COBIT® e ITIL®

due framework complementari

Maggio, 2007

Disclaimer

Responsabilità

Il presente documento intitolato "COBIT® e ITIL® due framework complementari", è il risultato del contributo dei singoli autori che sono i detentori dei diritti delle parti di loro pertinenza così come risulta dalla attribuzione dei singoli capitoli.

Il documento è stato prodotto per fini formativi e gli autori non garantiscono che il suo utilizzo consenta di raggiungere alcun risultato, inclusi quelli illustrati. Non si deve pertanto considerare il presente documento come comprensivo di tutte le informazioni, i metodi e/o le procedure necessari per ottenere i risultati descritti. Nel valutare l'appropriatezza di qualsiasi informazione, metodo o procedura contenute nel documento, ciascun utilizzatore deve applicare la propria esperienza ed il proprio giudizio professionale, adattati alle circostanze ed al contesto. Gli autori non garantiscono che l'Opera sia esente da errori. Gli autori non risponderanno di eventuali e qualsivoglia danni diretti od indiretti che dovessero derivare dall'utilizzo dei contenuti della pubblicazione.

Divulgazione

Gli autori concedono alle associazioni itSMF Italia, AIEA e alla SDA Bocconi, il diritto di pubblicare e diffondere il documento in via riservata ed esclusiva per un periodo di sei mesi dalla data iniziale di pubblicazione (maggio 2007). Dopo tale periodo di circolazione ristretta, il documento potrà essere divulgato liberamente dalle associazioni itSMF Italia ed AIEA, dalla SDA Bocconi e dagli autori, fatti salvi i diritti di autore. Le opinioni e le considerazioni presenti in questo documento sono da riferirsi ai soli autori e non riflettono necessariamente la posizione ufficiale di itSMF Italia, AIEA e SDA Bocconi, né dei rispettivi Enti o Società di appartenenza degli autori, in particolare di ISACA, ITGI, itSMF.

Nessuna parte di questa pubblicazione può essere utilizzata, copiata, riprodotta, modificata, distribuita, memorizzata in un sistema di archiviazione o trasmessa in qualsiasi formato diverso da PDF e tramite qualsiasi mezzo (elettronico, meccanico, fisico o altro) senza l'autorizzazione scritta delle associazioni, della SDA Bocconi e degli autori.

La riproduzione di parti di questa pubblicazione per utilizzo interno non commerciale o per finalità accademiche è consentito al termine del periodo di circolazione ristretta (sei mesi a partire dal maggio 2007) ma deve indicare l'attribuzione inequivocabile dell'origine dell'informazione. Nessun altro diritto è concesso.

La presente pubblicazione è diffusa a titolo gratuito.

Marchi

Information Systems Audit and Control Association®, ISACA® , IT Governance Institute® sono marchi registrati dell'Information Systems Audit and Control Association. ITGI® è un marchio registrato dell' Information Systems Audit and Control Association.

COBIT® è un marchio registrato dell'Information Systems Audit and Control Association e dell'IT Governance Institute.

Il logo è un marchio registrato dell'Office of Government Commerce. ITIL® è un marchio registrato dell'Office of Government Commerce ed è registrato al US Patent and Trademark Office. IT

Infrastructure Library® è un marchio registrato dell'Office of Government Commerce.

Il logo itSMF è un marchio registrato dell'IT Service Management Forum.

SOMMARIO

1 Introduzione

Chi si occupa di Sistemi Informativi deve fronteggiare esigenze spesso inconciliabili: da una parte quella di seguire con rapidità fabbisogni aziendali difficilmente anticipabili, dall'altra la necessità di presidiare con metodi e strumenti strutturati l'assetto tecnico-organizzativo del Sistema Informativo.

Da questa contrapposizione nasce il dilemma in merito al giusto compromesso tra la robustezza dell'architettura complessiva del Sistema Informativo (tecnologie, processi e organizzazione) e la necessità di dare risposte concrete alle esigenze aziendali.

La disponibilità e la conseguente adozione di standard e best practice utilizzabili come riferimenti per la descrizione dei processi e il controllo del Sistema Informativo è una delle leve a disposizione per rendere meno stridente il contrasto tra teoria e realtà.

La sola disponibilità di strumenti come COBIT® e ITIL® non basta però a risolvere il problema.

E' necessario, infatti, comprendere in quale contesto essi siano applicabili e con quali sinergie o sovrapposizioni.

Prendendo come riferimento COBIT® e ITIL® e grazie alla collaborazione tra AIEA, ITSMF Italia e SDA Bocconi questo lavoro intende dare un primo contributo all'utilizzo sinergico e complementare di queste due fonti di conoscenza che si stanno diffondendo come riferimenti de-facto per l'IT.

Il lavoro è strutturato nei seguenti capitoli:

1. Introduzione

   Presentazione dei contenuti e degli autori.

2. Le ragioni degli approcci strutturati al governo dell'IT

   Perché approcci strutturati possono aiutare l'IT e quali.

3. COBIT®

   Introduzione a COBIT®.

4. ITIL® – IT Infrastructure Library

   Introduzione ad ITIL® *v2.*

5. Confronto COBIT®- ITIL®

   Differenze, similitudini e sinergie tra i due framework.

6. Caso di applicazione congiunta: Configuration Management

   Esempio di utilizzo congiunto dei due framework.

7. Caso di applicazione congiunta: Service Level Management

   Esempio di utilizzo congiunto dei due framework.

8. L'evoluzione di COBIT® e ITIL®

   Le novità di COBIT® *4.1 e* ITIL® *v3.*

9. Bibliografia e fonti

1.1 Gli autori

Gli autori di questa pubblicazione, pur essendo singolarmente artefici di una specifica parte del documento, hanno operato in team ed hanno rivisto e riconosciuto il manoscritto nel suo complesso. Gli autori dei singoli capitoli sono evidenziati nell'ambito di ciascuno di essi; nel seguito sono riportati tutti in ordine alfabetico del cognome.

Marco Cipelletti	Vice Presidente itSMF Italia - Direttore dei Sistemi Informativi Cemat SpA
Federico Corradi	consigliere itSMF Italia - socio e Responsabile Consulenza Servizi, Cogitek S.r.L
Annamaria Iannelli	consigliere itSMF Italia - Business Development Manager Services Practice, Sun Microsystems Italia
Severino Meregalli	Head Information Systems Unit – SDA Bocconi
Orillo Narduzzo	CISA - CISM - Vice Presidente AIEA - ISACA Milan Chapter - Responsabile ICT Auditing, Banca Popolare di Vicenza
Stefano Niccolini	CISA - CISM - socio AIEA - ISACA Milan Chapter - Federazione Lombarda Banche di Credito Cooperativo
Andrea Pederiva	CISA - socio AIEA - ISACA Milan Chapter - Banca Antonveneta SpA
Maxime Sottini	consigliere itSMF Italia - CEO iCONS, Innovative Consulting S.r.l.

2 Le ragioni degli approcci strutturati al governo dell'IT

di Severino Meregalli

2.1 Perchè il governo dell'IT ha bisogno di approcci strutturati

La complessità strutturale, l'importanza della disponibilità di adeguati sistemi informativi e la rilevanza dei budget assorbiti per la loro gestione richiedono di identificare e perseguire nuove modalità di concepire e gestire i sistemi informativi. Ciò richiede di spostare l'attenzione sul tema della IS Governance e sulle modalità necessarie a ottenere una ragionevole coerenza tra necessità dell'azienda e supporto del sistema informativo. In estrema sintesi, l'IS Governance si occupa di migliorare strutturalmente il livello di allineamento dei sistemi informativi con le esigenze aziendali e, a tal fine, ricerca e raccomanda l'adozione di nuove e più adeguate modalità per la loro gestione.

2.2 La Gestione e la Governance dei Sistemi Informativi: il ruolo degli approcci strutturati

L'identificazione e il perseguimento di un nuovo modo di concepire gestire i sistemi informativi aziendali sposta l'attenzione sul tema delle modalità per ottenere continuativamente una (ragionevole) coerenza tra sistema informativo e azienda tenendo anche conto della compatibilità economica. La IS Governance può quindi essere descritta come:

"un insieme di logiche e strumenti finalizzati alla creazione di un assetto strutturale e di un contesto di governo del sistema informativo aziendale che lo rendano costantemente coerente con le esigenze aziendali in un contesto di economicità".

L'obiettivo di un ben congeniato sistema di IS Governance è quindi quello di aumentare la capacità del sistema informativo di dare risposte alle esigenze informative e di controllo dei costi in un ambiente che non consente di anticipare compiutamente i fabbisogni aziendali. Infatti a fronte di cambiamenti aziendali che evidenziano fabbisogni informativi e di automazione non definibili in anticipo (es. nuovo management, acquisizioni, merger), diviene critico poter contare su una architettura complessiva del sistema informativo in grado di garantire buone performance anche a fronte di sviluppi imprevisti.

