dall'esterno e le pratiche di gestione chiave o gli scopi delle attività sono i fattori di successo cui deve tendere il proprietario del processo.

I modelli di maturità sono stati riallineati alla nuova struttura dei processi e la tabella delle caratteristiche della maturità è stata revisionata e migliorata introducendo le seguenti nuove caratteristiche:

- Consapevolezza e comunicazione
- Politiche, standard e procedure
- Strumenti e automazione
- Competenze ed esperienza

(Continua a pagina 7)

COBIT 4.0: The New Face of COBIT

(Continua da pagina 6)

- Responsabilità e competenza
- Definizione e misura degli obiettivi

Tutto il nuovo materiale sarà disponibile nel quarto trimestre 2005 e formerà il contenuto di base da cui dipende il pianificato nuovo sviluppo delle pratiche di controllo e delle linee guida di audit.

Control Practices

Le pratiche di controllo saranno modificate ed aggiornate in seguito per allinearle ai nuovi obiettivi di controllo.

Audit Guidelines

Le linee guida di audit attuali furono sviluppate nel 1996, prima che fossero prodotte le Management Guidelines e le Control Practice, pertanto fanno riferimento unicamente agli obiettivi di controllo. Esse descrivono e supportano un generico processo di audit fatto di acquisizione di conoscenza, valutazione del controllo, test di conformità e quantificazione del rischio.

Nella nuova versione, le linee guida di audit saranno sostituite da una nuova pubblicazione, *IT Assurance Guide using COBIT*, che descriverà come si può far leva su COBIT per supportare parecchie tecniche di assurance, comprese quelle già coperte dalle linee guida di audit:

- Concetti di valutazione del rischio
- Valutazione rischio/valore del business
- Pianificazione e definizione dell'ambito dell'assurance
- Valutazione del controllo e test
- Maturità del controllo e del processo (auto-valutazione)
- Quantificazione del rischio ed efficacia del rapporto

Pertanto la nuova pubblicazione fornirà una guida migliore delle attuali *Audit Guidelines* e farà riferimento all'insieme completo dei componenti di COBIT. Il materiale attuale cui si fa riferimento nelle *Audit Guidelines* sarà sostituito da contenuti più ampi come segue:

- Chi intervistare – schemi RACI
- Cosa ottenere – input di processo
- Cosa valutare – obiettivi di controllo e pratiche di controllo
- Cosa testare – Fasi dell'assurance, che saranno aggiunte alle pratiche di controllo



(Continua a pagina 8)

COBIT 4.0: The New Face of COBIT

(Continua da pagina 7)

- Elementi per individuare e quantificare il rischio – input e output di processo, KPI e KGI, benchmark dal COBIT Online.

Il contenuto di dettaglio necessario a supportare ognuna delle tecniche verrà mantenuto in COBIT Online e sarà disponibile per download in un numero di tabelle di assurance.

Saranno disponibili nel 2006.

L'impatto sull'utenza attuale

COBIT 4.0 è un'evoluzione della 3a Edizione ed è basato essenzialmente sugli stessi principi e strutture base.

Pertanto non si deve "gettare via" il lavoro fatto fino ad ora.

COBIT 4.0 si appoggia sulla 3a Edizione e fornisce contenuti più aggiornati e migliori come pure elementi aggiuntivi.

Nelle appendici sono fornite matrici di riferimento che mostrano come i processi e gli obiettivi di controllo si mappano in entrambe le direzioni per aiutare l'eventuale conversione di documenti e strumenti attuali nei nuovi schemi.

Le misure sono migliori rispetto alla 3a Edizione, costruiti sugli stessi principi KGI/KPI, e forniscono un migliore orientamento al business ed esempi per aiutare gli utenti a definire migliori misurazioni per conto loro.

Il nuovo materiale inerente la descrizione del processo, le attività e le responsabilità renderà più facile capire l'ambito e lo scopo di ogni processo e renderà più chiara la proprietà del processo.

L'utilizzo di COBIT per istituire o migliorare i processi IT è pertanto considerevolmente rafforzato.

La nuova *Assurance Guide* espanderà le linee guida di audit attuali, aggiungendo nuove tecniche e facendo riferimento a tutto il contenuto del nuovo COBIT 4.0.

COBIT Online avrà due versioni disponibili per la maggior parte del 2006. Ci sarà una 3a Edizione "congelata" di COBIT Online e un COBIT Online 4.0, che diventerà il nuovo repository mantenuto con continuità. Pertanto gli utenti di COBIT Online saranno pienamente supportati.

I prodotti derivati da COBIT, come la *COBIT Security Baseline*[™], *COBIT Quickstart*[™], *IT Governance Implementation Guide*, *IT Control Objectives for Sarbanes-Oxley* e i report di mapping di COBIT saranno riallineati e aggiornati.

I benefici che potrà apportare agli utenti

Le modifiche effettuate in COBIT 4.0 sono sostanziali e dovrebbero aiutare gli utenti a ottenere molti benefici come:

Più completa e più piena copertura della governance dell'IT – Aiuta a mettere a fuoco le aree opportune e mette in grado la direzione IT e gli auditor di dimostrare come è governata l'IT

Contenuto più facile da capire e più accessibile – Aiuta tutti gli interessati a lavorare ad un insieme condiviso di obiettivi con una comune comprensione dei temi

Migliore armonizzazione con altre pratiche – Aiuta l'integrazione e l'uso di COBIT come la metodologia "ombrello"

Migliorata informazione sui processi IT, su scopi orientati al business e metodi di misura, modelli di maturità raffinati – Aiuta gli utenti ad allineare meglio la governance dell'IT con le sollecitazioni del business e poi a sviluppare e confrontare le caratteristiche dei processi e le prestazioni.

(Continua a pagina 9)

COBIT 4.0: The New Face of COBIT

(Continua da pagina 8)

Questo articolo è stato scritto quando la pubblicazione era sottoposta alla revisione finale. I commenti di molti di questi revisori sono stati estremamente positivi:

“Non assomiglia ad un tomo accademico – quando tu uccidi la gente con ovvietà su ogni pagina. Questo documento ha il potenziale per diventare sporco, con le orecchie e usato con profitto – proprio quello che vogliamo”.

“Noi abbiamo la filosofia di andare oltre le aspettative dei clienti - in questo caso avete raggiunto il 110%. Questo documento ha realmente la possibilità di essere una pietra miliare”.

“La nuova versione è un grosso, buono, concreto e costruttivo salto in avanti dalla terza edizione”.

“Le descrizioni degli input e degli output sono brillanti. Questo aiuterà a comprendere l’impatto quando si valutano i rischi”.

“L’integrazione dei modelli di maturità con gli obiettivi di controllo è effettivamente buona e operativa. Questo dà agli auditor una ‘guida rapida’ per riportare i rilievi alla direzione”.

“Sono positivamente sorpreso dalla grandezza del miglioramento dalla versione 3 alla versione 4. Coerenza, qualità e usabilità sono cresciute significativamente”.

“L’ho trovato un documento molto leggibile, molto coerente e un potente strumento di audit”.

“Globalmente, penso che ci sia dietro una sorprendente quantità di lavoro e tanto di cappello a tutti quelli che hanno contribuito. Mi piace particolarmente l’aggiunta di input, output e degli schemi RACI”.

Tali entusiastiche recensioni non sono determinate dal lavoro di una sola persona o anche di un piccolo gruppo. ITGI è estremamente grato al Comitato Guida di COBIT per il suo lavoro di guida del progetto, e alle centinaia di volontari in tutto il mondo che hanno scritto alcune parti, rivisto bozze, discusso il linguaggio, e fornito input, suggerimenti e critiche. Il valore dei contributi combinati di questi esperti globali non sarà mai considerato abbastanza.

