

# COBIT®

## Focus

**La newsletter dedicata alla comunità degli utenti COBIT®**

Aprile 2007, Volume 1

### Direzioni per lo sviluppo di COBIT

di Roger Debreceny, Ph.D., FCPA

È prossimo il rilascio, per gli associati ISACA®, di COBIT® 4.1 e di una serie di documenti correlati che saranno pubblicati in maggio: *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance*, seconda edizione; *IT Governance Implementation Guide: Using COBIT® and Val IT™*, seconda edizione; *IT Assurance Guide: Using COBIT®*; *COBIT® Security Baseline*, seconda edizione. Infine *COBIT® Quickstart*, seconda edizione, seguirà a breve nel secondo trimestre del 2007. Tutto ciò è il risultato finale di quasi tre anni di significativi miglioramenti del framework. Preso nel suo insieme, il framework *Control Objectives for Information and related Technology (COBIT®)* fornisce, anche grazie ai suoi tool e linee guida, un supporto completo alle aziende che desiderano migliorare il contributo dell'Information Technology alle performance aziendali. Dopo un periodo di intenso lavoro che ha portato al rilascio della nuova versione e dei nuovi documenti di supporto, la comunità COBIT e IT governance ha adesso delineato la strategia per i prossimi due anni.

Coloro che lavorano allo sviluppo di COBIT sono guidati e gestiti dal COBIT Steering Committee (CSC), che lavora insieme all'IT Governance Institute® (ITGI™) ed al suo staff ed ai gruppi di sviluppo COBIT in tutto il mondo. Il CSC è formato da professionisti volontari la cui passione è migliorare la governance e la performance dell'IT. Anche i gruppi di sviluppo sono una attività completamente volontaria. Con una nuova suite di prodotti stabile, il focus del lavoro del CSC è adesso di supportare l'adozione di COBIT da parte del più ampio numero di aziende ed organizzazioni. Parlando con gli IT manager in diversi paesi di tutto il mondo si è riscontrato infatti un grande d'interesse nell'usare COBIT ed altri framework e standard correlati, tra cui l'IT Infrastructure Library (ITIL) e gli standard di sicurezza informatici dell'International Organization for Standardization's (ISO's). Gli IT manager hanno riconosciuto che l'adozione di COBIT permette di avere un framework globale che comprende gli altri standard, fornisce una base per migliorare l'allineamento della funzione con il resto dell'azienda ed aiuta a meglio

#### In questo numero...

**Direzioni per lo sviluppo di COBIT**  
di Roger Debreceny.....pag. 1

**Garantire fondamenta solide a COBIT**  
di Angelo Esposito .....pag. 3

**Alcune utili linee guida presentate all'e-Symposium COBIT**  
di Gary Hardy.....pag. 6

**Ruolo del training nell'adozione di COBIT**  
di Arjan Woertman.....pag. 8

**Nuovi Case Study COBIT disponibili online.....pag. 10**

**La foschia dei framework e standard: dove si colloca COBIT?**  
di Delton Sylvester .....pag. 11

#### 2007 Calendario degli eventi

10-11 Settembre	COBIT® User Convention Johannesburg, Sud Africa <a href="http://www.isaca.org/cobituserconvention">www.isaca.org/cobituserconvention</a>
-----------------	--

raggiungere gli obiettivi d'impresa e migliorare l'affidabilità, funzionalità e efficacia in relazione ai costi dell'IT.

Allo stesso tempo molte organizzazioni IT hanno ancora una serie di domande senza risposta. Quali framework sono i più adatti alla nostra realtà? Dobbiamo iniziare con un solo framework o adottare simultaneamente più framework? Che percorso occorre intraprendere per migliorare la nostra governance IT? Qual è l'ambito della governance e dei diversi framework di controllo?

Tutte queste domande convergono sul tema fondamentale dell'adozione di COBIT sia all'interno dell'azienda sia all'interno delle strutture organizzative di cui ci si serve. Supportare l'adozione di COBIT sarà il focus del CSC nei prossimi due anni. Al suo meeting di settembre, il CSC ha definito le principali direzioni dei piani strategici e tattici (ai quali si riferisce il processo COBIT PO1). Il CSC si sta orientando verso il completamento dei piani di implementazione di dettaglio (al quale il processo COBIT AI1 si riferisce) e la definizione di programmi di lavoro rivolti ai gruppi di sviluppo di COBIT, gli altri volontari e le risorse professionali.

Alcune delle decine di aree che il CSC ha identificato come punti chiave per supportare l'adozione di COBIT sono:

- **definizione di una road map per l'adozione del framework nelle aziende** - questo progetto è pensato per essere il complemento alla linea guida fornito nell'*IT Governance Implementation Guide*. Il progetto vuole aiutare chi ha deciso di adottare COBIT grazie ad un gran numero di case study, best practice, tool e modelli di applicazioni interne.
- **Workbench** - COBIT Online® fornisce un utile tool elettronico per supportare l'IT governance di una azienda e dare assurance ai professionisti nel loro uso dei contenuti IT. Notevoli miglioramenti a COBIT Online sono previsti nel prossimo anno.
- **Controlli applicativi** – I controlli applicativi

sono sistematicamente forniti in COBIT® 4.0 e negli ulteriori avanzamenti previsti in COBIT 4.1. I controlli applicativi sono un'area di particolare difficoltà per ottenere il controllo all'interno del più ampio ambiente informativo. Per migliorare le linee guida fornite nel framework COBIT 4.1, ITGI pianifica di produrre linee guida sulla gestione e costruzione di controlli applicativi per i business manager, l'IT management e la comunità dell'audit e dell'assurance. La guida comprenderà case study e assistenza pratica per il management.

- **End-user computing** – l'end-user computing non riguarda esclusivamente COBIT. Ci si aspetta che le aziende useranno i processi di controllo definiti in COBIT per gestire i considerevoli rischi insiti nell'end-user computing. A volte è difficile, per la maggior parte dei business e IT manager ed i professionisti dell'assurance, applicare le linee guida generali tenendo conto delle specificità dell'end-user computing. Lo scopo di questo progetto è dimostrare come i principi COBIT possono essere applicati all'end-user computing.