Per ottenere questo ambizioso obiettivo è necessario agire su più aree contemporaneamente. Nella figura 1 viene presentato uno schema di riferimento per la IS governance che mostra in forma grafica le principali aree in cui è possibile scomporre il tema.

Le aree evidenziate in figura 1 rappresentano i temi che dovrebbero essere oggetto di riflessione in sede di progettazione del sistema di governante. Le stesse aree diverranno poi gli ambiti di gestione del sistema di IS Governance. L'eterogeneità delle aree e dei temi coinvolti nella realizzazione di un sistema di IS Governance richiedono l'utilizzo di metodi e strumenti specifici e specializzati. In questo contesto la disponibilità di conoscenza strutturata sotto la forma di best paractice, normative e standard di riferimento è una fonte indispensabile per favorire il processo di progettazione, implementazione operativa e di gestione di un sistema di IS Governance.

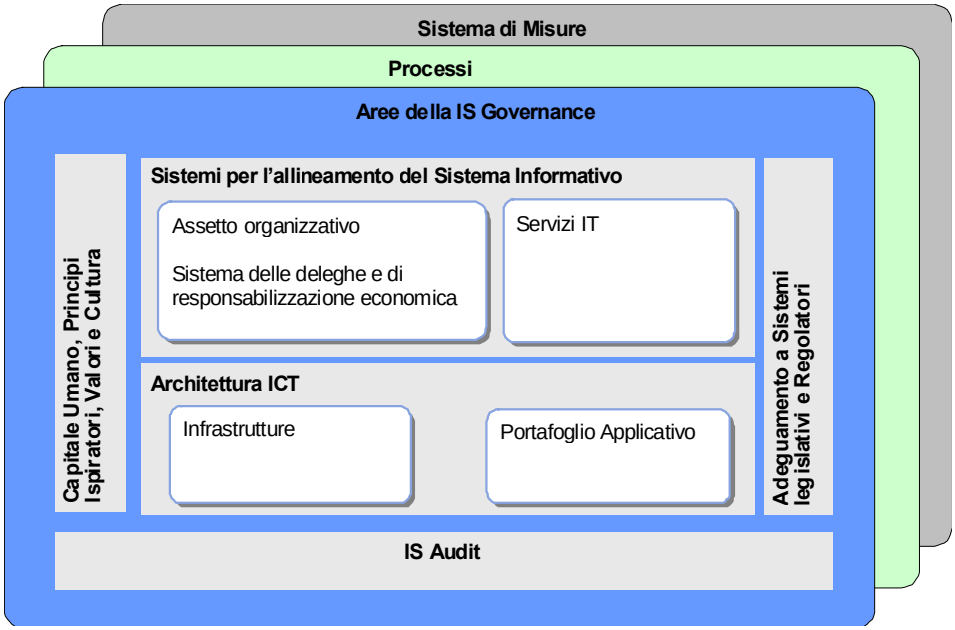

Figura 1 - Uno schema di riferimento per la Governance del Sistema Informativo

In sintesi lo schema rappresenta tre livelli:

- le aree/temi in cui si può suddividere la IS Governance;
- i processi relativi alla gestione delle singole aree;
- le misure necessarie a valutare le performance globali o specifiche del sistema di IS Governance.

2.3 Le principali fonti di conoscenza strutturata

A supporto delle attività di gestione dei Sistemi Informativi sono nati e si sono diffusi molti sistemi di conoscenza strutturata e codificata, che di caso in caso hanno preso la forma di standard, raccolte di best practice, riferimenti per la certificazione, sistemi legislativi, check list e modelli di riferimento. Pur essendo questo documento finalizzato a favorire una migliore comprensione delle caratteristiche di COBIT® e ITIL® si è ritenuto utile richiamare alcune delle più importanti fonti di conoscenza strutturata focalizzate nell'ambito dei Sistemi informativi. Ciò al fine di favorire una visione complessiva dello scenario delle fonti rilevanti per il Governo dei Sistemi Informativi.

Nella parte seguente sono descritte e messe a confronto alcune tra le fonti di conoscenza più utilizzate e diffuse. Ogni fonte è descritta sinteticamente in termini di:

- descrizione e finalità;
- ente emittente;
- contenuti;
- fonti e bibliografia.

Nella scelta delle fonti da inserire nel presente repertorio si è utilizzato il criterio della rilevanza e quello della rappresentazione della varietà dei temi della IS Governance.

Le scelte non esprimono dunque un giudizio di merito, ma solo il tentativo di descrivere la ricchezza e la varietà delle fonti disponibili tenuto conto del contesto nazionale di applicabilità.

2.4 CMMI

2.4.1 Descrizione e finalità

Il CMMI (Capability Maturity Model Integration) è una raccolta di best practice per il miglioramento dei processi focalizzato in particolare sui processi di sviluppo e manutenzione, supporto prodotti e servizi. Può essere usato per guidare il miglioramento dei processi in un singolo progetto, una divisione o una intera organizzazione. Il CMMI aiuta l'integrazione tra le funzioni di una organizzazione, fissa obiettivi di miglioramento, fornisce linee guida per l'adozione di processi per il miglioramento della qualità e aiuta a valutare i processi nello stato di partenza.

Si basa su una specializzazione del più generico CMM (Capability Maturity Model). CMMI è utile per:

- verificare la maturità dei processi implementati;
- effettuare benchmarking tra processi;
- ridurre i rischi di progetto.

2.4.2 Ente Emittente

E' pubblicato a cura del SEI (Software Engineering Institute) della Carnegie Mellon University.

SEI, Software Engineering Institute

Carnegie Mellon University

Pittsburgh, PA 15213-3890

FAX: (412) 268-5800

customer-relations@sei.cmu.edu

2.4.3 Contenuti

Il CMMI è organizzato in due parti:

- CMMI for Development (CMMI-DEV v1.2), che contiene le best practice da utilizzare per le organizzazioni che si occupano dello sviluppo di prodotti e applicazioni;
- CMMI for Acquisition (CMMI.AM v1.1), che contiene le best practice per progetti in cui le soluzioni sono acquistate.

2.5 ISO/IEC 20000

2.5.1 Descrizione e finalità

Lo standard ISO/IEC 20000 ha sostituito il precedente British Standard, BS 15000. E' stato sviluppato per fornire una base comune ed accettata a livello internazionale nel campo della gestione dei servizi IT. Copre gli aspetti del management dei servizi IT che rappresentano l'80% della spesa totale IT di gran parte delle organizzazioni. E' coerente con l'impostazione ITIL® a cui si richiama. Si propone di consentire alle organizzazioni di misurare la propria capacità di erogazione dei servizi, consentendo di confrontare tale capacità fra organizzazioni diverse.

2.5.2 Ente Emittente

E' uno standard emesso da ISO (International Organization for Standardization) e dallo IEC (International Electrotechnical Commission).

2.5.3 Contenuti

La prima parte (ISO/IEC 20000-1:2005 Information Technology Service Management) definisce i requisiti che deve soddisfare un service provider per erogare ai propri clienti servizi IT con un livello di qualità accettabile. La norma è rilevante per chi è responsabile di: progettare, implementare o mantenere il sistema di gestione dei servizi IT. E' possibile far certificare un ambito di servizi e/o di organizzazione indipendentemente dagli altri.

La seconda parte (ISO/IEC 20000-2:2005), deve essere utilizzata insieme alla precedente, e fornisce più dettagliate linee guida e raccomandazioni inerenti i processi di erogazione dei servizi IT. Tali linee guida e raccomandazioni sono l'espressione riconosciuta di standard di qualità industriali. Il documento è utilizzabile.anche come guida per gli auditor.

2.6 ISO/IEC 27000

2.6.1 Descrizione e finalità

Gli standard ISO della serie 27000 sono dedicati al vasto tema della sicurezza dei sistemi informativi. Come è avvenuto per altri standard essi saranno composti da una serie di documenti e da specifici standard. Alcuni di questi sono già stati definiti come il 27001 che rimpiazza e integra altri standard come il BS 7799.

2.6.2 Ente Emittente

E' uno standard emesso da ISO (International Organization for Standardization) e dallo IEC (International Electrotechnical Commission).

2.6.3 Contenuti

ISO/IEC 27001 è uno standard per i sistemi di gestione della sicurezza. Il suo nome completo è "ISMS: Information technology – Security techniques -- Information security management systems – Requirements". Esso stabilisce i requisiti per: definire, implementare, gestire, controllare, rivedere, mantenere e migliorare un sistema di sicurezza documentato (ISMS – Information Security Management System).

E' composto da due parti. La prima, ha la sua genesi dal British Standard BS7799, diventato ISO/IEC 17799:2000 e successivamente, dopo revisioni, ISO/IEC 17799:2005. E' un insieme di practice organizzate in 11 aree e 39 obiettivi di controllo di sicurezza. Per ogni area fornisce gli obiettivi di sicurezza ed i controlli da effettuare. Include anche linee guida per la loro implementazione.