Gary Hardy e Erik Guldentops, CISA, CISM

Gary Hardy

È Direttore di IT Winners, una società di consulenza indipendente operante in South Africa e specializzata in IT Governance e nel miglioramento delle performance. Hardy è associato ad ISACA dal 1981 ed ha ricoperto diverse cariche sociali, tra di esse il Comitato per la promozione degli associati. E’ tra i fondatori e continua a far parte del COBIT Steering Committee. E’ anche l’animatore di un forum di discussione sull’IT Governance al quale partecipano importanti CIO della Gran Bretagna. Hardy si occupa di IT, IT audit and IT Governance da più di 25 anni in diversi ambiti: industria, internal audit, external audit e consulenza.

Erik Guldentops, CISA, CISM

È consulente dell’IT Governance Institute e professore alla Management School della Università di Antwerp, Belgio, dove insegna sicurezza e controlli informatici, IT Governance e risk management. Ha concluso la sua carriera in SWIFT nel 2001 come Direttore Sicurezza, dopo essere stato Direttore Auditing. Ha iniziato e guidato lo sviluppo di COBIT all’inizio degli anni ‘90 e attualmente lavora in diversi comitati e gruppi di lavoro promossi dall’ITGI.

Francesco Marchiori, CISA

Opera in ambito informatico-bancario da più di 25 anni. E’ stato capo progetto e da 10 anni è IS Auditor presso il gruppo Banca Lombarda Piemontese. Da 5 anni collabora nel Gruppo di Ricerca COBIT promosso da AIEA per la traduzione e diffusione di COBIT.

COBIT: Frequently Asked Questions

La traduzione delle risposte alle più frequenti domande su COBIT 4.0

Le differenze rispetto alla precedente edizione

*Traduzione a cura del
Gruppo di Ricerca AIEA: COBIT4*

1. Qual è la storia del modello COBIT?
2. Come si è evoluto COBIT 4.0?
3. Quali cambiamenti sono avvenuti nel business per stimolare un aggiornamento di COBIT?
4. Quali sono le aree più interessate dagli aggiornamenti di COBIT?
5. Quali componenti di COBIT sono stati modificati nella nuova versione 4.0?
6. Cosa comprende il nuovo volume COBIT 4.0?
7. Quali sono le differenze tra COBIT 4.0 e COBIT 3a edizione?
8. COBIT 4.0 sostituisce la terza edizione di COBIT?
9. Dove posso trovare COBIT 4.0?

1. Qual è la storia del modello COBIT?

La prima componente del modello COBIT, il quadro di riferimento o *framework*, è stato definito e pubblicato nella prima edizione nel 1994. Successivamente gli standard internazionali, l'attività di ricerca e le linee guida utilizzate come prassi di riferimento contribuirono alla formulazione degli obiettivi di controllo (*Control objectives*).

Al fine di fornire indicazioni sulle modalità di verifica dell'appropriata implementazione dei controlli, furono definite le linee guida per la revisione (*Audit Guidelines*).

Gli studi e le ricerche effettuati per la prima e la seconda edizione (1998) comprendevano l'analisi delle fonti internazionali classificate; il lavoro è stato svolto da istituti internazionali e da gruppi di lavoro in Europa (Free University of Amsterdam), negli Stati Uniti (California Polytechnic University) ed in Australia (University of New South Wales). I ricercatori effettuarono la raccolta, la revisione, la valutazione e l'acquisizione di standard tecnici internazionali, codici di condotta, standard di qualità, standard internazionali professionali, prassi e requisiti di set-

(Continua a pagina 11)

COBIT: Frequently Asked Questions

(Continua da pagina 10)

tore, con riferimento al framework di COBIT o a specifici obiettivi di controllo. Dopo la raccolta e l'analisi, i ricercatori approfondirono ciascun dominio e processo e ne suggerirono modifiche, inserendo o modificando i relativi obiettivi di controllo.

Il consolidamento dei risultati venne approvato dal Comitato Direttivo di COBIT.

Nel 2000 venne rilasciata la 3^a Edizione di COBIT, con la quale furono introdotte le linee guida per la gestione (*Management Guidelines*) ed aggiornati i contenuti della seconda edizione, sulla base di nuovi o aggiornati standard internazionali di riferimento. Inoltre, il modello fu rivisto e migliorato al fine di supportare i controlli sulla gestione, consentire il monitoraggio delle prestazioni (*performance management*) e sviluppare ulteriormente il Governo dell'IT.

2. Come si è evoluto COBIT 4.0?

L'IT Governance Institute, tramite il suo Comitato Direttivo di COBIT, si pone come obiettivo il costante sviluppo della conoscenza contenuta in COBIT (*COBIT body of knowledge*). A tal fine, negli ultimi due anni, il Comitato ha condotto una ricerca su diversi aspetti riguardanti gli obiettivi di controllo e le linee guida per il Management. Tale ricerca è stata condotta sulla base dell'esperienza e con il contributo volontario di associati ad ISACA, utenti di COBIT, consulenti esperti e docenti universitari. Gruppi a livello locale, costituiti da 6 a 10 esperti, a Bruxelles (Belgio), Londra (Regno Unito), Chicago (USA), Canberra (Australia), Città del Capo (Sud Africa), Washington DC (USA) e Copenhagen (Danimarca), si sono riuniti, in media due o tre volte l'anno, al fine di svolgere le attività di ricerca o revisione loro assegnate dal Comitato Direttivo di COBIT. Inoltre alcuni progetti di ricerca sono stati assegnati a facoltà universitarie ad indirizzo aziendale, come la University of Antwerp Management School (UAMS, Belgio) e la University of Hawaii (USA).

I risultati di queste attività sono stati proposti in alcuni workshop, coinvolgendo in ciascuno circa 50 esperti di livello internazionale, che si sono concentrati sulle seguenti componenti del modello: gli obiettivi di controllo, le linee guida per il Management, il modello di maturità. Il Comitato Direttivo di COBIT ha consolidato tutti i risultati ottenuti; la revisione della bozza da parte di 90 specialisti ha completato il processo.

3. Quali cambiamenti sono avvenuti nel business per stimolare un aggiornamento di COBIT?

Molti cambiamenti nel modo di operare delle aziende hanno reso necessario l'aggiornamento di COBIT:

- *La crescente attenzione sull'IT Management* — La necessità di fornire un'appropriata guida sulla gestione e il controllo degli attuali ambienti operativi IT

(Continua a pagina 12)

COBIT: Frequently Asked Questions

(Continua da pagina 11)

- *Enti sempre più interessati all'assurance* — La necessità di rispondere ai bisogni degli auditor, degli organi regolatori (*regulators*), degli esperti di sicurezza e di altre figure coinvolte nel fornire garanzie (*assurance*) circa le prestazioni dell'IT in condizioni diverse.
- *Una maggior attenzione per la governance ai massimi livelli aziendali* — Garantire un'attenzione adeguata dell'azienda per la governance e l'esistenza di meccanismi per allineare la gestione ed i controlli degli obiettivi IT con le necessità delle imprese.
- *La crescente maturità delle migliori pratiche e standard IT*— Assicurare che le imprese adottino in misura sempre maggiore linee guida specializzate come ITIL e ISO 17799; in questo contesto COBIT può essere utilizzato come integratore e quadro di riferimento generale, continuando ad essere considerato altamente credibile ed una guida pratica per la totalità dei controlli IT.
- *Un utilizzo integrato da parte dei tre principali utenti: il management, gli informatici e gli auditor* — Assicurare che la struttura, la presentazione ed il linguaggio utilizzato sia di facile comprensione e applicazione da parte degli stakeholder ai livelli direttivi, come pure dei professionisti e degli addetti.
- *Una crescita nella regolamentazione e nella conformità* – Assicurare che COBIT copra in modo totale l'ambito del Governo dell'IT e mostri come correlare i domini dell'IT Governance ed il COSO framework, così che COBIT possa continuare ad essere considerato come il modello di riferimento de facto per i controlli dell'IT e per l'IT Governance.