#### Nota dell'editore

ITGI e CSC sono sempre pronti ad ascoltare coloro che appartengono alla vasta comunità COBIT. Come possiamo servirvi meglio? Per favore utilizzate i meccanismi di feedback in [www.isaca.org/cobit](http://www.isaca.org/cobit) o contattate Brian Selby [bselby@isaca.org](mailto:bselby@isaca.org)

#### Roger Debreceeny, Ph.D., FCPA

È il presidente del COBIT Steering Committee. È Shidler College Distinguished Professor di Accounting nel Shidler College of Business, University of Hawai'i at Mānoa. Insegna accounting information systems, auditing e assurance. Le sue ricerche sono volte ai campi dei controlli IT, auditing e assurance, business reporting su Internet, tra cui XBRL e accounting information systems. L'autore può essere contattato [roger@debreceeny.com](mailto:roger@debreceeny.com).

#### Opportunità per la formazione su COBIT

ISACA offre numerose opportunità per la formazione su COBIT, tra le quali: un corso di implementazione di COBIT di due giorni ed una grande varietà di sessioni COBIT nelle conferenze in tutto il mondo. "Implementazione di COBIT per l'IT Governance" è offerto in ciascuna conferenza della serie Computer Audit, Control and Security (CACCS) così come nelle conferenze internazionali. Il seminario è anche disponibile in formula "onsite training" con erogazione da parte di varie società e trainer facenti parte della lista ufficiale approvata da ISACA.

Per maggiori informazioni e per avere la lista dei formatori autorizzati si può contattare [conferences@isaca.org](mailto:conferences@isaca.org).

## Garantire fondamenta salde a COBIT

di Angelo Esposito

A seconda del tipo di azienda, implementare il framework COBIT può essere estremamente facile o incredibilmente difficile. Per le aziende che hanno una buona base di conoscenza (se non addirittura una effettiva pratica) di processi e procedure, la battaglia è meno cruenta rispetto ad una azienda con una mentalità da "selvaggio West" o di una in cui tutte le decisioni sono guidate da una sola persona. I pericoli inerenti all'aver una sola persona responsabile per ogni decisione chiave di management sono stati evidenziati fino alla nausea e così non ne ripareremo qui. Questo articolo si focalizza invece nel modo in cui le aziende devono operare per garantire un fondamento saldo di COBIT a partire dal quale l'intero framework può essere costruito.

### Un esempio

I consulenti (incluso l'autore di quest'articolo) sono spesso chiamati in soccorso di progetti IT che rischiano di fallire. Questo è stato proprio il caso nell'esempio che segue. Negli ultimi 18 mesi, l'azienda era stata impegnata in un aggiornamento massiccio delle infrastrutture, aggiornamento destinato ad avere un impatto, virtualmente, su ogni aspetto della sua organizzazione. Con il progetto indietro di vari mesi rispetto alla schedulazione e considerevolmente al di sopra del budget prefissato, il management era alla ricerca di un modo per far ripartire il processo ormai in stallo e rimetterlo sul binario corretto.

Giunto in azienda da non più di due giorni, il consulente scoprì immediatamente la causa delle difficoltà del progetto: non era stato chiaramente identificato il business sponsor; al contrario l'azienda aveva designato più manager per supervisionare i vari aspetti del progetto. Questo approccio avrebbe potuto funzionare se ci fosse stato un amministratore a capo di tutta la gerarchia ma, sfortunatamente, non era questo il caso in questione. Il risultato era che nessuno era responsabile di coordinare le diverse visioni del management e condurre il progetto alla sua conclusione.

Durante la sua analisi il consulente aveva facilmente riconosciuto problemi e difficoltà che aveva già incontrato in molte altre aziende. La dimensione del problema poteva non essere vasta come nel caso in esame ma le cause e gli effetti erano molto simili. La situazione, comune a molti casi, poteva essere sintetizzata come segue: o l'azienda non aveva individuato un business sponsor unico oppure lo aveva designato ma lui (o lei) era priva dei requisiti necessari richiesti dall'incarico. Ciò, naturalmente, pone una domanda: quali sono i requisiti e le qualifiche che deve avere un buon business sponsor?

### Stabilire un forte processo

L'obiettivo di controllo COBIT A11.1 "Definizione e manutenzione delle funzioni di business e dei requisiti tecnici" recita che "la necessità di creare una nuova applicazione o funzione richiede una analisi preliminare sulle effettive necessità..." L'obiettivo di controllo recita, inoltre, che l'azienda deve avere "la capacità per gestire un processo che assicuri l'integrità, l'accuratezza e l'attualità dei requisiti di business come punti di partenza per il controllo dei nuovi sistemi che devono essere acquisiti o sviluppati." Infine l'obiettivo rende obbligatorio che i requisiti proposti siano sotto la ownership di un business sponsor.

In teoria tutto ciò è l'ideale. Si fissa un obiettivo, si definisce un ambiente nel quale tale obiettivo deve avere luogo e si assegna l'ownership ad una parte responsabile per la sua gestione e supervisione. Nella pratica spesso tutto ciò non è possibile. La ragione principale può essere ricondotta direttamente all'incapacità del management di selezionare il giusto business sponsor.

In molte aziende infatti non sono stabiliti i criteri per la selezione dei business sponsor. Di solito l'incarico viene assegnato a un executive che si presenta al senior management richiedendo una nuova applicazione o funzione e promettendo in cambio di incrementare i profitti. Avendo l'assicurazione di maggiori profitti, il management di solito concede carta bianca per sviluppare un prototipo. Alcune aziende si riferiscono a questa

fase con il termine "proof of concept". Con queste premesse ed un solo un obiettivo in mente, il business sponsor non ha nessun interesse né ad esaminare alternative né a condurre una preliminare analisi costi-benefici. (In un caso memorabile, l'executive management ha approvato un progetto ideato per consolidare e gestire diversi progetti di piccole dimensioni senza rendersi conto che Microsoft aveva già annunciato i propri piani per un Project Server). Non dovrebbe sorprendere dunque che tali iniziative o falliscano completamente o comunque non riescano a mantenere i risultati promessi.

In altri scenari, il business sponsor è o un senior-level executive con poco tempo o poca inclinazione nel definire in modo appropriato i requisiti di business oppure l'incarico è affidato ad un manager di livello gerarchico medio con limitate conoscenze degli obiettivi strategici di business che devono essere garantiti. In entrambi i casi questi errori critici hanno un effetto catastrofico a cascata perché impediscono che gli obiettivi susseguenti, dall'analisi dei rischi via via fino al delivery e supporto, possano essere svolti con successo. Quando l'obiettivo di controllo fondamentale, assicurare cioè l'accuratezza dei requisiti di business e tecnici, è a rischio l'intero progetto rischia la frammentazione.