La seconda, ha genesi dal British Standard BS7799-2, divenuto poi ISO/IEC 27001:2005. Nonostante questa seconda parte sia stata introdotta come supporto alla precedente, è diventata rapidamente il documento più rilevante poiché fornisce linee guida per costruire e mantenere l'ISMS presso un'organizzazione.

2.7 PMBOK

2.7.1 Descrizione e finalità

PMBOK (Project Management Body of Knowledge) E' una guida che raccoglie la conoscenza disponibile nel campo del Project Management. Fa parte del sistema ANSI (American National Standard – ANSI/PMI). L'obiettivo del PMBOK è quello di identificare e diffondere best practice riconosciute nel campo della gestione dei progetti. Il PMI promuove inoltre un lessico comune per discutere e applicare la disciplina del Project Management.

2.7.2 Ente Emittente

E' emesso dal Project Mamagement Institute (PMI) che ne cura la diffusione e l'aggiornamento.

2.7.3 Contenuti

Il PMBOK presenta la disciplina del Project Management organizzando la conoscenza concernente tale dominio in due dimensioni:

- la prima dimensione riguarda i processi di project management, suddivisi a loro volta in cinque gruppi;
- la seconda dimensione tratta le aree di conoscenza utili per il project management che sono trasversali rispetto ai processi per il Project Management.

I cinque gruppi di processi descritti sono:

1. Inizio: definisce e autorizza il progetto od una sua fase.
2. Pianificazione: definisce e affina gli obiettivi, i piani e le azioni necessarie per raggiungere gli obiettivi e lo scopo del progetto.
3. Esecuzione: integra le persone e tutte le altre risorse necessarie per la conduzione del piano di progetto.
4. Controllo: misura regolarmente e monitora il progresso del progetto, per identificare gli scostamenti rispetto al piano di iniziale ed intraprendere le necessarie azioni correttive.
5. Chiusura: formalizza l'accettazione dei risultati del progetto e lo porta alla sua conclusione.

Le aree di conoscenza oggetto di approfondimento nel PMBOK sono le seguenti:

1. Gestione dell'integrazione
2. Gestione delle finalità
3. Gestione del tempo
4. Gestione dei costi
5. Gestione della qualità
6. Gestione delle risorse umane
7. Gestione della comunicazione
8. Gestione dei rischi

2.8 PRINCE2

2.8.1 Descrizione e finalità

PRINCE2 (Projects IN Controlled Environments) è una metodologia per il Project Management che mira a definire un metodo generico per il project management che affronti tutte le discipline coinvolte. Si concentra in particolare sugli aspetti relativi alla giustificazione del progetto e al collegamento dello stesso con le esigenze del business. PRINCE2 è una metodologia nata in ambito prevalentemente ingegneristico, legato allo sviluppo e costruzione di sistemi, è stata formulata per essere utilizzabile come metodologia per la gestione di progetto applicabile indipendentemente dall'oggetto del progetto.

Gli obiettivi dichiarati di PRINCE2 includono:

- Favorire una comprensione condivisa dei processi e delle responsabilità del project management;
- Fornire un approccio al project management che sia valido a prescindere dal tipo di progetto;
- Garantire il coinvolgimento attivo degli utenti e di quanti sono portatori di interessi coinvolti dal progetto;
- Garantire un corretto focus sugli aspetti di business nel contesto del processo decisionale del progetto;
- Promuovere l'adozione di best practice collaudate nel campo del project management.

Gli sviluppi più recenti di PRINCE 2 (2005) hanno esteso la metodologia con contenuti dedicati al Program Management, vale a dire al coordinamento delle attività nell'ambito di un portafoglio di progetto. Vale la pena notare in questo contesto che tale aspetto risulta particolarmente pregnante ai fini dell'IT Governance, nell'ambito della quale il Project Portfolio Management riveste un ruolo di specifico rilievo.

2.8.2 Ente Emittente

PRINCE2 è stato lanciato nel 1996 in ambito governativo in Gran Bretagna per dare seguito alle richieste degli utenti in merito al miglioramento della gestione dei progetti in ogni campo e non solo in quelli aventi come oggetto i sistemi informativi. Il metodo PRINCE e stato emesso per la prima volta nel 1989 a cura della Central Computer and Telecommunications Agency (CCTA), ora British Office of Government Commerce (OGC) che continua a occuparsi della sua evoluzione.

2.8.3 Contenuti

Il modello complessivo di project management di PRINCE2 prevede otto distinti processi di management che coprono tutto il ciclo di vita di un progetto.

Essi sono:

1. Starting Up (SU). E' la fase di preparazione di un progetto ed è finalizzata ad assicurare che i pre-requisiti necessari per il suo avvio (es. mandato) siano soddisfatti.
2. Directing a project (DP). E' destinato al project board, racchiude attività di controllo e decisionali.
3. Initiating a project (IP). Riguarda la pianificazione, la definizione dei costi di progetto e la formulazione di dettaglio del business case. Il risultato principale di questo processo è il documento che definisce il cosa, il perché, il chi e il quando del progetto.

4. Managing stage boundaries (SB). Produce le informazioni necessarie per far decidere il project board sulla prosecuzione del progetto: tale decisione va riconsiderata ad ogni passaggio di fase (stage).
5. Controlling stage (CS). Sono le attività da intraprendere da parte del project manager per controllare, gestire il progetto e riferire al project board.
6. Managing product delivery (MP). Riguarda i processi collegati alla creazione e consegna dei risultati.
7. Closing a project (CP). E' il processo necessario per chiudere e finalizzare il progetto anche nel caso di fine prematura.
8. Planning (PL). E' il processo necessario per lo sviluppo di piani nelle varie fasi del ciclo di vita del progetto.

Oltre ai processi, PRINCE2 sviluppa anche 8 componenti, ovvero aspetti da gestire in un progetto, per i quali fornisce linee guida e raccomandazioni: il Business Case, l'organizzazione di progetto, i piani di progetto, i controlli, la gestione del rischio, la gestione della qualità, il configuration management dei prodotti di un progetto, il change control (ovvero il controllo dei cambiamenti effettuati sugli elementi oggetto di configuration management in un progetto).

Le tecniche di project management, come ad esempio quelle per la realizzazione dei piani, sono volontariamente fuori ambito per PRINCE2. Fanno eccezione le seguenti: il product-based planning (cuore ed elemento distintivo della metodologia), le tecniche per gestire il change control e per l'esecuzione delle quality review (controllo di qualità).

2.9 NIST 800

2.9.1 Descrizione e finalità

Gli standard emessi dal NIST (National Institute of Standards and Technology) si basano sull'ipotesi della loro accettazione e diffusione nel campo dello sviluppo e manutenzione dei sistemi informativi come linguaggio comune nella community che si occupa dei temi affrontati nelle varie sezioni del NIST. La serie 800 si concentra sul tema della sicurezza e delle architetture necessarie per il suo ottenimento.

I principi alla base del NIST 800 sono i seguenti:

- la sicurezza informatica supporta la missione dell'organizzazione;
- la sicurezza informatica è una parte integrante di buone prassi di management;
- la sicurezza informatica dovrebbe mirare ad un buon rapporto costi/benefici;
- i responsabili dei Sistemi hanno responsabilità sulla sicurezza che vanno oltre i confini delle loro organizzazioni;
- la sicurezza informatica richiede un approccio complessivo ed integrato;
- la sicurezza informatica dovrebbe essere periodicamente rivalutata;
- la sicurezza informatica è vincolata da fattori sociali.

Lo standard NIST 800 fornisce prassi comuni per la sicurezza senza fare distinzione tra aspetti tecnici, operativi e controlli manageriali. Tutte le indicazioni sono fornite secondo la stessa struttura che è simile allo standard internazionale ISO/IEC 17799 che è stato utilizzato come reference in sede di definizione del NIST 800.

2.9.2 Ente Emittente

E' emesso a cura del National Institute of Standards and Technology (NIST), ente appartenente al Dipartimento del Commercio degli Stati Uniti (US Department of Commerce).

2.9.3 Contenuti

Il documento descrive la sicurezza secondo l'approccio del ciclo di vita di un sistema. Secondo questa prospettiva che è tipica dello standard NIST le aree di conoscenza sono le seguenti:

- Inizio. Nella definizione degli obiettivi di un sistema vengono analizzate la riservatezza delle informazioni elaborate e le caratteristiche rilevanti dal punto di vista della sicurezza del sistema stesso.
- Acquisizione. Nella fase di acquisizione o sviluppo si definiscono le specifiche collegate alla sicurezza. Tali specifiche saranno utilizzate nella fase di costruzione del sistema.
- Implementazione. Nella fase di installazione e attivazione del sistema le funzionalità per la sicurezza sono utilizzate. Tali funzionalità saranno testate e, dopo l'esito positivo, verrà accettato formalmente il sistema.
- Gestione/mantenimento. Le misure di sicurezza e gli audit devono essere messi in atto nel corso della fase di produzione del sistema.
- Dismissione. Al termine del ciclo di vita del sistema le informazioni devono essere trasferite su altri sistemi e la strumentazione (es. dischi, nastri, storage) deve essere dimessa in modo sicuro.