4. Quali sono le aree più interessate dagli aggiornamenti di COBIT?

- *IT Governance* - Aggiornamento centrato sulle cinque aree che costituiscono l'IT Governance secondo la definizione di ITGI: allineamento strategico, creazione di valore, risk management, gestione delle risorse, misura delle performance. COBIT copriva già molte di queste aree, ma l'analisi ha evidenziato alcune difformità che sono ora state superate rivedendo il titolo di alcuni processi IT ed aggiungendo alcuni nuovi obiettivi di controllo. COBIT 4.0 contiene una matrice di raccordo fra tutti i processi IT ed i cinque domini dell'IT Governance.
- *Requisiti di business* – L'orientamento di COBIT ai requisiti di business è sempre stato un principio fondamentale concretizzato negli "*information criteria*". L'approfondita ricerca condotta dall'Università di Antwerp in merito alle modalità con cui l'IT contribuisce al raggiungimento degli obiettivi aziendali, nell'ambito di diversi settori economici, ha mostrato in modo diffuso l'esistenza di una relazione fra gli obiettivi aziendali e gli obiettivi dell'IT. La nuova versione di COBIT contiene una tabella che mostra le relazioni tra gli obiettivi di business, gli obiettivi IT ed i processi IT di COBIT per aiutare gli utilizzatori ad identificare il collegamento tra l'IT ed il

(Continua a pagina 13)

COBIT: Frequently Asked Questions

(Continua da pagina 12)

business nella propria organizzazione. Questo lavoro ha migliorato gli indicatori chiave di obiettivo e di prestazione.

- *Armonizzazione* – Al fine di agevolare gli utenti nell'integrazione di COBIT 4.0 con altre linee guida maggiormente dettagliate - ITIL, ISO 17799, PMBOK e PRINCE2 - si è provveduto ad armonizzare i termini ed i concetti utilizzati in COBIT 4.0
- *Creazione di valore* – L'enfasi sui controlli per gestire i rischi deriva dal fatto che COBIT è nato come strumento di audit. COBIT 4.0 bilancia meglio i concetti di rischio e valore e utilizza i risultati di recenti ricerche in tema di *value management* nel campo dell'IT.
- *Struttura dell'impresa (Enterprise architecture)* – COBIT 4.0 fornisce schemi RACI (chi è Responsabile, chi è incaricato di svolgere l'attività—Addetto—, chi deve essere Consultato, chi deve essere Informato) per aiutare a definire correttamente i ruoli e le responsabilità in ciascuno dei processi IT. I concetti di organizzazione aziendale (*enterprise architecture*) utilizzati sono ora illustrati all'interno del quadro di riferimento (*framework*), collegando tra loro obiettivi, risorse, informazioni e processi.
- *Definizioni e flussi dei processi* – Al fine di migliorare la comprensione del modello dei processi IT, COBIT 4.0 descrive ogni processo, i relativi flussi di input ed output, i riferimenti incrociati con gli altri processi.
- *Linguaggio e presentazione*— In COBIT 4.0 è stato usato un linguaggio più conciso, attuale ed operativo (*action-oriented*). Gli obiettivi di controllo e le linee guida per il management sono stati raggruppati insieme in ogni processo IT.
- *Feedback* – Gli utenti inviano regolarmente commenti e suggerimenti; questi, insieme ai feedback ricevuti dalle tre "COBIT User Conventions", sono stati usati per migliorare il contenuto di COBIT 4.0.

5. Quali componenti di COBIT sono stati modificati nella nuova versione 4.0?

Obiettivi di Controllo

- Allineamento "dal particolare al generale", tra COBIT e IT Governance. Un'analisi su come gli obiettivi di controllo di dettaglio possono essere mappati sui cinque domini dell'IT Governance per identificare possibili non coperture.
- Allineamento "dal generale al particolare", tra COBIT e IT Governance. Una ricerca sulle più importanti prassi di IT Governance che non erano state considerate appieno nella versione 3 di COBIT al fine di ridurre potenziali carenze.
- Armonizzazione di COBIT con altri standard di maggior dettaglio. Una dettagliata mappatura tra COBIT ed ITIL, CMM, COSO, PMBOK, ISF e ISO/IEC17799 per consentire l'allineamento con tali standard per quanto riguarda il linguaggio, le definizioni e i concetti.

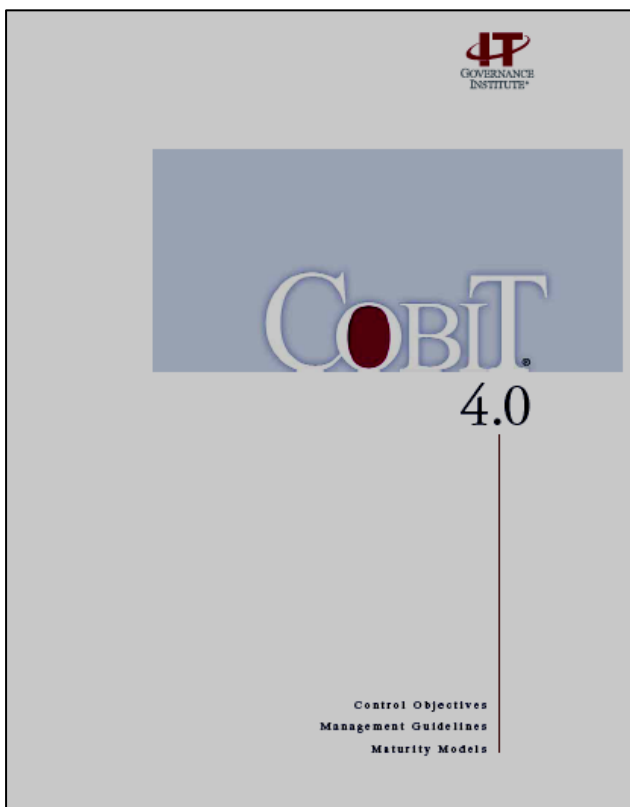
(Continua a pagina 14)

COBIT: Frequently Asked Questions

(Continua da pagina 13)

Sebbene ci siano 34 obiettivi di controllo di alto livello sia in COBIT 3ª Edizione sia in COBIT 4.0, questi 34 obiettivi non sono però gli stessi. I cambiamenti possono essere così sintetizzati:

- Il dominio M è ora diventato ME, con il significato di Monitoraggio e Valutazione (*Monitor and Evaluate*).
- M3 ed M4 erano processi di Audit e non processi IT; sono stati rimossi, perchè sono adeguatamente coperti da un certo numero di standard di IT Audit, ma, nella nuova versione aggiornata del *framework*, sono stati inseriti dei riferimenti per sottolineare che i manager hanno bisogno e debbono usare le funzioni di "assurance".
- ME4 comprende il processo di supervisione della IT Governance.
- ME3 è il processo connesso alla supervisione della conformità a norme e regolamenti, tale finalità era precedentemente inclusa nel processo PO8.
- Il Processo *PO8-Conformità* è stato quindi rimosso; volendo mantenere la numerazione consistente con quella della 3ª Edizione per *PO9-Valutare i rischi* e *PO10-Gestire i progetti*, il vecchio processo PO11 ne ha preso il posto ed è diventato *PO8-Gestire la qualità*. Il dominio PO ha ora 10 processi invece di 11.
- Il dominio AI ha richiesto due modifiche: l'aggiunta di un processo di *procurement* (acquisizione) e la necessità di includere in AI5 le funzioni di "release management". Quest'ultima modifica e la necessità che questo processo fosse l'ultimo del dominio AI ha fatto sì che fosse classificato come AI7. Lo spazio così creato è stato pertanto usato per aggiungere il nuovo processo *AI5- Acquisire le risorse IT*. Il dominio AI ha ora sette processi invece di sei.



Linee Guida per il Management

Chiarimento della relazione causa effetto fra KGI e KPI, attraverso l'identificazione con maggior dettaglio di come i KPI conducano al conseguimento dei KGI.

Revisione della qualità dei KGI, KPI e CSF, attraverso il miglioramento della qualità delle metriche grazie alla precedente analisi della relazione causa effetto tra KPI e KGI.

Suddivisione dei CSF tra quanto deve pervenire dall'esterno (input) e quanto deve essere fatto internamente al processo (*management practice*):

Analisi di dettaglio dei concetti che sottendono le metriche. Assieme ad esperti di metriche sono stati approfonditi e migliorati i concetti alla base di ciascuna metrica per costruire metriche in cascata fra i processi IT e quelli aziendali identificando criteri

(Continua a pagina 15)

COBIT: Frequently Asked Questions

(Continua da pagina 14)

di qualità per le metriche stesse.