Esiste una soluzione a questo problema? Ovviamente il punto di partenza è scegliere un appropriato business sponsor. Idealmente il business sponsor dovrebbe essere un senior executive che è in grado di comprendere in maniera corretta la direzione strategica ma anche tattica cioè anche i problemi giornalieri. Lui/lei

istantaneamente rispetto ma non così alto che il suo coinvolgimento possa intimidire o inibire i subordinati. Lo sponsor dovrebbe essere in grado di comprendere gli input e gli output del business, saper gestire, quando serve, le risorse esterne e saper comunicare in modo efficace quando ciò si rende necessario.

Ma la corretta individuazione del business sponsor è solo una componente, anche se forse tra le più importanti, del puzzle. Anche i business sponsor con tutte le caratteristiche in regola possono fallire. Molto spesso, il management insiste perché il business sponsor ricopra nuovi incarichi e contemporaneamente mantenga le vecchie responsabilità. Ma raramente un individuo può gestire molteplici impegni con successo. Inoltre quando da un lato si ha la familiarità di attività conosciute e dall'altro qualcosa che è nuovo e inconsueto, la maggior parte delle persone si dedica maggiormente a ciò che conosce. I potenziali business sponsor non rappresentano una eccezione a questa regola. Per vincere questa resistenza il senior management deve garantire che lo sponsor selezionato non solo abbia la giusta esperienza e gli skill richiesti ma che anche dedichi il tempo appropriato e le risorse per ricoprire in modo efficace e con successo l'incarico.

Il primo step è delegare in modo formale le responsabilità giornaliere dello sponsor a qualcun altro in azienda. C'è anche un vantaggio indiretto nel fare ciò: non solo ci si assicura che lo sponsor abbia tempo adeguato da dedicare al suo incarico ma si crea l'opportunità di assegnare ad un altro impiegato un nuovo e differente incarico;

## **Aggiornamento ricerche COBIT**

### **Nuovi documenti/white paper disponibili per il download...**

- *COBIT® Mapping: Mapping of CMMI for Development V1.2 With COBIT® 4.0*, marzo 2007
- *IT Control Objectives for Sarbanes-Oxley, 2<sup>nd</sup> Edition* – versione giapponese, febbraio 2007
- *COBIT® Mapping: Mapping of ITIL With COBIT® 4.0*, dicembre 2006
- *COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0*, dicembre 2006
- *COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0*, dicembre 2006

Questi download sono disponibile, ove non diversamente indicato, ai membri ISACA® in [www.isaca.org/downloads](http://www.isaca.org/downloads).

### **In arrivo...**

- *COBIT® Mapping: Mapping of TOGAF With COBIT® 4.0*
- *COBIT® Mapping: Mapping of COSO ERM With COBIT® 4.1*
- *COBIT® Mapping: Mapping of NIST 800-53 With COBIT® 4.1*

dovrebbe avere un ruolo aziendale abbastanza alto nell'organigramma per ottenere

di solito quest'ultimo sarà un membro delle staff di livello più basso che l'azienda vuole far

crescere professionalmente. Questo scambio incrociato di talenti contribuisce a rafforzare il management team, rafforza il morale degli impiegati aprendo loro nuove opportunità e rende più semplice che l'obiettivo di assicurare che siano garantiti requisiti di business accurati e aggiornati. Dopo aver "liberato" il tempo del business sponsor, il senior executive deve anche assicurarsi che lo sponsor abbia accesso al giusto mix tra membri dello staff interno e risorse esterne. Gli obiettivi di COBIT recitano che lo sponsor deve "identificare, documentare ed analizzare i rischi associati con i processi di business..." Valutare i rischi del processo è la componente singola più critica per decidere se andare avanti con l'iniziativa proposta. Senza un accurato assessment dei benefici e dei possibili rischi, il senior management non può prendere decisioni ben informate e ciò potrebbe portare al disastro. In questo frangente, allo sponsor è necessario il servizio di un analista di risk management. Lavorando insieme, essi possono effettuare un assessment completo ed obiettivo sui rischi potenziali che possono nascere da minacce legate alla integrità dei dati, alla sicurezza, alla privacy e garantire la compliance con le leggi ed i regolamenti esistenti. Questo assessment è particolarmente critico dato ormai tutte le aziende si muovono in un contesto normativo e regolatorio molto complesso.

L'obiettivo AI1.3 richiede di effettuare uno studio di fattibilità delle iniziative proposte; nonostante esso sia uno degli obiettivi di controllo più importanti, esso è anche uno dei più sottovalutati. Occorre ribadire allora che lo studio di fattibilità offre numerosi benefici al business sponsor.

- Apre il suo orizzonte a possibilità ulteriori oltre a quelle che esistono all'interno dell'azienda.
- Permette di incorporare soluzioni o idee che sono considerate best practice dall'industry di riferimento.
- Propone metodi alternativi (alcuni buoni altri cattivi) che possono aiutare a bypassare ostacoli o trovare soluzioni in modo più veloce.
- Fornisce un più ampio quadro dell'industry e dei competitor (presenti e futuri).

In aggiunta questo obiettivo dà allo sponsor l'opportunità di entrare in contatto con altre persone in azienda che possono avere suggerimenti ma che magari sono riluttanti a fornire spontaneamente le proprie idee ed opinioni. Lo studio di fattibilità ha inoltre un altro beneficio intangibile. Richiedendo opinioni e contributi in azienda lo sponsor può distinguere tra quelli che supportano l'iniziativa e quelli che

sono decisi ad opporsi ad essa. Questa conoscenza è fondamentale nel momento in cui occorre prendere delle decisioni. Il business sponsor ideale deve valutare in modo oggettivo i fatti e non farsi influenzare da scelte "politiche" o personali. Ciò può essere garantito raccogliendo le informazioni essenziali ed usando i dati per sviluppare modelli realistici costi-benefici. Come aiuto in questo esercizio e per assicurare che i modelli siano a "prova di proiettile" lo sponsor deve servirsi di un analista finanziario con skill in questo tipo di progetti. Niente è più convincente di una fila di numeri realistici. È difficile contestare un modello costi-benefici che prevede un 15 per cento di aumento dei profitti con un corrispondente 10 per cento di diminuzione delle spese. Allo stesso tempo però un modello poco credibile sarebbe immediatamente sospetto. Il business sponsor ideale dovrebbe cercare di emulare Sherlock Holmes: la teoria si deve adattare ai fatti e non si deve, viceversa, forzare i fatti affinché aderiscano ad una teoria preconfezionata.