2.10 TOGAF

2.10.1 Descrizione e finalità

Il TOGAF (The Open Group working within the Architecture Forum) è un metodo per lo sviluppo dettagliato di un'architettura IT. Il TOGAF va inquadrato all'interno di una più ampia iniziativa che mira a facilitare l'integrazione tra domanda e offerta ICT al fine di diffondere nuove tecnologie ICT nelle imprese. Le prime versioni sono state basate sui riferimenti architetturali.

2.10.2 Ente Emittente

The Open Group, nell'ambito dell'Architecture Forum è l'ente che cura la pubblicazione e la diffusione del TOGAF. The Open Group è un consorzio di circa 250 soci, raggruppanti le maggiori imprese operanti nell'IT o con l'IT nel mondo, dedicato allo sviluppo o diffusione di metodi e pratiche per il miglioramento dell'efficienza dell'IT; al consorzio partecipano organizzazioni utente, con il ruolo prevalente di definizione dei need dei business che utilizzano l'IT, organizzazioni che producono sistemi e/o erogano servizi IT, con il ruolo prevalente di favorire lo sviluppo di standard aperti per i sistemi IT. The Open Group dichiara che le organizzazioni utenti partecipanti al consorzio rappresentano circa 50 miliardi di dollari di spesa nell'IT, pari a circa il 25% della spesa IT nel mondo.

2.10.3 Contenuti

La versione attuale si concentra ancora sostanzialmente sulle architetture tecnologiche. Le più recenti evoluzioni stanno spostando il TOGAF verso una visione più complessiva dell'architettura che comprende anche le componenti non tecniche del Sistema Informativo.

Il TOGAF è composto di tre parti:

1 Il metodo per lo sviluppo dell'architettura (AMD – Architecture Development Method) spiega come definire un'architettura che sia coerente con i business requirement.

2 L'Enterpise Continuum: un catalogo virtuale di tutto il patrimonio architetturale aziendale e settoriale.

3 Le risorse (TOGAF Resource Base) quali template, guidelines e altre informazioni disponibili per aiutare l'architetto ad utilizzare l'AMD.

Nella sua evoluzione il TOGAF sta andando a coprire anche la relazione tra architettura ICT e impresa con particolare riguardo agli stakeholder e a tutte le attività che vanno oltre la mera progettazione (transformation, deployment, management e governance).

2.11 Zackman Framework

2.11.1 Descrizione e finalità

Lo Zachman Framework è uno schema di riferimento "globale" per la progettazione delle architetture dei sistemi informativi.

Esso mira a una serie di risultati:

- diventare una sorta di esperanto per facilitare la comunicazione, la ricerca e l'implementazione delle conoscenze inerenti la architetture dei sistemi informativi;
- consolidare competenze e conseguentemente diffondere cultura in merito ai concetti architetturali da parte di tutte le comunità interessate al tema (settore pubblico e privato, tecnici e manager, clienti e fornitori, ecc.);
- mantenere la neutralità del metodo, focalizzandosi sull'integrazione e sul posizionamento come strumenti che contrastano la competizione e l'errata collocazione delle compoenenti di un sistema.

2.11.2 Ente Emittente

E' emesso e mantenuto dallo Zachman Institute for Framework Advancement (ZIFA) che ha come missione la diffusione dello Zachman Framework come strumento per la definizione dell'architettura dei sistemi informativi d'impresa.

2.11.3 Contenuti

Lo schema si presenta come una tabella a doppia entrata che descrive tutte le aree di un sistema informativo che è necessario progettare in una visione olistica del Sistema Informativo stesso. Le colonne contengono le domande a cui bisogna dare risposta per progettare un sistema informativo. Ogni quesito/area è abbinato alla parte del sistema informativo che è necessario progettare per dare risposta alle varie domande. Esse sono:

- Cosa (Dati)
- Come (Funzioni)
- Dove (Rete)
- Chi (persone)
- Quando (tempo)
- Perché (motivazione)

Sulle righe sono invece rappresentate le aree su cui vanno declinati gli aspetti citati nelle colonne e l'associazione degli stessi ai ruoli coinvolti nella progettazione (tra parentesi).

Essi sono:

- Finalità (pianificatore)
- Business Model (proprietario)
- System Model (designer)
- Modello tecnologico (costruttore)
- Rappresentazione dettagliata (sub-contractor)

2.12 Six Sigma

2.12.1 Descrizione e finalità

Il Six Sigma è una metodologia rigorosa che utilizza la statistica per misurare e migliorare le performance operative di una azienda identificando ed eliminando i difetti di produzione e quelli collegati ai processi di erogazione dei servizi. La logica Six Sigma può essere definita e trattata a tre diversi livelli: metriche, metodologia e filosofia.

La finalità del sistema Six Sigma è quella di aumentare i profitti attraverso l'eliminazione della variabilità, dei difetti e dello spreco che minacciano la lealtà dei clienti. L'obiettivo è quindi l'implementazione di una strategia basata sulla misurazione che si focalizza sui miglioramenti di processo e sulla riduzione della variabilità, ottenuti attraverso il lancio di specifici progetti Six Sigma.

Six Sigma è una metodologia che fornisce al business gli strumenti per migliorare l'affidabilità dei propri processi. Questo aumento delle performance e il decremento della varianza dei processi porta alla riduzione dei difetti a ad un grande miglioramento dei profitti, del morale aziendale e della qualità dei prodotti.

2.12.2 Ente Emittente

Il termine "Six Sigma" è stato introdotto da Bill Smith, un ingegnere della Motorola, all'inizio degli anni 80. Oggi è un marchio registrato dalla Motorola. Il metodo viene affinato a cura di un movimento che si catalizza intorno ad alcune associazioni che hanno come obiettivo la diffusione dei sistemi di misura finalizzato al continuous improvement.

2.12.3 Contenuti

I progetti Six Sigma sono basati su due sub-metodologie che vengono esposte e documentate nello standard:

- DMAIC (define, measure, analyze, improve, control), un metodo per il miglioramanto di processi esistenti;
- DMADV (define, measure, analyze, design, verify), un metodo di miglioramento adatto per sviluppare nuovi prodotti o processi.

Come in precedenza illustrato, la metodologia può essere suddivisa in tre componenti:

1 Metriche. Sistemi e logiche per affrontare il tema della complessità del prodotto/processo analizzati.

2 Metodologie. Strumenti e percorsi per la soluzione dei problem (es. DMAIC)

3 Filosofia. Incentrata sulla necessità di ridurre le varianti nel business e di prendere decisioni basate su evidenze numeriche e focalizzate sul cliente.

2.13 COSO

2.13.1 Descrizione e finalità

E' un report composto da quattro volumi ed è dedicato al tema del miglioramento della qualità della rendicontazione finanziaria e degli aspetti etici attraverso l'implementazione di efficaci sistemi di controllo interno.

2.13.2 Ente Emittente

E' emesso dal Committee of Sponsoring Organizations della Treadway Commission (COSO) che è un'organizzazione volontaria nata nel 1958 per supportare un'iniziativa della commissione Americana sulle Frodi Finanziarie volta allo studio dei fattori che possono portare a frodi. Sponsorizzano l'iniziativa anche l'American Institute of Certified Public Accountants, il Financial Executives Institute, l'Institute of Internal Auditors e l'Institute of Management Accountants.

2.13.3 Contenuti

Il report è composto da quattro volumi:

1 Executive summary. Fornisce una panoramica sul quadro di riferimento dei controlli interni.
2 Framework. Definisce e descrive il sistema dei controlli interni. Fornisce anche una serie di criteri per valutare il sistema dei controlli interni vigente.
3 Reporting to External Parties. Fornisce le linee guida per emettere report finanziari secondo una metodica controllata. Si rivolge in particolare alle organizzazioni che emettono i report e alle entità di controllo che li ricevono.
4 Evaluation tools. E' una serie di materiali utili per valutare il sistema dei controlli interni.

2.14 Balanced Score Card (BSC)

2.14.1 Descrizione e finalità

Il metodo delle Balanced Score Cards (BSC) è un sistema di management che aiuta le organizzazioni a chiarire la visione e strategia e a tradurla in azione. Esso fornisce un feedback sia sui processi di business interni che sui risultati esterni. Il metodo delle BSC ha trovato diverse implementazioni settoriali e funzionali, tra cui una serie specificamente pensata per il governo dei sistemi informativi attraverso le metriche specializzate.

2.14.2 Ente Emittente

L'approccio BSC è stato sviluppato nei primi anni '90 a cura di Robert Kaplan (Harvard Business School) e David Norton. Oltre che ad un vasto movimento di "practitioner" che hanno sviluppato un'ampia documentazione ed esperienze di applicazione, le BSC sono promosse e documentate a cura dello Balanced Scorecard Institute.