Collegamento fra gli obiettivi aziendali, gli obiettivi IT e gli obiettivi di processo. Una ricerca approfondita in otto differenti settori economici ha permesso di conseguire una visione più dettagliata di come i processi di COBIT facciano da supporto per conseguire specifici obiettivi IT e per estensione gli obiettivi aziendali; i risultati sono stati poi generalizzati.

Revisione dei contenuti del modello di maturità per garantire consistenza e qualità dei livelli di maturità tra diversi processi e all'interno di ciascun processo, anche attraverso il miglioramento e l'ampliamento delle definizioni degli attributi del modello di maturità.

6. Cosa comprende il nuovo volume COBIT 4.0?

Il nuovo volume di COBIT 4.0 è suddiviso in 4 sezioni:

- l'*Executive Overview*
- il *Framework* (Quadro di riferimento)
- la parte principale del modello (*Core Content*) costituita da obiettivi di controllo, di alto livello e di dettaglio, dalle linee guida per il management e dal modello di maturità
- le Appendici, che contengono diverse mappature e riferimenti (*cross-references*), un'ampia informativa sul modello di maturità, una bibliografia ed elenco delle fonti, la descrizione dei prossimi passi nello sviluppo di COBIT, un dizionario)

La parte principale del modello (*Core Content*) è suddivisa in base a 34 processi IT. Ciascun processo è articolato in quattro sezioni di circa una pagina ciascuna, organizzate in modo da fornire un quadro completo su come controllare, gestire e misurare il processo.

Le quattro sezioni per ogni processo, nell'ordine, sono:

- l'obiettivo di controllo di alto livello del processo:
 - * la descrizione del processo che riassume gli scopi del processo
 - * l'obiettivo di controllo di alto livello descritto utilizzando uno schema "a cascata" che riassume le finalità, le metriche e le *practice* del processo
 - * la collocazione del processo rispetto ai domini, ai criteri di valutazione delle informazioni (*information criteria*) e le risorse IT.
- gli obiettivi di controllo di dettaglio del processo
- le linee guida di gestione (*Management Guidelines*): input e output del processo, la tabella dei ruoli RACI (*Responsabile, Addetto, Consultato e Informato*), scopo e metriche

(Continua a pagina 16)

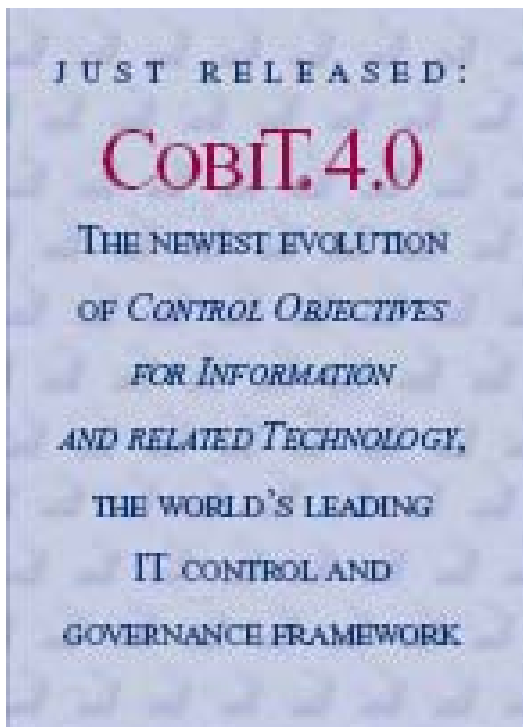
COBIT: Frequently Asked Questions

(Continua da pagina 15)

- il modello di maturità del processo.

Un diverso modo di descrivere il contenuto del processo è il seguente:

- Gli input di processo sono ciò che il responsabile del processo aziendale chiede agli altri.
- L'illustrazione del processo descrive quello che il responsabile del processo aziendale deve fare.
- Gli output di processo sono costituiti da ciò che il responsabile del processo aziendale deve produrre.
- Gli scopi e le metriche illustrano come il processo deve essere misurato.
- La tabella RACI definisce cosa deve essere delegato ed a chi.
- Il modello di maturità mostra come il processo possa essere corretto per essere migliorato.



7. Quali sono le differenze tra COBIT 4.0 e COBIT 3a edizione?

COBIT 4.0 sostituisce le seguenti parti della terza edizione: Executive Summary, Framework, *Control Objectives* e *Management Guidelines*.

È in corso l'aggiornamento delle *Control Practices* e delle *Audit Guidelines* per allinearle ai cambiamenti apportati al framework e ai contenuti di COBIT 4.0.

L'*Implementation Tool Set* della terza versione è sostituito dall'*IT Governance Implementation Guide*, pubblicata nel 2003, comunque l'*Implementation Tool Set* è ancora disponibile e contiene diverse indicazioni utili.

(Continua a pagina 17)

COBIT: Frequently Asked Questions

(Continua da pagina 16)

8. COBIT 4.0 sostituisce la terza edizione di COBIT?

No. COBIT 4.0 è un'evoluzione di COBIT 3^a Edizione e non invalida in alcun modo le implementazioni o le attività basate su COBIT 3^a Edizione, in quanto pienamente compatibili con COBIT 4.0. La sezione introduttiva di COBIT 4.0 offre l'opportunità, ove possibile, di migliorare ulteriormente la Governance dell'IT e il sistema di controllo fornendo esempi di transizione. Tale transizione è supportata da una serie di mappature incluse in allegato a COBIT 4.0; inoltre, per facilitare tale attività di transizione, rimarrà disponibile anche la versione 3.2 di COBIT Online che non subirà alcun aggiornamento.

COBIT Online continuerà con regolarità ad essere aggiornato con nuove versioni, le successive alla 3.2 saranno rilasciate in formato elettronico; se necessario, gli aggiornamenti verranno occasionalmente pubblicati in formato cartaceo.

9. Dove posso trovare COBIT 4.0?

COBIT 4.0 è disponibile dalla fine di novembre 2005. Buona parte dei suoi contenuti può essere scaricata o anche acquistata, assieme agli altri prodotti di COBIT, all'indirizzo www.isaca.org/bookstore.

(traduzione a cura del Gruppo di Ricerca COBIT 4.0)

Gruppo di Ricerca COBIT 4.0

Sono iniziati i lavori del Gruppo di Ricerca finalizzato alla traduzione e diffusione della versione **4.0 di COBIT®**.

I lavori sono coordinati dal Vicepresidente Orillo Narduzzo. I primi documenti saranno disponibili entro la prossima primavera.

I Componenti del Gruppo di Ricerca sono: Arduini Stefano, Elefante Alfonso, Galasso Paola, Gallistru Alfredo, Giambarini Luigi, Marchiori Francesco, Martini Andrea, Marzo Marinella, Narduzzo Orillo, Ongetta Silvano, Pederiva Andrea, Pertile Luca, Piemonte Alberto, Porcelli Mauro, Salvato Marco, Spreafico Giulio, Trapè Andrea, Valenti Silvia.

L'Audit del Sistema di Gestione per la Qualità: un grande assente il Sistema Informativo

di Riccardo Bianconi

Le riflessioni che seguono sono il frutto dell' esperienza fatta sottoponendo ad Audit, negli ultimi dodici anni, diverse centinaia di Organizzazioni diverse. Dall' osservazione di tutte queste realtà mi sono formato una convinzione, che ritengo possa avere pochissime eccezioni. Si tratta del fatto che, ad oggi, praticamente tutte le Organizzazioni dedite ad attività produttive, di servizio o commerciali, sono dipendenti in modo totalizzante dai propri Sistemi Informativi, che nella fattispecie si materializzano quasi del tutto con i Sistemi Informatici, fatta salva quella parte della gestione delle informazioni che è demandata all'uomo¹. Le eccezioni sono pochissime e sicuramente non sono rilevanti nell'ambito del business.