Valutare gli investimenti in hardware e software richiesti per le nuove iniziative richiede il coinvolgimento e l'expertise del dipartimento IT. Per la maggior parte dei business sponsor lavorare da soli a tale aspetto può essere frustrante: di fronte allo sforzo richiesto essi cadono immediatamente malati specie quando occorre discutere su temi tecnologici che essi comprendono solo vagamente. In questi casi l'assistenza del chief information officer (CIO) o del suo designato è fondamentale. Un buon CIO – cioè uno che ha gli interessi di business dell'azienda a cuore – sarà lieto di lavorare con il business sponsor per garantire la più alta qualità ed individuare la soluzione a più basso costo disponibile. Insomma valutare correttamente i requisiti hardware e software è difficile. Il business sponsor collaborare con la sua controparte tecnologica per comprendere in pieno cosa è possibile fare cosa è cosa non lo è. Rivedere criticamente l'ambiente tecnologico attuale e determinare i cambiamenti necessari per supportare la nuova iniziativa non è facile. Tuttavia ciò non deve impedire allo sponsor di porre domande e questioni fino a che le alternative non sono chiare. I costi IT sono spesso i più importanti in agenda. È vitale che lo sponsor comprenda quali sono i costi "core" e quelli "aggiuntivi"; fallire in questo compito può portare a sottostimare in modo significativo o sovrastimare le cifre economiche dell'intero progetto. Inoltre, un buon business sponsor comprende la criticità di saper gestire nei tempi

corretti l'esecuzione dei suoi obiettivi chiave. È necessario allora stabilire prioritariamente le regole ed i criteri la review del progetto e la convalida delle sue varie fasi. I punti in cui si prendono le decisioni se andare avanti o meno devono essere chiaramente identificati e condivisi da tutte le parti coinvolte – specialmente il senior management. In un mondo ideale il senior management dovrebbe inoltre avere definito i criteri minimi di accettazione ed il business sponsor deve avere il coraggio di rifiutare requisiti che non soddisfano tali standard. Il business sponsor deve essere indifferente alle beghe politiche interne. Ci può essere del personal interno o dipartimenti che hanno interesse che una particolare iniziativa o progetto sia approvato. Il business sponsor deve avere alle spalle l'autorità del senior management quando prende la decisione finale se procedere o meno. Permettere a chiunque in azienda e fuori di interferire con interessi personali sul processo

decisionali è la causa principale del fallimento dei progetti, specie di quelli IT. Dato che il costo dell'IT è una porzione significativa delle spese operative del business, è dovere del management di finanziare solo quei progetti che soddisfano i requisiti di business e producono valore. In conclusione le aziende che vogliono eliminare o diminuire il numero di progetti IT che falliscono devono concentrarsi sul processo di selezione del business sponsor delle iniziative proposte. La scelta del business sponsor giusto è il fondamento sul quale il resto della struttura sarà costruita e costituisce la differenza tra il successo ed il fallimento. Le basi dei progetti possono essere ben saldi o friabili: la scelta tocca a voi.

### Angelo Esposito

è presidente di ATP Consulting, società con base a San Diego, California, USA che assiste le aziende nell'implementazione, in modo efficace, del framework COBIT.

## Alcune utili linee guida presentate all'e-Symposium COBIT

di Gary Hardy

Il 30 gennaio 2007 ISACA ha ospitato l'e-Symposium su COBIT. L'invito a partecipare era stato rivolto ai membri ISACA, a chi pur non essendo membro fosse certificato CISA o CISM e, infine, a chi aveva effettuato il download del materiale COBIT dal sito ISACA. In totale più di 4.800 persone si sono registrate per l'evento, e online, la partecipazione "live" ha toccato quota 2.200 durante le tre ore dell'evento. L'e-Symposium è stato archiviato ed è disponibile per il download in [www.isaca.e-symposium.com](http://www.isaca.e-symposium.com) per coloro che non hanno potuto partecipare alla trasmissione in diretta.

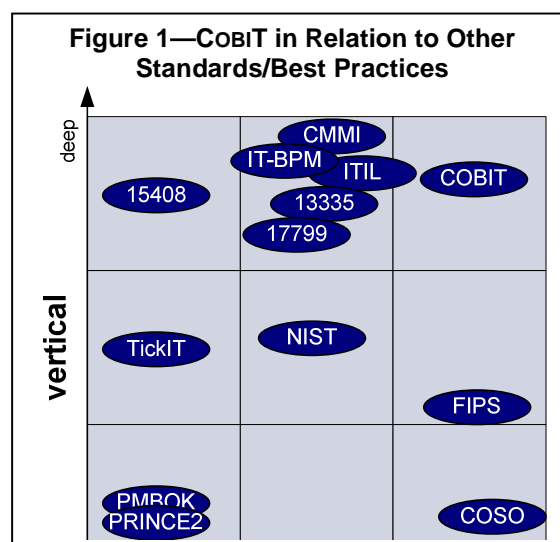
Durante l'e-Symposium sono stati presentati gli interventi di Jimmy Heschl, Gary Hardy, Roger Debreceeny e Debbie Lew.

La presentazione di Jimmy Heschl ha approfondito i principali cambiamenti in COBIT 4.1 che possono essere sintetizzati come segue:

- non è un aggiornamento ma solo un fine-tuning del framework
- miglioramento della executive overview
- miglioramento della parte relativa alle misurazioni delle performance

- sviluppo delle control practice con aggiustamenti negli obiettivi di controllo
- raggruppamento / ridenominazione di alcuni obiettivi di controllo
- semplificazione di alcuni controlli applicativi
- aggiornamento della lista degli obiettivi di business ed IT (appendice I)

Heschl ha inoltre discusso del progetto "COBIT



mapping" disponibile in [www.isaca.org/downloads](http://www.isaca.org/downloads) per gli associati ISACA ed ha confrontato COBIT con gli altri standard e best practices (vedi **figura 1**).