2.14.3 Contenuti

Il metodo si articola e descrive quattro prospettive che sono quelle utilizzate per lo sviluppo di obiettivi e azioni per raggiungerli, di metriche per la raccolta di dati e per l'analisi dei risultati relativi ad ogni singola area. Le aree sono quattro:

- la prospettiva dell'apprendimento e della crescita;
- la prospettiva dei processi di business;
- la prospettiva del cliente;
- la prospettiva finanziaria.

2.15 Un quadro di riferimento degli approcci più diffusi

Nel presente paragrafo, sulla base delle caratteristiche delle fonti elencate, viene proposta una collocazione delle stesse all'interno del quadro di riferimento proposto all'inizio del capitolo. Tale collocazione è solo indicativa e intende soprattutto segnalare quale sia la principale peculiarità di ogni standard e normativa. Nei casi di corpi di conoscenza che coprono vaste aree si sono privilegiate quelle su cui si focalizza maggiormente il riferimento scelto.

Come si può osservare gran parte delle aree in cui è stato scomposto il tema della IS Governance sono collegabili a una o più fonti di conoscenza strutturata. La mappatura mostra due aspetti per certi versi contraddittori.

Da una parte dimostra l'esistenza di svariate fonti di conoscenza e best practice fondamentali per supportare operativamente il processo di progettazione, implementazione e gestione di un sistema di IS Governance. La numerosità delle fonti disponibili, che sono ben di più di quelle descritte nel presente documento, e l'ampiezza delle aree coperte costituiscono un patrimonio fondamentale per chi voglia affrontare il tema del governo dei Sistemi Informativi.

Al tempo stesso tale ricchezza di sistemi di riferimento porta però a sovrapposizioni e a evoluzioni non sempre coordinati ed organici. Questo fatto richiede dunque uno sforzo di astrazione e collocazione degli strumenti disponibili all'interno di un framework che funga da guida per la scelta e l'adozione dei riferimenti di volta in volta coerenti con le esigenze aziendali. L'assenza di un quadro di riferimento aziendale che crei un contesto sinergico per l'adozione di strumenti quali ITIL® e COBIT® può allontanare dall'obbiettivo di incidere positivamente sulle performance complessive del Sistema Informativo Aziendale.

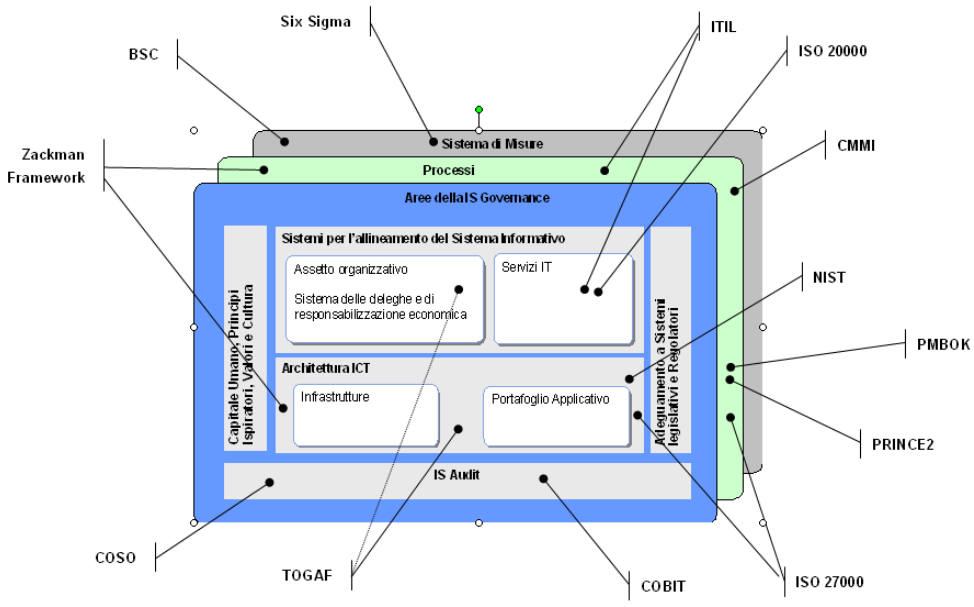

Figura 2 - Mappatura delle fonti di conoscenza all'interno del framework per la IS Governance

3 COBIT

Di Orillo Narduzzo, Stefano Niccolini, Andrea Pederiva.

3.1 Origini ed evoluzione di COBIT

Per capire la storia di COBIT® è necessario conoscere la storia di ISACA, Information Systems Audit & Control Association, associazione internazionale di professionisti dell'Information Systems Audit e dell'IT Governance[1].

ISACA nasce nel 1969, con il nome di Edp Auditors Association. Dopo alcuni anni di incubazione, EDPAA conosce una veloce espansione a livello internazionale e raggiunge i 50 "chapters" nel 1981 ed i 100 "chapters" nel 1986. Nel 1979 viene fondata AIEA – Capitolo di Milano di ISACA, primo dei capitoli europei.

Nel 1976 viene costituita EDPAF, EDP Auditors Foundation, con il compito di pubblicare la prima rivista di settore, l'allora "EDP Auditor Journal" oggi "IS Control Journal", nonché di promuovere, condurre e sviluppare progetti di ricerca nell'ambito della professione di IS Auditor.

E' di quegli anni la pubblicazione delle prime ricerche sui "Control Objectives" applicabili all'IT.

Il progetto di sviluppo di COBIT® si può far risalire al 1992 come collaborazione volontaria di ricercatori presso alcune Università in Europa (Free University of Amsterdam), Stati Uniti (California Polytechnic University, Pomona) ed Australia (University of New South Wales), con il coordinamento di EDPAF.

Le Università coinvolte furono incaricate di predisporre una prima bozza dei "Control Objectives" a partire da un framework predefinito e integrando materiale proveniente da standard professionali, standard tecnici, codici di condotta, standard di qualità e professionali, pratiche di industry.

Nel 1994, su proposta e guida di Erik Guldentops, i Control Objectives furono rivisti; venne identificato un insieme tipico di processi di gestione dell'IT naturalmente aggregati in domini, e si individuarono per ciascuno di tali processi le migliori pratiche di controllo finalizzate alla gestione dei rischi. Il lavoro fu coordinato dal COBIT® Steering Committee, e COBIT® 1.0 fu infine pubblicato nel 1996, edito da "ISACF – Information Systems Audit & Control Foundation", il nuovo nome di EDPAF. COBIT® 1.0 era già costituito dal nucleo di quella che sarebbe diventata la cosiddetta "suite COBIT®": il Framework e i Detailed Control Objectives.

La seconda edizione di COBIT® fu rilasciata da ISACF nel Luglio del 1998. COBIT® 2.0 presentava una versione rivista del Framework e dei Control Objectives, sulla base di un insieme di documenti di riferimento più completo; veniva completato con le Audit Guidelines, contenenti linee guida di audit relative ad un generico processo di revisione sull'IT e specifiche per ciascuno dei processi di gestione dell'IT presenti nel framework; COBIT® 2.0 includeva inoltre una prima versione dell'Implementation ToolSet ed era disponibile su CD Rom.

[1] Website: www.isaca.org; ISACA associa oggi oltre 50.000 professionisti in 170 capitoli di 140 paesi diversi.

A Luglio 2000 fu pubblicato COBIT® 3.0 dal nuovo editore di COBIT®: l'IT Governance Institute (ITGI) fondato proprio nel 1998, con finalità di ricerca e diffusione della conoscenza sui temi dell'IT Governance.

Le novità introdotte con la pubblicazione di COBIT® 3.0 segnano rispetto alle versioni precedenti un punto di discontinuità in termini qualitativi e di contenuti, coerente con il crescente interesse di ISACA e di ITGI per i temi dell'IT Governance.

La principale innovazione introdotta, in linea con la mission di ITGI per l'IT Governance, furono infatti le Management Guidelines, comprensive di Maturity Model, Key Performance Indicator, Key Goal Indicators e Critical Success Factors per ciascuno dei 34 processi.

La pubblicazione delle IT Management Guidelines – risultato di un progetto di ricerca condotto da Gartner Group - introdusse per la prima volta nella suite COBIT® degli strumenti specificamente finalizzati alla gestione ed al governo dell'IT, ulteriori rispetto ai precedenti contenuti a supporto delle attività di revisione sull'IT.

Le Management Guidelines ampliavano in modo significativo la platea dei destinatari di COBIT®; alla comunità degli IT auditor si aggiungevano in modo specifico il ruolo degli IT manager, e più in generale tutte le figure con responsabilità di gestione dell'IT.

La pubblicazione delle Management Guidelines colse nel segno, rispondendo ad una domanda di conoscenza che chiedeva di razionalizzare metodi e pratiche che andavano diffondendosi.

Il crescente interesse per COBIT® negli anni successivi indusse ISACA a sviluppare nel 2003 "COBIT® Online", accedibile via internet, inizialmente costituito da un database contenente i Control Objectives, e successivamente arricchito con la possibilità di filtrare i contenuti di COBIT® rispetto ai più importanti elementi costitutivi del modello (quali ad esempio i processi, le risorse IT, i requisiti di business per le informazioni ed altro).