Forse, per qualcuno, questa affermazione potrà sembrare una smaccata banalità, ma l'oggetto della riflessione fatta in queste righe non è la convinzione in sé, bensì le conseguenze che dovrebbero derivarne per le attività di Auditing dei Sistemi di Gestione aziendali.

Nel valutare la capacità di un'Organizzazione di conformarsi ai requisiti della Norma UNI EN ISO 9001:2000, si rileva molto frequentemente che i processi, tutti, sono gestiti attraverso delle applicazioni [software] che "girano" sui Sistemi Informatici, i quali, a loro volta possono prevedere l' utilizzo di periferiche specifiche e dedicate. Ad esempio, possiamo far riferimento ad attività amministrative dei processi produttivi, come il "passaggio di stato" di un lotto di parti lavorate: ad esempio il "versamento a magazzino" di semilavorati, che debbono essere registrati nella loro condizione attuale, per quantità, tipo, ordine, ubicazione, così, come possiamo far riferimento ad aspetti operativi di gestione della produzione: si pensi alla gestione delle attrezzature a controllo numerico o dei magazzini automatizzati etc. Il Sistema Informativo è onnipresente e, nella maggior parte dei casi, è diventato indispensabile. Per essere più chiari, facciamo riferimento proprio alle macchine operatrici a controllo numerico: evidentemente non sarebbe possibile farle funzionare senza il relativo SW di controllo e senza un reparto di ingegneria, capace di elaborare o personalizzare, attraverso altri SW specialistici, le necessarie matematiche ed i parametri dei driver.

La tipologia di area di affari nella quale opera ogni singola Organizzazione, come appare ovvio, determina in larga parte la possibile scelta architetturale delle soluzioni tecniche ed organizzative necessarie al funzionamento dei processi, in primis quelli primari di produzione dei beni o dei servizi, ma sempre più spesso, anche quelli di supporto, come, ad es: la gestione delle manutenzioni delle proprie apparecchiature ed impianti o la gestione delle risorse umane o, ancora, la gestione degli approvvigionamenti o delle consegne a terzi. A seconda del business, ci saranno architetture di sistema ed infrastrutture specifiche: potremmo citare il caso delle attività commerciali che si appoggiano ai circuiti telematici per la gestione dei cosiddetti POS [Point-of-Sales Systems], i microterminali dedicati alla lettura delle carte di credito ed agli addebiti. Ovvero, potremmo citare le infrastrutture informatiche per il Commercio Elettronico o per lo scambio elettronico di dati (EDI - Electronic Data Interchange), utilizzate per il trasferimento di ordini e/o fatture o autorizzazioni di pagamento. È eclatante il caso della gestione della produzione di Organizzazioni molto strutturate, ove i processi sono

(Continua a pagina 19)

L'Audit del SGQ: un grande assente il SI

(Continua da pagina 18)

gestiti a mezzo di SW tipo ERP – Enterprise Resource Planning – che coinvolgono tutti i processi gestionali ed operativi. Se poi, con una visione più generale, osserviamo quante Organizzazioni si avvalgono di piccole reti interne, o di collegamenti internet, o dell'impiego della posta elettronica o del remote banking, si ha evidenza che i Sistemi Informatici pervadono davvero tutte le Organizzazioni.

Se ne potrebbe fare a meno? O sono diventati strategici ed insostituibili?

Le uniche Organizzazioni che possono essere escluse da tale scenario sono quelle come un Sistema di Gestione "Non Critico", per come definito dall' ISACA², potendo gestire i processi solo con registrazioni cartacee e sulla base della buona memoria degli operatori. Ad esempio una trattoria!

Con questa premessa, appare evidente che, nell' ambito del processo di Audit del Sistema di Gestione per la Qualità di un' Organizzazione, la mancata valutazione delle modalità di gestione del S.I. (Sistema Informatico), a fronte delle esigenze del più generale Sistema di Gestione dell' Organizzazione, non appare accettabile. Non ultimo, perché un possibile problema su tale sistema, si ripercuote in modo sostanziale, talora esiziale, sul business.

Il tema della criticità della gestione del S.I. (Sistema Informatico) Aziendale potrebbe essere ulteriormente analizzato almeno su tre diverse dimensioni:

1. La gestione del S.I. a fronte dell'esigenza di preservare le informazioni critiche (confidenzialità, disponibilità, integrità) per il business e, comunque, tutelate per legge (*per tali aspetti si veda anche la Norma ISO 27001*); si tratta, evidentemente di un aspetto specialistico, con una chiara area di sovrapposizione tra Security e Qualità, in quanto il mantenimento della riservatezza delle informazioni, così come la loro corretta conservazione e disponibilità, è spesso un requisito implicito del Cliente. Ce ne è quanto basta per dire che non può essere un aspetto negletto in un Sistema di Gestione per la Qualità.
2. La gestione del S.I. a fronte dell'esigenza di preservare le informazioni critiche per la sicurezza [fisica]³ degli utenti e dei lavoratori. Si pensi, ad esempio a quanto dipenda tale sicurezza dalla preservazione dell'integrità, disponibilità e dalla corretta elaborazione dei dati relativi alla gestione del traffico aereo, nella torre di controllo di un aeroporto. Volendo, si può prendere a riferimento la gestione della sicurezza nel trasporto ferroviario di passeggeri. In queste situazioni, la sicurezza è fornita non solo dall'affidabilità meccanica dei mezzi, ma sempre di più da quella della gestione delle informazioni: riconoscimento, instradamento e, in caso di nebbia, avverse condizioni meteo ovvero nelle ore notturne guida da remoto; instradamento dei convogli ferroviari, ove la gestione della segnaletica di sicurezza e dei relativi allarmi è direttamente gestita da sistemi informatici. La vita dei passeggeri, si può ben dire, è legata all' interazione intelligente dell'operatore qualificato con i sistemi informativi, che debbono essere sempre efficienti ed in grado di "sopravvivere" ad eventuali avarie puntuali o complesse. *Per tale aspetto, si dovrebbe prendere in esame un' applicazione congiunta delle Norme ISO 27001 ed ISO 15408 – i cosidd-*

(Continua a pagina 20)

L'Audit del SGQ: un grande assente il SI

(Continua da pagina 19)

detti Common Criteria, dedicati, questi ultimi, alla security HW e SW. Si faccia riferimento anche allo schema di certificazione OCSI⁴.

Non c'è che dire: la gestione corretta, professionale, sistematica e qualificata dei Sistemi Informativi ed Informatici in particolare, è una garanzia dovuta da qualunque Organizzazione che gestisca processi critici.

1. Da ultimo, la gestione del S.I. a fronte dell'esigenza di mantenere attivo il Sistema di Gestione Aziendale, sia per gli aspetti amministrativi-contabili, sia per quelli amministrativi-operativi. *Quest'ultimo aspetto è tipicamente funzionale alla mera applicazione della UNI EN ISO 9001:2000*; d'altronde, l'avaria o la ridotta prestazione del S.I., sempre, si ripercuote sulle prestazioni delle Organizzazioni: quindi sulla capacità delle stesse di soddisfare i propri Clienti. In definitiva di mantenerne la fiducia e la fedeltà nel comportamento di acquisto dei beni o servizi prodotti.

Difficilmente si potrà ritenere credibile, in un'ottica di qualità, intesa come capacità di essere efficaci verso i propri Clienti, un Sistema di Gestione che non preveda l'esistenza di adeguate prassi (procedure) di gestione del sistema informatico, il quale, a sua volta, materializza costantemente le procedure operative dello stesso Sistema di Gestione. Non è indispensabile la formalizzazione di tale gestione secondo i canoni definiti dalla letteratura tecnica al riguardo (es. CobiT[®] o ITIL[®])⁵, ma, non per questo, la questione può essere bellamente ignorata, ovvero lasciata al caso, o, magari, alla buona volontà ed alla competenza occasionale di qualche volonteroso presente in azienda. Almeno, non in un'azienda che richieda la certificazione secondo lo standard UNI EN ISO 9001:2000!