Gary Hardy ha approfondito il tema dell'implementazione di COBIT e dell'IT governance. I punti chiave della sua presentazione sono stati:

- Primo, comprendere perché implementare l'IT governance – riscoprire i driver.
- Implementare l'IT governance con un approccio elastico e pratico come mezzo per gestire le sfide ed i rischi dell'IT
- Rendere l'IT governance una responsabilità condivisa tra il business e l'IT, con il pieno commitment e la supervisione del board.
- Dato che si sono molti stakeholder, essere sicuri di averli identificati e coinvolti tutti .
- Usare COBIT come aiuto per:
  - facilitare il mapping degli IT goal rispetto ai business goal e vice versa
  - permettere un miglior allineamento basato sul focus al business
  - fornire una view, comprensibile per il management, di cosa fa l'IT
  - definire una chiara ownership e responsabilità orientate ai processi
  - fornire una comprensione condivisa tra tutti gli stakeholder basata su un linguaggio comune
  - garantire i requisiti COSO rispetto all'ambiente di controllo IT
- Comprendere che per avere successo rispetto ai requisiti COBIT occorre il coinvolgimento, l'awareness ed il commitment del top management; una chiara ownership dei processi IT coinvolti; e operare perché il passaggio verso le migliori practice di management avvenga in modo sostenibile.
- Usare COBIT come il framework IT di più alto livello ed insieme di best practice e risorse.
- Usare un approccio guidato dagli obiettivi di business e management per una IT governance ed un migliore IT management.
- Usare COBIT lo strumento principe per il controllo.

Roger Debreceeny ha discusso di come gli IT auditor e gli altri professionisti dell'IT assurance possono utilizzare COBIT per un ampio spettro di incarichi di assurance. I punti chiave della sua presentazione sono stati i seguenti:

- molti incarichi di assurance possono utilizzare COBIT, compresi:

- Financial statement audits
- Compliance audits
- Privacy audits
- SAS 80 internal control audits
- Value-for-money
- Process improvement
- COBIT fornisce le fondamenta per operare secondo buone prassi al di là del fatto che l'azienda utilizzi o meno il framework stesso.
- quali componenti COBIT usare nei vari incarichi.
- le control practice forniscono una guida eccellente per i professionisti dell'assurance rispetto a:
  - progettazione dei controlli
  - elementi delle management practice che devono essere posti in essere per supportare un dato obiettivo di controllo
- La nuova *IT Assurance Guide* fornisce una linea guida su come utilizzare COBIT per l'assurance e contiene i dettagli per l'assurance testing.

La presentazione di Debbie Lew si è focalizzata sui trend correnti dell'IT governance e ha anche descritto le possibili direzioni future di COBIT nei prossimi anni. I punti chiave della sua presentazione sono stati i seguenti:

- negli scorsi anni la compliance ha dominato lo scenario IT negli USA; adesso dobbiamo:
  - ottenere benefici reali dagli investimenti effettuati nella compliance
  - ridurre il costo della compliance
- l'IT governance deve essere usata per:
  - guidare la creazione del valore a partire dagli investimenti IT
  - assistere il CIO nella gestione degli ambienti IT complessi
  - integrare in maniera migliore la enterprise governance ed il risk management
- COBIT è l'unico IT governance framework che gestisce il ciclo di vita completo degli investimenti IT.
- COBIT si posiziona come strumento per la governance strategica dell'IT, sopra gli altri standard e best practice IT che forniscono linee guide di maggior dettaglio.
- Nella curva di adozione della tecnologia di Gartner, COBIT è al momento posizionato nella fase di 'early majority adoption'.
- La direzione futura prevede:
  - management framework integrati e testati
  - copertura del ciclo di vita completo dell'IT
  - adozione diffusa

Debreceeny ha descritto il lavoro in corso nel COBIT Steering Committee previsto per i prossimi due anni con il focus sull'adozione pratica di COBIT anche grazie agli ulteriori miglioramenti nel framework tra cui:

- maggiori linee guida
- maggiori tool
- più case study
- più training
- certificazione

Ciascun speaker ha anche risposto alle domande dei partecipanti all'e-Symposium. Come parte del processo di registrazione all'e-Symposium, è stato condotto un breve survey. 2.876 persone registrate hanno risposto al survey. I risultati sono schematizzati come segue.

- Il sessanta per cento degli intervistati usa COBIT nella propria organizzazione.
- Tra coloro che hanno risposto di usare COBIT, il 31 per cento usa COBIT per l'IT audit, il 10 per cento usa COBIT per l'IT governance ed il 4 per cento usa COBIT per l'IT management.
- Approssimativamente il 50 per cento di chi ha risposto valuta la difficoltà di implementare COBIT o migliorare l'IT governance usando COBIT come 'da facile a medio'.

- altri standard o framework usati insieme a COBIT (o al posto di) sono ISO 17799 (29 per cento), ITIL/CMM(I) (23 per cento) e PMBOK/PRINCE2 (6 per cento).
- Le aziende ottengono aiuto e linee guida su COBIT dai trainer commerciali (4 per cento), dagli external auditor (18 per cento), dai consulenti IT (28 per cento) e dalle pubblicazioni ITGI (49 per cento).
- Quarantaquattro per cento di chi ha risposto ha indicato di essere interessato a partecipare allo sviluppo di ulteriori ricerche e case study per l'adozione di COBIT.

### **Gary Hardy**

è il direttore di IT Winners, una società di consulenza indipendente con base in Sud Africa, specializzata in IT governance e miglioramento delle performance. Hardy è membro dell'ISACA dal 1981 ed ha ricoperto diverse posizioni di rilievo tra cui la partecipazione a diversi board dell'associazione. È advisor per ITGI e tra i fondatori e membri del COBIT Steering Committee. Hardy partecipa a progetti IT, IT audit ed IT governance da più di 25 anni per varie industry, in ambito internal audit, external audit e consulting.

## **Ruolo del training nell'adozione di COBIT**

### **di Arjan Woertman**

A cominciare dal 1996, lungo la sua evoluzione verso uno strumento di auditing, COBIT ha assunto sempre più le caratteristiche di prodotto specifico per una IT governance completa, caratteristiche che ne hanno facilitato l'adozione in tutto il mondo. Come standard, esso è coerente con le altre best practice accettate a livello globale come ITIL, ISO/IEC 27001 ed il Capability Maturity Model (CMM).