Inoltre, con "COBIT® Online" è stata introdotta la possibilità di confrontare la propria organizzazione con altri utenti – omogenei per industry, dimensioni, area geografica – rispetto ad alcuni indicatori quali ad esempio il livello di maturità dei processi.

La suite COBIT® venne ulteriormente arricchita nel 2004 con le COBIT® Control Practices: definite come "key control mechanisms" finalizzati al conseguimento degli obiettivi di controllo; in sostanza, le Control Practices dettagliano le concrete attività di controllo da porre in essere per il conseguimento degli obiettivi di controllo previsti dal framework COBIT®. Con il rilascio delle Control Practices la versione di COBIT® venne portata a 3.1.

Le attuali Control Practices sono basate sugli obiettivi di controllo di COBIT® 3.0 e prevedono almeno due attività di controllo per ciascun obiettivo di controllo di dettaglio; è in corso l'allineamento delle Control Practices agli obiettivi di controllo di COBIT® 4.0.

Sempre nel corso del 2004 venne avviato il progetto per le revisione dell'intera suite COBIT®; tale progetto aveva come obiettivo quello di rispondere alle sfide ed alle opportunità nel frattempo emerse, anche come conseguenza dell'evoluzione del quadro normativo, che avevano fatto emergere l'esigenza di standard per la Corporate Governance, e che avevano favorito l'affermarsi di COSO quale framework di riferimento per la Corporate Governance e di COBIT® per la sua declinazione sull'IT.

In tale ambito ricordiamo in particolare la pubblicazione "COBIT® Control Objectives for Sarbanes-Oxley", prima e seconda edizione, risultate essere le pubblicazioni più scaricate dal sito ISACA nel 2005.

Con il progetto COBIT® 4.0 si è inoltre consolidata la struttura di ricerca guidata da ISACA per lo sviluppo di COBIT® stesso; tale struttura di ricerca è governata dal COBIT® Steering Committee.

Lo Steering Committee guida i gruppi di ricerca, composti da volontari soci ISACA, docenti universitari ed esperti di settore di tutto il mondo; la finalizzazione e l'approvazione ultima di tutto il materiale è riservata allo Steering Committee.

Il progetto per la revisione di COBIT® 3.1 si è concluso con il rilascio di COBIT® 4.0 a dicembre 2005. Le principali modifiche introdotte con la versione 4.0 rispetto alla versione 3.1 si possono riassumere come segue:

- E' stato rivisto il modello dei processi; in particolare è stato introdotto il processo di "IT Procurement" ed eliminato il processo "Esecuzione di audit indipendenti" considerato non IT; altri processi sono stati rivisti, rinominati e/o aggregati; complessivamente i processi sono rimasti 34, suddivisi in 4 domini; il volume COBIT® 4.0 include una mappatura completa e di dettaglio fra le due versioni 3.1 e 4.0;
- Il modello dei processi e gli obiettivi di controllo sono stati meglio allineati al contenuto di ITIL®;
- I Control Objectives sono stati riformulati utilizzando i verbi alla forma imperativa piuttosto che al condizionale;
- Le Management Guidelines sono state incluse in un unico volume insieme ai Control Objectives; le principali innovazioni nell'ambito delle Management Guidelines includono la soppressione dei Critical Success Factors, la rivisitazione degli indicatori di Performance e di Risultato su più livelli secondo la teoria delle Balanced Scorecard multilivello, l'introduzione di un modello di riferimento organizzativo rappresentato mediante diagrammi RACI (Responsible, Accountable, Consulted, Informed), e la definizione di relazioni di input/output fra i processi dell'IT previsti dal framework.

Con il rilascio di COBIT® 4.0 la suite assume la propria configurazione attuale, illustrata con maggiore dettaglio al successivo paragrafo "I contenuti di COBIT® ".

La figura n.1 illustra in sintesi le principali tappe nell'evoluzione di COBIT® .

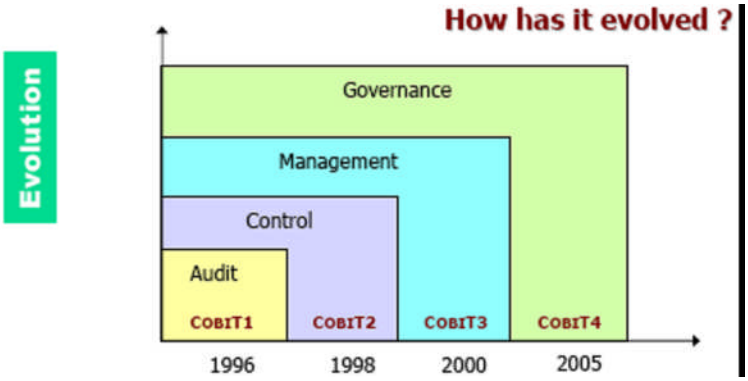

Figura 1 – Principali tappe nell'evoluzione di COBIT.

L'evoluzione e la diffusione di COBIT® sono andate di pari passo con un sempre maggiore riconoscimento dell'insostituibilità delle risorse IT per l'ottenimento degli obiettivi di business di qualsiasi impresa moderna e della necessità di porre in primo piano le problematiche del top management anche nell'ambito del governo dell'IT.

Per tale ragione accanto al tradizionale know how concernente il controllo e l'audit dei sistemi informativi, COBIT® si è evoluto fino a includere gli attuali strumenti di Governance per l'IT, al quale, interno o esterno all'organizzazione utente, vengono

riconosciute specificità che rendono necessario l'utilizzo di strumenti di gestione e controllo tipicamente imprenditoriali.

Nella sua evoluzione, COBIT® ha anche perseguito l'obiettivo di diventare uno standard "*de facto*", "generalmente accettato ed applicabile", per il governo ed il controllo dell'IT. Il successo di COBIT® nel perseguire tale obiettivo è testimoniato dal suo riconoscimento come framework di riferimento per la Governance dell'IT dalla Commissione Europea e da altri organismi governativi nel mondo.

Il termine "generalmente accettato e applicabile" è esplicitamente inteso con lo stesso significato dei *Generally Accepted Accounting Principles* (GAAP).

3.2 Chi lo utilizza e perché

Pubblicato inizialmente come supporto alle attività di revisione dell'IT, COBIT® nella sua veste attuale è strumento fruibile per molti ruoli aziendali.

Anche come conseguenza dell'ampio insieme di potenziali ambiti di utilizzo del framework, l'applicazione di COBIT® non può essere immediata: è indispensabile una applicazione selettiva che tenga conto di elementi di discrimine, tra i quali ad esempio:

- le caratteristiche dell'azienda (tipo di business, dimensione, disponibilità/avversione al rischio, requisiti regolamentari, politiche interne, ecc.);
- gli obiettivi dell'area aziendale all'interno della quale si intende applicare la metodologia.

Discutiamo nei paragrafi seguenti le principali applicazioni dei contenuti della suite COBIT® per alcuni fra i principali ruoli aziendali:

- Alta Direzione;
- Direzione e Direzione IT;
- Responsabili d'area/di processo nell'ambito della Direzione IT;
- Auditor.

3.2.1 Alta Direzione [2]

In COBIT® 4.0 è dichiarato l'obiettivo di proporsi come metodologia che possa supportare l'Alta Direzione nell'implementazione di opportune pratiche di IT Governance.

A tal fine COBIT® va visto come strumento che:

- mette a disposizione dell'Alta Direzione un insieme di strumenti applicabili per il governo ed il controllo dell'IT;
- supporta l'Alta Direzione nell'applicazione di tali strumenti proponendo opportuni percorsi per l'implementazione dell'IT Governance, descritti in particolare nei documenti dell'IT Governance Institute.

I principali strumenti che COBIT® mette a disposizione per governare e valutare la funzione IT sono costituiti da:

- Strumenti per la definizione del modello dei processi e dell'organizzazione IT, costituiti dal modello dei processi con i relativi input ed output documentali e dai modelli organizzativi "Chi fa che cosa" documentati nei diagrammi RACI[3];

[2] Executive Management and Boards

[3] Responsible, Accountable, Consulted, Informed.

- Strumenti di benchmark per la maturità dei processi; COBIT® 4.0 include un modello di maturità per ciascuno dei processi di governo e gestione dell'IT. Tali modelli consentono alle singole organizzazioni di misurare il livello di maturità dei propri processi IT; tale indicatore può essere confrontato nel tempo, osservando l'andamento del livello di maturità dei propri processi, nonché confrontato con il livello di maturità dei processi IT di altre organizzazioni – il più possibile simili per dimensioni, settore ed area geografica – accedendo ai dati di benchmark raccolti e pubblicati da ISACA;
- Strumenti di misurazione dell'efficacia, efficienza e rischio nei processi di governo e gestione dell'IT; per ogni processo viene proposto un modello di balanced scorecard multilivello, comprensivo di obiettivi e metriche (KPI – Key Performance Indicator e KGI – Key Goal Indicator) per i livelli Business, IT, e Process [4];
- Strumenti per la definizione e valutazione del proprio sistema di controllo interno sull'IT, da confrontarsi con il modello di riferimento COBIT® proposto nel volume "Control Objectives"; tale framework è il modello di riferimento generalmente accettato nel mondo per il controllo interno sull'IT[5].