Sia pure con modalità "non standardizzate", una gestione della infrastruttura deputata al corretto funzionamento del flusso delle informazioni di supporto ai processi gestionali e, perché no, alla creazione del valore economico, è pur sempre necessaria. Ove manchi, prima o poi se ne pagherà lo scotto: si pensi alla situazione di avaria catastrofica che colga di sorpresa l'Organizzazione oggetto di analisi. Tantissimi casi lo testimoniano. Non occorre riferirsi agli attentati dell'11 Settembre 2001, è sufficiente limitare l'orizzonte di osservazione alla nostra realtà: server critici in avaria senza parti di ricambio o senza back-up aggiornato dei dati, servizi di "Call Center" che collassano sotto pressione e divengono lenti ed inadeguati, black-out generali che paralizzano i servizi ben oltre il tempo necessario per il ripristino dell'alimentazione elettrica ...

Come può esistere una Gestione della Qualità che ignori gli strumenti per conseguire gli obiettivi aziendali? Ebbene, il S.I. rappresenta lo strumento per eccellenza per raggiungere gli obiettivi dei processi operativi e strategici, e quindi gli obiettivi collegati relativi alla soddisfazione del Cliente⁶.

Quanto è importante tutelare la riservatezza delle informazioni relative alla catena di fornitura? Quanto è importante tutelare il cosiddetto know-how aziendale? Basta fare una semplice mano di conti e poche considerazioni essenziali, per divenire consapevoli del danno immenso che può derivare dalla superficiale gestione della Security del S.I.. Un modem abusivo per navigare su internet, connesso alla rete aziendale di una PMI, che fa capo all'unico server, di fatto al "*Sancta Sanctorum*" dell'azienda, ... come per incanto tutti i segreti commerciali, produttivi, tutta la conoscenza del business è alla portata di qualunque malintenzionato che abbia messo gli occhi sull'azienda, per acquisirla o per "clonarne" i processi. Oppure, con una certa approssimazione, si può valutare in un attimo quale immenso danno possa derivare da una gestione superficiale⁷, degli archivi dei programmi o delle basi dei dati o, magari, delle componenti HW, necessarie alla produzione ovvero alla gestione del processo di marketing o, più semplicemente, di quello commerciale. Quanto costerebbe un'interruzione operativa di un'ora? Di un giorno? Di una settimana? Quanto costerebbe la perdita o l'alterazione

(Continua a pagina 21)

L'Audit del SGQ: un grande assente il SI

(Continua da pagina 20)

delle informazioni contenute in tali banche dati? Eppure questo evento pernicioso può accadere, ad esempio per il mancato monitoraggio sistematico dello "stato di salute" degli Hard Disk, piuttosto che una cattiva ubicazione dei Server, piuttosto che l'accesso al S.I. con privilegi non adeguati, per non parlare della crescita non monitorata e non gestita per tempo, delle esigenze di calcolo e di banda sulla rete interna a fronte dei servizi "promessi" sul mercato. Cosa dire, inoltre, della gestione delle risorse umane addette alla condotta del S.I.? Pensiamo all'esigenza di programmare per tempo il loro "dimensionamento" ed aggiornamento, in funzione delle scelte strategiche di sostituzione o di ampliamento del parco macchine o del SW!

Il potenziale verificarsi di un'anomalia afferente uno solo di questi eventi rappresenta un rischio importante da gestire; e se il caso decidesse di farli accadere contemporaneamente ...?

Per meglio comprendere il punto in questione, proviamo a ragionare per assurdo: proviamo a ritenere possibile e corretto il fatto di non gestire in modo controllato il S.I., seppure abbiamo visto come questo sia lo strumento che governa i processi aziendali, quasi fosse il sistema nervoso centrale dell'azienda.

Proviamo ad immaginare un'ipotetica Organizzazione, mentre predispone la struttura del proprio sistema di gestione per la Qualità a fronte dello Standard ISO 9001:2000; immaginiamoci le risorse umane intente a studiare ed analizzare i processi, e le loro interazioni. Da questo studio preliminare alla definizione delle componenti del Sistema di Gestione per la Qualità, dovrebbe derivare una mappatura delle criticità a fronte degli obiettivi operativi e strategici, utile per individuare le specifiche esigenze di controllo⁸ e di coordinamento, quindi le esigenze di proceduralizzazione delle attività, ovvero dei processi, che necessitano di essere gestiti in modo controllato, per garantire le prestazioni desiderate.

Ma se questi processi sono strutturati sulla base di un S.I. che ne materializza la dinamica, che li sostanzia ed al quale non si può più rinunciare, in quanto supporto attraverso il quale si rendono operative le decisioni, le attività con le loro interazioni, in definitiva i processi stessi: è possibile non includere il monitoraggio delle procedure di gestione di questa risorsa strategica in tale analisi dei processi? La gestione del S.I., lo si noti, è un processo essa stessa, parte integrante dei processi di supporto del processo di "main stream" del business. Ragionando ancora per assurdo, se questo non venisse inserito nel Sistema di Gestione, si tralascerebbe un processo di supporto, come se si fosse tralasciata, ad esempio, la gestione delle risorse umane, ovvero dell'assistenza post vendita (ove esista). Sarebbe un'evidente incoerenza. Infatti, cosa recita la Norma? Leggendo il § 6.3 delle Norme UNI EN ISO 9001:2000 ed UNI EN ISO 9004:2000 si evince con chiarezza che le diverse organizzazioni debbono definire, predisporre e mantenere le infrastrutture necessarie a conseguire la conformità ai requisiti dei prodotti⁹, ivi comprese le "attrezzature ed apparecchiature di processo", sia HW, sia SW. Volendo fare un piccolo sforzo, vale la pena di prendere in esame anche il § 6.5 della UNI EN ISO 9004:2000, che ci rimanda di corsa agli aspetti di gestione della Security (integrità, disponibilità e riservatezza) delle informazioni. Sì, ma domandiamoci: dove risiedono e dove vengono elaborate tali informazioni? Guarda caso, proprio nel S.I., ed attraverso di esso!

Tornando alla definizione di prodotto, è chiaro che questo, vuoi che si tratti di un bene o di un servizio, può essere ottenuto in conformità ai requisiti del cliente solo se vi è un controllo dei processi. Gli obiettivi dei diversi processi, d'altronde, potranno essere conseguiti solo grazie alle attività di controllo (!) esercitate sugli stessi. Ma come viene realizzato tale controllo nella realtà? Fatte salve le attività di coordinamento e di verifica esercitate dall'uomo, il flusso operativo delle attività e dei processi è affidato all'impiego efficace ed efficiente del S.I., con le proprie procedure ed istruzioni che sostanziano i processi.

(Continua a pagina 22)

L'Audit del SGQ: un grande assente il SI

(Continua da pagina 21)

L'Alta Direzione ed il Management in genere si devono preoccupare che tale "controllo di processo" esista e che sia efficace (possibilmente anche in un'ottica di efficienza), affinché siano conseguiti gli obiettivi aziendali. A questo fine, debbono preoccuparsi delle necessarie risorse, tra le quali deve essere considerato centrale proprio il nostro S.I. Lo si elimini, per esercizio teorico, dalle risorse tecniche aziendali, per comprendere gli effetti sul business.