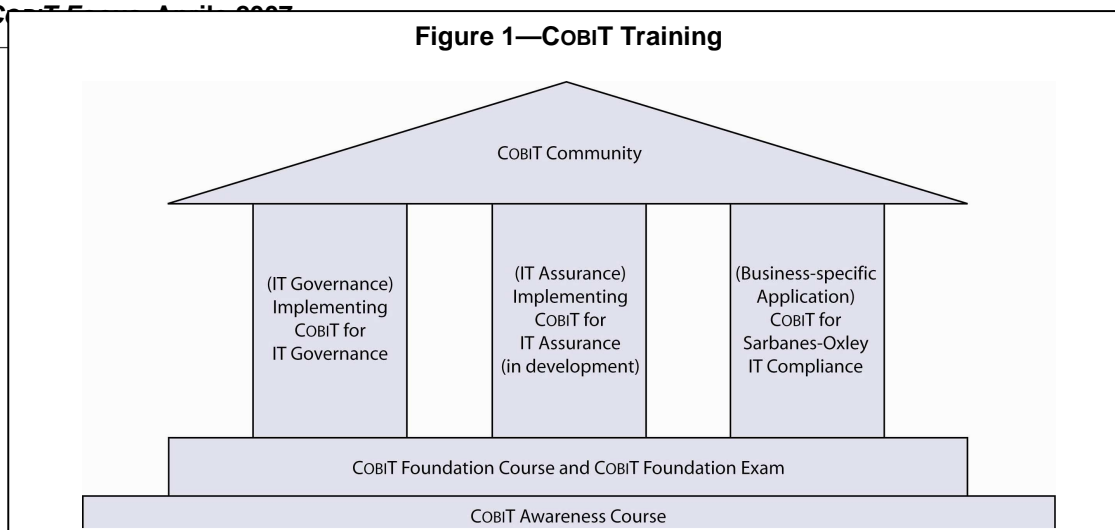
L'evoluzione di COBIT è stata continua ed è stata resa possibile anche grazie ai suggerimenti ed all'aiuto da parte di volontari e professionisti di tutto il mondo sotto la guida dell'ITGI e di ISACA. Uno dei punti di forza di COBIT è proprio la capacità di condividere le conoscenze ed expertise per mezzo della membership professionale di ISACA.

I membri supportano attivamente la continua evoluzione di COBIT eppure essi rappresentano solo una piccola porzione della comunità degli utilizzatori di COBIT la cui sfida maggiore è

proprio riuscire ad implementare in pratica, ed in maniera efficace, il modello di IT governance. Il framework COBIT ed il materiale di supporto per diventare effettivamente utilizzabile e, cosa ancora più importante, essere implementato in modo efficace hanno infatti bisogno di essere compresi ed internazionalizzati da parte di chi intende avvalersene

Senza una corretta guida e formazione coloro che sono responsabili per l'adozione di COBIT rischiamo di imbarcarsi in un viaggio pericoloso come fu per Cristoforo Colombo, il quale, pur essendo un famoso esploratore di successo rimase convinto sino alla morte di essere sbarcato sulle coste della Cina. Colombo viaggiò a lungo ma non seppe mai esattamente dove si trovasse nel grande schema delle cose.

Tutto ciò è ben cosciente in ISACA e pertanto è stata sviluppata una strategia anche formale per la formazione con l'obiettivo di guidare la comunità degli utilizzatori verso la migliore



comprensione di COBIT (vedi la **figura 1**). Con tale conoscenza, gli utilizzatori hanno chance migliori di seguire correttamente la rotta. La **figura 1** mostra i corsi COBIT che sono disponibili attraverso la rete di partner di ISACA e di ITpreneurs. I seguenti tre corsi sono indispensabili per coloro che vogliono intraprendere un viaggio intorno a COBIT.

#### **COBIT Awareness Course**

L'e-learning COBIT® Awareness Course è usato per costruire l'awareness sull'uso ed i benefici di COBIT in azienda ed è di solito rivolto a chi lavora nell'IT ed agli utenti dei processi di business chiave nonché gli owner dei processi di business. In sole due ore alle aziende viene proposto un caso reale di adozione di COBIT così da poter avere tutte le risposte di cui hanno bisogno

#### **COBIT Foundation Course**

L'e-learning COBIT Foundation Course™ è stato introdotto nel 2005 ed è stato recentemente aggiornato per tener conto delle novità di COBIT 4.1. La versione in aula del corso è stata aggiunta lo scorso anno.

Lo scopo del COBIT Foundation Course è offrire all'audience, una rapida overview del framework. Ciò li aiuta ad ottenere una chiara comprensione del framework e delle altre componenti di COBIT e dei contesti nei quali può essere usato.

#### **Implementing COBIT for IT Governance**

Questo corso, dedicato all'implementazione di COBIT, è erogato solo in aula. Il corso è essenziale per tutti coloro che hanno intenzione di giocare un ruolo importante nel processo di implementazione. Continuando con la similitudine del viaggio di Colombo, chi frequenta questo corso impara ad usare il compasso ed il sestante e a predisporre

l'imbarcazione per intraprendere il viaggio intorno a COBIT. In due giorni si impara quale sia la road map verso l'implementazione di COBIT e ad applicare i casi di studio e gli esempi relativi alla road map stessa.

Questi tre corsi aiutano le aziende nel costituire le competenze interne che supportano l'adozione di COBIT. Il training formale è una importante componente per adottare con successo COBIT ma ovviamente non è la soluzione magica per risolvere ogni problema. Proprio come Colombo, le aziende devono considerare anche altre cose. Una tempesta può portare fuori rotta la nave e la paura di ciò che è sconosciuto può condurre l'equipaggio anche alla rivolta

#### **Nota dell'editore**

ISACA collabora con ITpreneurs per realizzare e rendere disponibili corsi di formazione su COBIT di alta qualità. Tali corsi sono disponibili attraverso il portale di learning di ISACA, <http://cobitcampus.isaca.org>, o attraverso la rete di partner di ITpreneurs. Un programma speciale è disponibile per i capitoli ISACA interessati ad organizzare corsi in aula per i propri associati.

#### **Arjan Woertman**

è il product manager responsabile per i prodotti dell'area COBIT di ITpreneurs. Woertman ha guidato un gran numero di progetti chiave di sviluppo per ITpreneurs, tra i quali corsi in aula e in modalità e-learning. Lavora a stretto contatto con i maggiori esperti e le autorità di riferimento per gli standard, tra cui ISACA, per tradurre le best practice e gli standard in prodotti di formazione innovativi.