Gli strumenti citati possono essere utilizzati dall'Alta Direzione nel contesto di corrette pratiche di governo dell'IT finalizzate a conseguire i principali obiettivi strategici definibili per l'IT:

1 Allineamento strategico dell'IT con il business;
2 Creazione di valore;
3 Gestione Economica delle Risorse (Applicazioni, Informazioni, Infrastrutture e Personale);
4 Gestione del Rischio;
5 Misurazione delle Performance.

Il conseguimento di ciascuno di tali principali macro-obiettivi prevede l'applicazione congiunta e coordinata di uno o più degli strumenti di management sopra elencati, insieme con le pratiche di governo e controllo previste da uno o più dei processi COBIT® in cui sono raggruppati i Control Objectives.

In ultima analisi l'utilizzo dell'IT da parte del vertice aziendale è finalizzato alla produzione strutturata e tempestiva di informazioni di dettaglio e di sintesi per sé e per gli utenti dell'organizzazione, interni ed esterni.

L'implementazione di opportune pratiche di IT Governance suggerite dal modello (v. figura n.2) è importante per il controllo complessivo sull'IT e per fornire un ragionevole livello di confidenza che gli obiettivi assegnati o che persegue l'IT siano coerenti con quelli di business e siano raggiunti in modo efficace ed efficiente.

[4] Tali strumenti di management sono conosciuti come IT Balanced Scorecard, e rappresentano l'evoluzione applicata all'IT delle Balanced Scorecard inizialmente proposte da Kaplan e Norton.

[5] Ad esempio, è noto che CobiT viene di norma utilizzato come modello di riferimento sulla base del quale arrivare a conclusioni condivise fra soggetti auditati e revisori, supportando il confronto e la comunicazione fra i vari soggetti potenzialmente coinvolti in una revisione dell'IT: personale IT, revisori IT interni, revisori IT esterni.

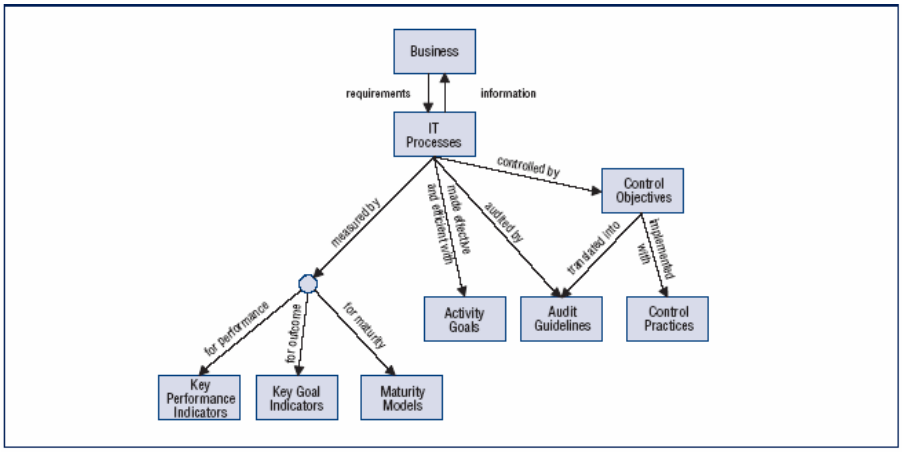

Figura 2 - Relazioni fra le componenti di COBIT .

3.2.2 Direzioni di Business e Direzione IT

Lo sviluppo, l'aggiornamento e la gestione dei sistemi informativi sono visti in COBIT® come un processo essenziale ma subordinato al raggiungimento degli obiettivi strategici dell'organizzazione utente.

La Direzione dei sistemi Informativi trova in COBIT® la definizione di una struttura di processi virtuosa volta ad assicurare la costruzione di un sistema informativo efficiente, efficace e documentato.

Indirizzato a una qualsiasi organizzazione che utilizzi l'IT a supporto delle proprie attività, COBIT® individua alcuni *Requisiti di Business* di tipo generale e su questi innesta il processo di collegamento con le risorse ed i processi IT.

Il riferimento ai processi suggeriti da COBIT® è utile per il progetto architetturale ed organizzativo dei Sistemi Informativi.

È possibile procedere senza la necessità di "reinventare la ruota" e con ragionevole confidenza di conseguire gli obiettivi avendo esaminato e considerato tutti gli aspetti rilevanti. In ogni passaggio i responsabili di business e i responsabili IT, sempre in modo coordinato ed eventualmente in modo congiunto, sono stimolati anche alla valutazione delle vulnerabilità e dei rischi ed alla definizione dei controlli.

Con l'utilizzo di COBIT®, le Direzioni di Business e la Direzione IT possono farsi parte diligente e proattiva verso l'Alta Direzione per l'adozione di buone pratiche di gestione dell'IT.

3.2.3 Funzioni di sviluppo e gestione dell'IT

COBIT® rende disponibili obiettivi di controllo specifici per singolo processo, utili per la definizione e la gestione dei processi di sviluppo ed erogazione dei servizi IT.

Anche a livello di pianificazione, progettazione, realizzazione ed erogazione di servizi IT, COBIT® si propone come strumento a presidio dei rischi che possono comportare sprechi di risorse e difficoltà nell'erogazione dei livelli attesi di servizio.

E' opportuno ricordare che gli obiettivi di controllo non devono essere considerati in modo "rigido" e che ogni organizzazione deve individuare gli obiettivi di controllo rilevanti rispetto al proprio business, alla propria dimensione, ed al contesto dei requisiti e dei rischi da presidiare; è necessario ricordare inoltre che COBIT® non si propone come framework di riferimento collegato a specifiche tecnologie.

In sintesi, i responsabili di singole aree o processi all'interno dei Sistemi Informativi potranno trovare in COBIT® un riferimento utile alla definizione del processo e/o alla organizzazione dell'area sotto la propria responsabilità. Essi potranno utilizzare COBIT® come promemoria dei requisiti che i processi debbono soddisfare – definiti assieme a opportune metriche per misurarne il livello di soddisfacimento – con la consapevolezza che il soddisfacimento di tali requisiti consente di essere ragionevolmente confidenti che gli obiettivi di ciascun processo saranno raggiunti.

3.2.4 Sicurezza

In COBIT® al processo di gestione della Sicurezza informatica sono dedicate specifiche sezioni, ed in particolare i processi PO09 – Assess and Manage IT Risks – nel dominio Planning & Organisation, e la sezione DS05 Ensure Systems Security – nel dominio Delivery and Support.

Dai contenuti di tali sezioni i responsabili per la gestione della Sicurezza possono ottenere specifiche indicazioni e riferimenti per il conseguimento dei requisiti di Disponibilità, Integrità e Riservatezza delle Informazioni.

3.2.5 Auditor

Il modello COBIT®, nato per supportare le attività di revisione dell'IT, continua ad onorare anche la sua mission originaria, pur avendola ampliata in modo sostanziale. L'auditor trova supporto in COBIT® a diversi livelli, in particolare nell'individuazione di:

- processi chiave e critici per la gestione dell'IT (supporto alla realizzazione di programmi di Audit basati sul rischio);
- linee guida complete per lo sviluppo di piani di Audit generali o specifici per obiettivi di controllo, componibili in modo coerente rispetto al mandato di Audit.

COBIT® non è diretto in modo esclusivo all'Auditor dei Sistemi Informativi. La metodologia si presta ad essere utilizzata anche parzialmente come supporto per Audit di tipo tradizionale (Operational e Financial Audit) laddove siano da svolgere verifiche anche sui sistemi informativi a supporto del business incluso nel perimetro (scope) dell'Audit.

Per l'auditor si tratta di uno strumento di lavoro utile e stimolante. Dato l'ambito di indagine, possono essere reperiti i processi IT significativi per l'ambito medesimo e gli obiettivi di controllo diventano il riferimento per le verifiche sullo stato del sistema dei controlli (preventivi, detettivi[6], correttivi) attivati dall'organizzazione a riduzione dei rischi associati ai processi medesimi.

3.3 L'utilizzo di COBIT

COBIT® non è un "manuale", bensì un insieme strutturato di "strumenti" destinati a diversi livelli nelle organizzazioni aziendali, individuati in:

a. Consiglio di Amministrazione e Alta Direzione;

b. Direzioni di Business e IT;

c. Aree professionali coinvolte nella Sicurezza;

d. Responsabili delle funzioni di Controllo Interno e di "Assurance".

[6] Detti anche "di rilevazione".