Da quanto esposto, ove le diverse organizzazioni che adottano un Sistema di Gestione per la Qualità (o anche, più seccamente, un Sistema Qualità in ottica di "assurance") ritengano che la gestione del S.I. possa essere esclusa dal più generale Sistema di Gestione, appaiono operare una scelta miope, ma anche non conforme ad un requisito normativo! Da qui si ha un'ulteriore evidenza, se ve ne fosse bisogno, che i requisiti della UNI EN ISO 9001:2000 e della UNI EN ISO 9004:2000 sono frutto di un attento percorso, che appare incompleto se si legge la prima senza l'ausilio della conoscenza della seconda, che indica le cosiddette "best practices" auspicabilmente da adottare. Ancora una volta, per dimostrarlo, dimentichiamo per un attimo gli obiettivi di efficacia ed efficienza dell'Organizzazione, adottando un approccio solo notarile (*molto sbagliato, invero*). Ebbene, occorre notare che la UNI EN ISO 9001:2000 richiede, addirittura attraverso delle procedure obbligatorie, che la documentazione del S.Q. e le registrazioni relative ai controlli in essere, siano formalizzate e gestite in modo controllato (con un controllo della loro configurazione ed una sicura predisposizione, gestione, archiviazione e conservazione). In cosa si sostanzia questo requisito? Forse gli estensori della Norma intendevano far creare "carta" che servisse a gestire altra "carta"? O, più verosimilmente, intendevano far gestire, con una sorta di controllo della configurazione, le regole interne, stabilite per il corretto funzionamento dell'organizzazione e dei processi? Allora, se questo era ed è l'obiettivo di questo "controllo", non certo meschino e notarile, e se ciò che è descritto verbalmente nella documentazione del S.Q. si sostanzia operativamente nelle strutture e nel SW del S.I., come è possibile pensare che questo non sia parte integrante del sistema di gestione della qualità aziendale? E, come tale, da sottoporre a monitoraggio ed audit così come gli altri elementi del sistema medesimo?

Certo è che non tutti gli elementi costitutivi il S.I. aziendale necessitano lo stesso livello di monitoraggio ed auditing; dovranno variare sia le modalità, sia le tecniche di auditing, sia le competenze degli Auditor.

Una cosa è sicura: il S.I. costituisce parte integrante e sostanziale del sistema di gestione della qualità aziendale e come tale va monitorato e sottoposto a valutazioni periodiche di adeguatezza tecnica ed operativa, sia sotto il profilo della mera riservatezza delle informazioni gestite (cosa non affatto banale), sia sotto quello della sua efficienza ed efficacia nel rendere disponibili le informazioni, mantenendole integre sia quando memorizzate, sia quando sottoposte alle elaborazioni necessarie alla gestione dei processi.

Riccardo Bianconi

SINCERT—Responsabile Ricerca e Sviluppo, Security e Safety

CISA exam passing (Dicembre 2005)

*Lead Auditor certificato CEPAS per i Sistemi di Gestione per la Qualità,
per la Salute e per Sicurezza sul Lavoro, per la ICT Security.*

(Continua a pagina 23)

L'Audit del SGQ: un grande assente il SI

(Continua da pagina 22)

NOTE

1. *Da questo momento in poi, mi riferirò solo ai Sistemi Informatici, pur nella consapevolezza dell'importanza della componente comportamentale e di consapevolezza delle risorse umane nella gestione delle informazioni.*
2. *ISACA – Information Systems Audit and Control Association; nell'accezione dell'ISACA, un sistema Non Critico è quello "le cui funzioni possono rimanere interrotte per un lungo periodo di tempo, con un costo a carico dell'azienda modesto o nullo, e (n.d.r. per il quale) si richiede un impegno limitato (o nullo) per il riavvio quando il sistema viene ripristinato".*
3. *Sicurezza fisica, riferita al danno biologico (e, se del caso, psicologico)*
4. *OCSI - Organismo di certificazione della sicurezza di sistemi e prodotti ICT che non trattino informazioni classificate concernenti la sicurezza interna ed esterna dello Stato. In questo caso le certificazioni dei prodotti informatici sono eseguite nell'ambito dello "Schema Nazionale per la valutazione e la certificazione della sicurezza delle tecnologie dell'informazione, ai fini della tutela delle informazioni classificate, concernenti la sicurezza interna ed esterna dello Stato" (DPCM 11/4/2002 G.U. n. 131 del 6/6/2002).*
5. *COBIT – Control objectives for information and related Technologies – modello di gestione ad ampio respiro dei Sistemi Informativi, predisposto da IT Governance Institute, oggi alla sua quarta revisione; ITIL [IT Infrastructure Library] – modello di gestione dei servizi IT, pubblicato da British Office of Government e Commerce (OCG), Central Computer and Telecommunications Agency (CCTA), Londra 1989.*
6. *Si parte, ovviamente, dal presupposto di "onestà intellettuale" che tale soddisfazione sia realmente perseguita dalla Direzione Aziendale. Tale problema dovrebbe essere oggetto di una valutazione di "Moral Hazard" da parte degli stessi Organismi di Certificazione.*
7. *Quindi non sottoposta alla tutela del monitoraggio sistemico, tipico della norma UNI EN ISO 9001:2000 o della ISO 27001*
8. *Per "controllo" si deve intendere ogni presidio organizzativo e/o tecnico, deputato alla gestione di un fattore di rischio di insuccesso nel raggiungimento di un obiettivo.*
9. *Occorre ricordare che con il termine "prodotto" si può intendere sia un bene di consumo ovvero industriale, sia un servizio e/o molto spesso la combinazione dei due elementi.*

DAL BOOKSTORE DI ISACA

- COBIT 4.0
- Val IT
- Security, Audit and Control Features SAP R/3, 2nd Edition
- Managing Risk in the Wireless Environment: Security, Audit and Control Issues
- IT Governance Domain Practices and Competencies series
- Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd
- IT Governance Global Status Report

Recensione**OS/390—z/OS: Security,
Audit and Control Features****Autore: Peter Thingsted, CISA - Editore: ITGI****Pagine 525, prezzo 55 dollari. - ISBN: 1-893209-39-3****a cura di Ezio Dona' e Federico Gozzi**

Il libro si rivolge fundamentalmente a professionisti IT nella sicurezza, auditors, manager IT, sistemisti.

Decisamente completo e denso di informazioni, deve essere "centellinato" nella lettura e presuppone - per la comprensione piena di molti punti - una solida cultura "MVS inside" e una pragmatica esperienza sistemistica. Con questi presupposti e' possibile che auditors e sistemisti "comunichino" proficuamente.

La pubblicazione tratta l'auditing e la sicurezza del sistema operativo dei mainframe IBM, aspetti demandati/integrati con il prodotto programma RACF. Da un punto di vista architetturale il sistema, nato nel lontano 1964, è stato gradualmente adeguato e recentemente ha avuto una importante evoluzione tecnologica che ha integrato molte features di Unix/Linux. Z/OS è un sistema operativo complesso con enormi potenzialità verso nuove soluzioni.

L'esposizione è ottimamente strutturata e descrive molteplici punti di attenzione per l'audit (si veda la scheda con l'indice del libro), ha il merito di raggruppare e collegare in un solo testo informazioni sparse su vari manuali tecnici del MVS e del RACF fornendo inoltre indicazioni pratiche su come approfondire eventualmente i temi affrontati.

Tutto il libro è particolarmente interessante per predisporre una checklist di verifiche sui parametri del sistema operativo, in particolar modo l'ampia appendice. Citiamo ad esempio la dettagliata analisi dell'IPL, evento particolarmente critico per quanto riguarda la sicurezza.

Ci sia consentita una piccola critica. Avremmo apprezzato la presenza di un capitolo sullo Storage e sui Cataloghi.

In sintesi un valido strumento di lavoro, concreto ed operativo, che vi consigliamo.

INDICE COMMENTATO

1. Background: Operating system mvs and integrity
Descrive i meccanismi di integrità del sistema MVS con indicazione dei momenti in cui è possibile modificarne le componenti.
2. Ibm Mainframe hardware and software evolution
Breve storia dell'evoluzione dell'Hardware e del software dei sistemi mainframe IBM, e identificazione delle principali componenti.

(Continua a pagina 25)

Recensione

OS/390—z/OS: Security, Audit and Control Features

(Continua da pagina 24)

3. Hardware architecture

Vengono indicate le funzioni hardware e l'architettura associata che permette al sistema operativo di mantenere la propria integrità e quella dei task che controlla.

4. From hardware to software control

Illustra i passi di un IPL, le componenti interessate, i moduli di sistema richiamati e l'interazione con l'operatore. Vengono indicate le funzioni dei vari comandi operatore e dei moduli da questi richiamati. Uno spunto interessante per la verifica di un processo fondamentale e particolarmente critico in quanto in questa fase è possibile modificare i parametri di sicurezza.