ITpreneurs è una società leader a livello globale nelle soluzioni di training per l'IT management e le best practice di IT governance.

## Nuovi Case Study COBIT disponibili online

Il sito web di ISACA ha pubblicato tre nuovi case study COBIT. Di seguito una breve sintesi degli stessi.

### **Bahrain Civil Service Bureau**

Il Bahrain Civil Service Bureau (CSB) è responsabile per la gestione delle risorse umane e le paghe per il personale di tutti i ministeri del regno. Dopo che il governo del Bahrain ha emesso una direttiva che richiede a tutte le entità governative di aderire a standard internazionalmente riconosciuti appropriati per i propri ambiti di intervento, CSB ha analizzato gli standard disponibili per l'information technology (IT) control e governance ed ha riconosciuto che COBIT fornisce un framework, personalizzabile per l'IT governance ed il controllo. COBIT è stato utilizzato per rafforzare l'infrastruttura IT del CSB ed rappresenta adesso la baseline per tutti i processi IT. L'IT governance è intesa come un progetto a lungo termine ed i processi di IT governance sono in corso al CSB.

### **Canadian Tire Financial Services Ltd.**

Canadian Tire Financial Services Ltd. (CTFS) ha oltre 1.700 impiegati e gestisce, anche finanziariamente, la Canadian Tire Options® MasterCard® per oltre tre milioni di possessori di carta di credito; si tratta di una importante entità nell'industry dei servizi finanziari. Avendo riconosciuto la necessità di implementare un programma di IT governance, la scelta di CTFS è ricaduta su COBIT. COBIT aiuta le imprese a comunicare al personale ed al management dell'IT perché è necessaria la massima cura nel sistema di controllo efficace e fornisce un framework per l'implementazione. Le componenti COBIT sono state usate con successo in diverse modalità come ad esempio per costituire il piano di review strategico per l'internal audit IT, valutare la maturità dei processi e validare l'accuratezza dello scoring dei rischi IT.

### **The Manta Group**

The Manta Group, una azienda che è una sorta di boutique per la consulenza manageriale, ha ritenuto che la IT governance fosse un fattore di differenziazione strategica per la propria clientela. L'attuale contesto del business, global

e network-centrico, richiede che l'IT contribuisca a migliorare i processi organizzativi attraverso metriche e controlli ben definiti. The Manta Group usa COBIT per aiutare i propri clienti a migliorare i loro processi e raggiungere l'allineamento con gli obiettivi di business per mezzo di controlli e metriche significative e pratiche. Dopo ricerche approfondite e con l'aiuto delle migliori expertise di riferimento, l'azienda ha ritenuto che COBIT fosse il solo framework di governance internazionalmente accettato a fornire un modello completo e sintetico per il governo e la creazione di valore dagli investimenti IT.

Per avere i testi completi di questi case study COBIT, così come di quelli sviluppati da altre aziende, tra cui Sun Microsystems, Unisys, Harley-Davidson, Allstate e Prudential, si può visitare [www.isaca.org/cobitcasestudies](http://www.isaca.org/cobitcasestudies).

### **Condividere le conoscenze su COBIT**

COBIT è di gran vantaggio per le aziende in tutto il mondo e c'è dunque una gran richiesta di case study che descrivano le diverse implementazioni.

Le esperienze descritte nei case study COBIT sono un modo efficace per condividere le esperienze di successo e le sfide che le organizzazioni affrontano. Non è necessario che si tratti di esempi di implementazioni complete: molte organizzazioni usano solo una parte di COBIT o lo usano solo in certe aree e anche queste esperienze rappresentano ottimi case study.

Inviare materiale per un case study è facile. Basta contattare [news@isaca.org](mailto:news@isaca.org) o +1.847.590.7466 per ricevere i dettagli su come agire e una lista di domande.

I membri dello staff valuteranno i case study sulla base delle informazioni fornite al fine di effettuare la review e l'approvazione definitiva. Una volta che il case study è stato approvato esso sarà incluso nella sezione dei COBIT case study dei siti web di ISACA e ITGI e, in certi casi, anche nelle pubblicazioni interne ed esterne e nel materiale di marketing.

## La foschia dei framework e standard: dove si colloca COBIT?

di Delton Sylvester

Esistono numerosi framework e standard che le aziende possono utilizzare. Il problema è che c'è, in questo momento, una certa confusione foschia su questi standard e le aziende non sono sicure di quali scegliere e di come adattarli alle proprie necessità.

Un classico esempio degli equivoci che spesso si creano sono affermazioni come la seguente: "abbiamo già [inserire qui il nome di un altro framework] e dunque non abbiamo bisogno di COBIT."

L'errore in tale affermazione può essere chiarito tenendo conto delle seguenti considerazioni sui principali framework e standard.