5. Apf principles ...

Spiega la funzione delle librerie APF, i privilegi dei moduli contenuti e le implicazioni di sicurezza che ne derivano. Suggerisce una sequenza di azioni per l'audit. Si sofferma in modo approfondito su questa parte che normalmente viene solo accennata nei manuali RACF.

6. Jes2 integrity and security issues

Descrive le fasi di lavoro del JES2, le diverse modalità di accesso e i parametri del JES. Vengono indicati i rischi e le modalità di protezione disponibili su RACF per le varie aree.

7. Tso/E and ispf

Descrive i fondamenti del TSO, la modalità di connessione, i principali comandi con l'indicazione di quelli sensitivi. Evidenzia le due possibili modalità di protezione: mediante SYS1.UADS o RACF.

8. Security server/racf integrity and security issues

Descrive il funzionamento del RACF, specifica le tipologie di risorse protette mediante le diverse classi (MVS, CICS, IMS, DB2, ...); passa quindi ad elencare le informazioni gestite nei vari segmenti dei profili utente, i possibili attributi del RACF, i programmi di utilità disponibili. Descrive le modalità per ottenere reports sulla configurazione (es. DSMON) o estrarre le informazioni da SMF e suggerisce i punti principali per una revisione del RACF. Riporta le ultime variazioni previste con la versione 2.8 di OS/390 dove è possibile notare l'introduzione della parte di controllo UNIX e nuove definizioni per utenze particolari (es. protected, restricted), oltre alla parte legata ai certificati digitali.

9. Mvs audit trails: trust, detective and preventive usage

Disegna il ciclo di vita delle registrazioni del log di sistema (SMF) e ne descrive l'evoluzione nelle diverse versioni del sistema operativo. Descrive i rischi di perdita delle registrazioni e i parametri da controllare in fase di IPL per una corretta registrazione. Evidenzia le exit routine mediante le quali è possibile controllare o filtrare le informazioni da registrare su SMF.

10. Sysplex main functions

Affronta le problematiche legate alla presenza di più sistemi MVS connessi in modalità Sysplex, evidenziando i rischi insiti nella creazione di più sistemi mediante clonazione; indica dove trovare i parametri di creazione e ne descrive la funzione.

Ezio Donà, CISA, ex IS Auditor in SEC SERVIZI, si occupa di informatica da oltre 30 anni, attualmente consulente.

Federico Gozzi, CISA, IS Auditor in Reale Mutua, si occupa di informatica e qualità da oltre 15 anni.

Grow Your Knowledge With COBIT

COBIT Foundation Course™ COBIT Foundation Exam

Organizations using COBIT benefit from the development of COBIT competences among their key professionals. COBIT training courses help professionals master COBIT and utilize this knowledge for effective implementation within their organizations. Sustainable COBIT competences helps IT organizations and departments align with the goals and objectives of the business and generate strategic value from IT.

With the growing adoption of COBIT, ISACA recognized the need for structured and formal education and worked together with ITpreneurs to develop authentic COBIT learning solutions. The COBIT curriculum comprises the following courses:

- COBIT Awareness Course (2 hours, self paced e-learning)
- COBIT Foundation Course (8 hours, self paced e-learning)
- COBIT Foundation Exam (1 hour, online 40 questions)
- COBIT for Sarbanes Oxley (4 hours, self paced e-learning) (release mid-2006)

(dal sito di ISACA: www.isaca.org)

ITGI: Val IT series

ITGI has released the first deliverables in the Val IT series, a set of publications designed to shed light on realizing value from IT investments. The first release of Val IT includes:

Enterprise Value: Governance of IT Investments, The Val IT Framework

Enterprise Value: Governance of IT Investments, The Business Case

Enterprise Value: Governance of IT Investments, The ING Case Study

COBIT already provides a comprehensive framework for the management and delivery of high-quality IT-based services. It sets best practices for the means of contributing to the process of value creation. Val IT now adds best practices for the end, thereby providing the means to unambiguously measure, monitor and optimize the returns, both financial and nonfinancial, from investment in IT. Val IT complements COBIT from a business and financial perspective and will help all those with an interest in value delivery from IT.

Val IT is available as a complimentary download from www.itgi.org and for purchase in hard copy at www.isaca.org/bookstore.

Sessioni di studio

Manno (CH) - 13 gennaio 2006
Sala Anfiteatro—Centro Galleria, 2

PROGRAMMA

- 14.15 Introduzione dei lavori (Giampiero Ceppi)
- 14.30 **Alessandro Cencioni**
Introduzione all'Enterprise Risk Management
- 15.20 **Eugenio Corti**
La gestione dei rischi informatici
- 16.10 Pausa caffè
- 16.25 **Pietro Ranieri**
Un caso pratico: considerazioni sul Risk Management
- 17.05 **Alberto Piamonte**
Un caso pratico: analisi dei rischi informatici
- 17.45 Dibattito con i relatori (Silvano Ongetta)
- 18.15 Termine dei lavori

Sessioni di studio

Torino - 20 gennaio 2006
R.S.I. Sistemi
Corso Stati Uniti, 29

PROGRAMMA

- 9.15 Introduzione dei lavori da parte del Chairman
- 9.30 **Andrea Pederiva (Deloitte ERS)**
Audit di progetto
Ambito di applicazione dell'audit di progetto
Metodi per l'audit di progetto
La gestione dell'audit di progetto
Il fattore umano
Metodi quantitativi
Esercitazione
- 17.30 Termine dei lavori



Sessioni di studio

Roma - 1 marzo 2006

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 **Tavola rotonda sul tema:**

*Basilea II: il rischio di credito e la qualità delle informazioni:
stato dell'arte e prospettive*

Chairman: **Elio Molteni (CA Italia)**

Intervengono:

Alessio Camilli (Onesis)

Andrea Magurano (Poste Italiane)

Francesco Santiloni (Monte Paschi Siena)

Enrico Viola (Eclat)

Domenico Natale (Sogei)

17.20 Dibattito con i relatori

18.30 Termine dei lavori



Sessioni di studio

Milano - 27 gennaio 2006

Unicredit Servizi Informativi
Via Livio Cambi, 1

PROGRAMMA

14.15 Introduzione dei lavori da parte del Chairman

14.30 **Jann Bongiovanni (Integra)**

Tracciabilità degli utenti in ambienti multiplatforma

15.20 **Natale Trampolini**

Access & Identity Management Assessment

16.10 Pausa caffè

16.25 **Alberto Piamonte (WiseMap)**

Analisi dei rischi informatici: un caso pratico con l'utilizzo di COBIT

17.30 Dibattito con i relatori

18.15 Conclusione dell'incontro a cura del Chairman

18.20 Termine dei lavori



Sessioni di studio

Roma - 1 marzo 2006

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 **Tavola rotonda sul tema:**

Outsourcing: stato dell'arte, problemi, opportunità, soluzioni

Chairman: **Raffaella D'Alessandro (Ernst&Young)**

Intervengono:

Giacomo Aimasso (EXO Service)

Maria Dattoli (Terna)

Marco Gentili (CNIPA)

Guido Leone (EDS)

**Luigi Neirotti (Studio Legale Tributario -
Ernst & Young)**



17.20 Dibattito con i relatori

18.30 Termine dei lavori

Sessioni di studio

Milano - 24 marzo 2006

Unicredit Servizi Informativi
Via Livio Cambi, 1

PROGRAMMA

14.15 Introduzione dei lavori da parte del Chairman

14.30 **Marco Misitano , CISSP, CISM (CISCO)**

VOIP e Sicurezza: binomio possibile?

15.20 **Claudio Telmon (Next Hop)**

*La virtualizzazione dell'infrastruttura di rete:
potenzialità e rischi*

16.10 Pausa caffè

16.25 **Elio Molteni, CISSP, CISM, BS7799 – (CA Italy)**

Identity Federation: la gestione delle identità in ambiente "trusted".

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

2006, Volume 4 n.1
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: **Riccardo Bianconi,**
Ezio Dona', Federico Gozzi, Francesco
Marchiori, Orillo Narduzzo.

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,

SCRIVETECI!!

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



Al servizio dei professionisti dell'IT Governance

Capitolo di Milano



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.