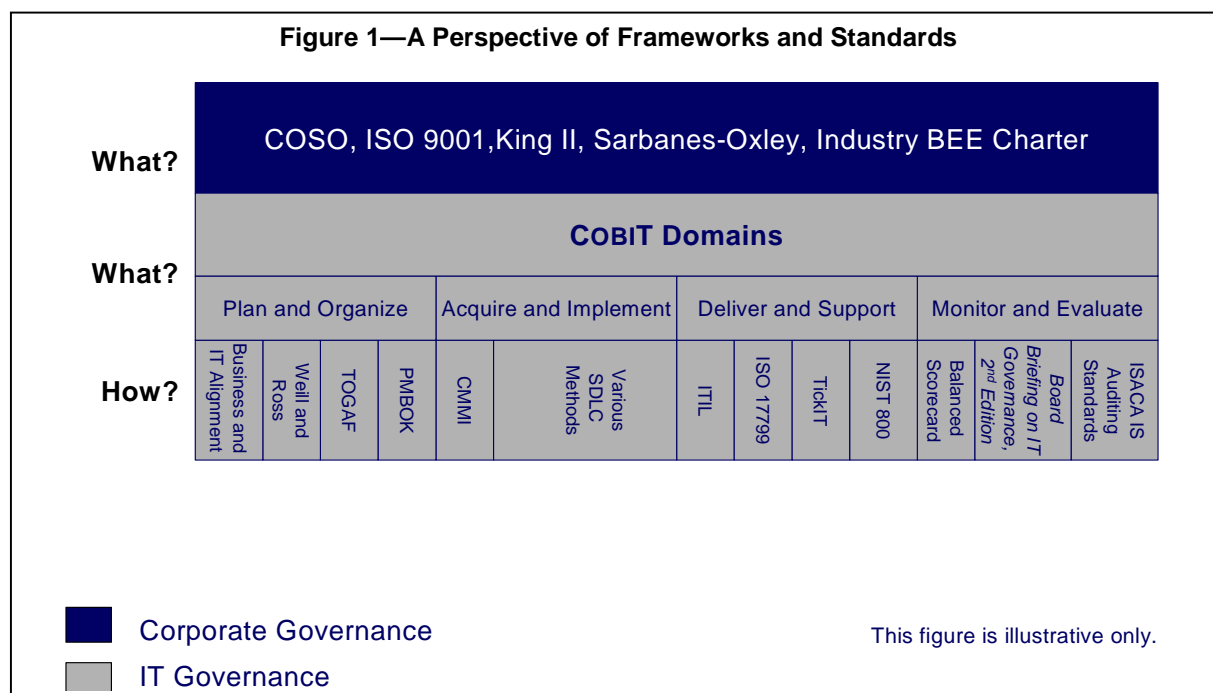
- **COSO Internal Control—Integrated Framework** - questo documento sviluppato dal Committee of Sponsoring Organizations of the Treadway Commission (COSO) consiste di quattro volumi dedicati al miglioramento della qualità del reporting finanziario e dell'etica del business per mezzo di un sistema di controllo interno efficace (corporate governance).
- **ISO 9001** - questo standard internazionale di qualità sviluppato dall'International Organization for Standardization è usato per aumentare la soddisfazione dei clienti e

gestire i requisiti regolatori (corporate governance).

- **IT Infrastructure Library (ITIL)** - si tratta di una collezione di best practice relative all'IT service management, con focus sui processi di servizio dell'IT, che si basa sul ruolo centrale dell'utilizzatore.
- **ISO 17799, Code of Practice for Information Security Management** - questo standard internazionale si basa su BS 7799-1. Elenca le best practice per implementare l'information security management
- **COBIT** - questo framework con i suoi tool di supporto si spinge oltre l'information security e l'IT service management per arrivare alla definizione delle practice generali per una IT governance sicura, efficiente, auditabile ed efficace. Esso copre tutti i processi IT, inclusa la strategia, la finanza e le risorse umane.

Sulla base di tali descrizioni, la **figura 1** mette in relazione COBIT con gli altri principali standard e framework con particolare riguardo alla corporate ed IT governance.

Come mostrato in **figura 1**, framework e



standard come COSO e ISO 90001 riguardano il cosa, cioè i principi e le linee guida, della corporate governance. COBIT riguarda il cosa (anche qui: i principi e le linee guida) della IT governance. Scendendo di livello, ITIL, per esempio, ci fornisce il come, cioè la traduzione operativa del cosa, all'interno dei domini "Deliver and Support" di COBIT per i processi che hanno a che fare con l'IT service management.

COBIT è il solo framework dedicato espressamente all'IT governance e ci aiuta a mettere sotto controllo le iniziative di IT governance. COBIT è un strumento potente di controllo e dovrebbe essere usato come baseline per ogni iniziativa di IT governance

### **Delton Sylvester**

ha oltre 10 anni di esperienza nell'industry IT con un focus chiave sul project management e l'IT governance, compresi Val IT, strategia IT, architetture IT e process design. Nel 2000-2003 è stato uno dei pionieri nell'implementazione di COBIT presso De Beers in Sud Africa. Sylvester è anche considerato un esperto su COBIT ed è spesso chiamato ad assistere le implementazioni COBIT presso le aziende. Sylvester ha anche giocato un ruolo chiave nell'implementazione della IT governance in SARS e sta al momento ridisegnando i processi IT e di business presso Hollard. Sylvester ha anche condotto corsi di disaster management che preparano i delegati a gestire i potenziali disastri nelle loro organizzazioni e recentemente è stato selezionato per realizzare un nuovo corso dal titolo "IT e la legge"..

### **COBIT Steering Committee**

Roger Debreceeny, Ph.D., FCPA, Chair, USA

Gary S. Baker, CA, Canada

Steven De Haes, Belgium

Rafael Eduardo Fabius, CISA, Uruguay

Urs Fischer, CISA, CIA, CPA (Swiss), Switzerland

Erik Guldentops, CISA, CISM, Belgium

Gary Hardy, South Africa

Jimmy Heschl, CISA, CISM, Austria

Debbie A. Lew, CISA, USA

Maxwell J. Shanahan, CISA, FCPA, Australia

Dirk Steuperaert, CISA, Belgium

Robert E. Stroud, USA

### **Editorial Staff**

Jane Seago

Chief Communications Officer

Laura Berendson

Senior Publications Manager

Jennifer Hajigeorgiou

Publications Manager

Kristen Kessinger

Media Relations

Deborah Vohasek

Media Relations

Commenti relative ai contenuti possono essere inviati a Jennifer Hajigeorgiou, publications manager, at [jhajigeorgiou@isaca.org](mailto:jhajigeorgiou@isaca.org).

*COBIT Focus* è pubblicato da ISACA e dall'IT Governance Institute. Le opinioni espresse in *COBIT Focus* rappresentano esclusivamente il punto di vista degli autori ed essi possono differire dalle policy e dagli "official statements" dell'ISACA e/o dell'IT Governance Institute e dei loro comitati nonché dalle opinioni degli altri autori, collaboratori o impiegati di *COBIT Focus*. *COBIT Focus* non attesta l'originalità dei contenuti degli articoli.

© 2007 Information Systems Audit and Control Association and IT Governance Institute. All rights reserved.

Insegnanti, docenti ed istruttori hanno il permesso di fotocopiare singoli articoli per uso non commerciale purché non richiedano un pagamento e non ne ottengano un guadagno.

Per altri tipi di copie, ristampe o repubblicazioni, deve esser ottenuto un permesso scritto da ISACA; contattare, per favore: Joann Skiba [jskiba@isaca.org](mailto:jskiba@isaca.org)

Questo numero di *COBIT Focus* è stato tradotto dalla lingua inglese da Agatino Grillo

[a.grillo@isacaroma.it](mailto:a.grillo@isacaroma.it) o [agatino.grillo@gmail.com](mailto:agatino.grillo@gmail.com)