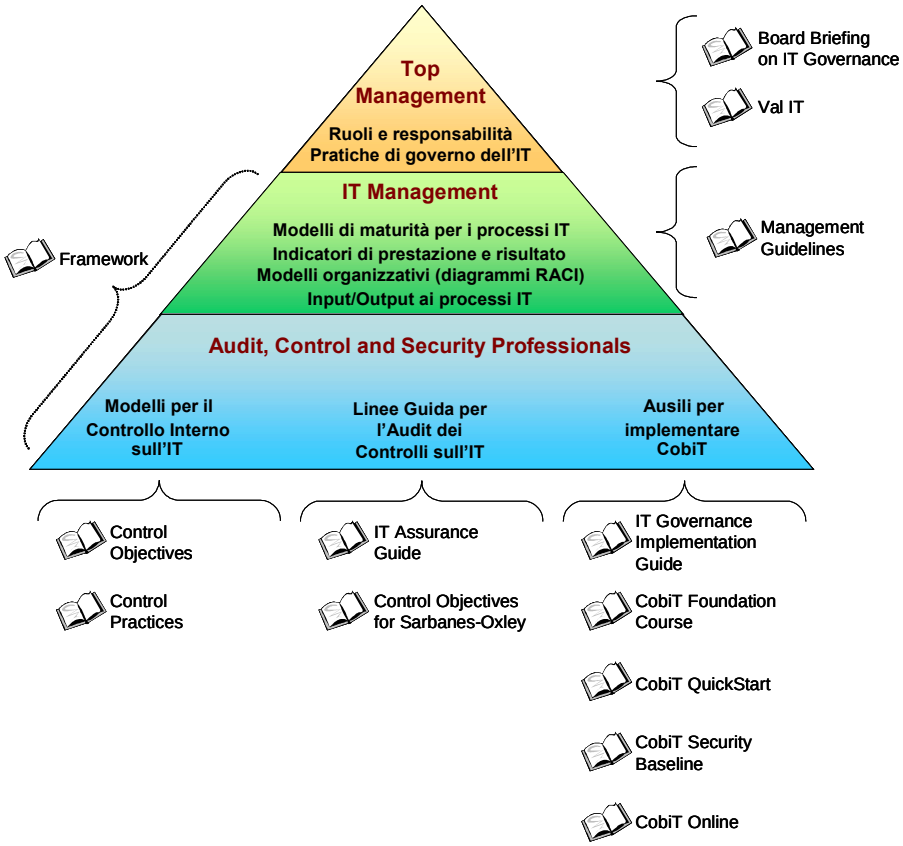

Figura 3 - Le componenti della suite COBIT.

Ciascuna componente della suite COBIT® include contenuti di norma dedicati a specifiche ruoli e/o profili aziendali, naturalmente correlati al contenuto di ogni altra componente:

- Il Framework è indirizzato all'Alta Direzione ed in generale a chi desidera conoscere COBIT® senza entrare nei dettagli degli obiettivi di controllo, delle management guidelines e delle altre componenti; esso definisce il quadro di riferimento al contempo pratico e concettuale al cui interno sono organizzate le pratiche per il governo ed il controllo dell'IT proposte dalla suite; come già ricordato, i contenuti di COBIT® sono prevalentemente organizzati secondo una struttura di processi di gestione dell'IT a due livelli, domini IT e processi IT;
- Gli Obiettivi di Controllo contengono le migliori pratiche per la definizione e gestione di un sistema di controllo interno sull'IT;
- Le Procedure di Controllo forniscono linee guida di dettaglio concernenti le modalità di implementazione per singoli obiettivi di controllo;
- L'IT Assurance Guide fornisce indirizzi generali sull'Information Systems Audit e funge da guida per l'Audit relativamente a tutti i processi IT contemplati da COBIT®;
- Gli Obiettivi di Controllo IT per Sarbanes Oxley forniscono una guida su come assicurare la conformità dell'ambiente IT ai requisiti SOXA basandosi sugli obiettivi di controllo COBIT®;
- L'IT Governance Implementation Guide fornisce una "road map" generale per realizzare un sistema di governo IT utilizzando le risorse COBIT® e l'insieme degli strumenti di supporto sopra elencati;

- COBIT® Quickstart™ fornisce indicazioni per il controllo sull'IT per aziende di minori dimensioni; per organizzazioni di maggiori dimensioni può essere utilizzato come indicazione dei primi passi verso la realizzazione di un sistema di controlli per l'IT;
- COBIT® Security Baseline™ descrive gli elementi essenziali che un'organizzazione deve considerare per adottare al proprio interno misure di Sicurezza delle informazioni.

La selezione dei contenuti fra gli strumenti proposti da COBIT® può comportare non tanto e non solo la scelta dello strumento più adatto agli obiettivi di uno specifico progetto, quanto piuttosto anche la selezione, all'interno di ogni pubblicazione, dei contenuti rilevanti, ad esempio in funzione delle caratteristiche dell'organizzazione oggetto di intervento.

Il ricorso all'outsourcing rappresenta un esempio tipico. Infatti, un'azienda che abbia conferito a terze parti in tutto o in parte lo sviluppo e la manutenzione dei sistemi informativi non applicherà i processi di controllo che COBIT® ha previsto per questa tematica; detta azienda si concentrerà invece sugli obiettivi di controllo relativi ai rapporti con le terze parti (DS 2 "*Manage third parties services*" e il dominio *Monitoraggio*).

3.3.1 Utilizzare le Management Guidelines

La suite COBIT® propone ai responsabili dell'IT e del business specifici strumenti di management definiti per ciascuno dei 34 processi; in particolare, le Management Guidelines definiscono per ciascun processo:

- Modello dei processi con Input e Output;
- Modelli organizzativi (RACI chart);
- IT Balanced Scorecard e Metriche;
- Maturity Model.

3.3.2 Input & Output e Modelli organizzativi (RACI chart)

Il modello dei processi di COBIT®, con l'indicazione dei documenti input ed output a ciascun processo, unitamente ai modelli organizzativi dei RACI chart, costituiscono uno strumento prezioso per la definizione di una organizzazione IT.

In particolare, il modello dei processi con i relativi input ed output, rappresentano per COBIT® un passo verso l'integrazione / integrabilità con i sistemi di qualità, che si basano proprio su una corretta definizione di opportuni flussi documentali.

La figura n.4 illustra, a titolo di esempio, il modello input/output per il processo PO5 – Manage the IT Investment.

I modelli organizzativi, RACI chart, identificano le principali attività previste dal processo, le relative responsabilità (nelle due accezioni di Responsible – chi fa – ed Accountable – chi risponde se qualcosa non funziona), e gli eventuali ruoli coinvolti con le modalità di Consultazione o Informazione. La figura n.5 illustra il diagramma RACI per lo stesso processo PO5; tale diagramma risponde alla tipica domanda organizzativa "Chi fa che cosa".

PO5 Manage the IT Investment

From	Inputs
PO1	Strategic plan and tactical IT plans, project and service portfolios
PO3	Infrastructure requirements
PO10	Updated IT project portfolio
AI1	Business requirements feasibility study
AI7	Post-implementation reviews
DS3	Performance and capacity plan (requirements)
DS6	IT financials
ME4	Expected business outcome of IT-enabled business investments

Outputs	To						
Cost/benefits reports	PO1	AI2	DS6	ME1	ME4		
IT budgets	DS6						
Updated IT service portfolio	DS1						
Updated IT project portfolio	PO10						

Figura 4 - Modello Input/Ouput di CobiT: esempio relativo al processo PO5 .

RACI Chart — **Functions**

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Maintain programme portfolio.	A	R	R	R	C					I	I
Maintain project portfolio.	I	C	A/R	A/R	C		C	C		C	I
Maintain service portfolio.	I	C	A/R	A/R	C	C				C	I
Establish and maintain IT budgeting process.	I	C	C	A		C	C	C	R	C	
Identify, communicate and monitor IT investment, cost and value to the business.	I	C	C	A/R		C	C	C	R	C	C

A **RACI** chart identifies who is Responsible, Accountable, Consulted and/or Informed.

Figura 5 - RACI chart di CobiT: esempio relativo al processo PO5 .

3.3.3 IT Balanced Scorecard e Metriche

Le metriche proposte da COBIT® possono essere utilizzate per implementare cruscotti di governo dell'IT basati sullo strumento delle IT Balanced Scorecard multilivello. COBIT® infatti individua i principali indicatori di Prestazione per il processo e di risultato per l'IT e per il Business relativi a ciascun processo ed a più livelli.

Una IT Balanced Scorecard multilivello combina infatti indicatori di performance e di risultato riferiti a più aree ed a più livelli dell'IT; in particolare, le aree trattate di norma includono: User Orientation, Business Contribution, Operation Excellence, Future Orientation, mentre i livelli inclusi generalmente comprendono: Activity/System, Process ed IT.

L'implementazione delle IT Balanced Scorecard richiede l'attivazione di sistemi strutturati per la raccolta di informazioni elementari ed il relativo reporting; COBIT® propone per ciascun processo specifici indicatori adattabili alle esigenze di ciascuna organizzazione.

La figura n.6 riporta per lo stesso processo “PO5 – Manage the IT Investment” gli indicatori proposti da COBIT® :

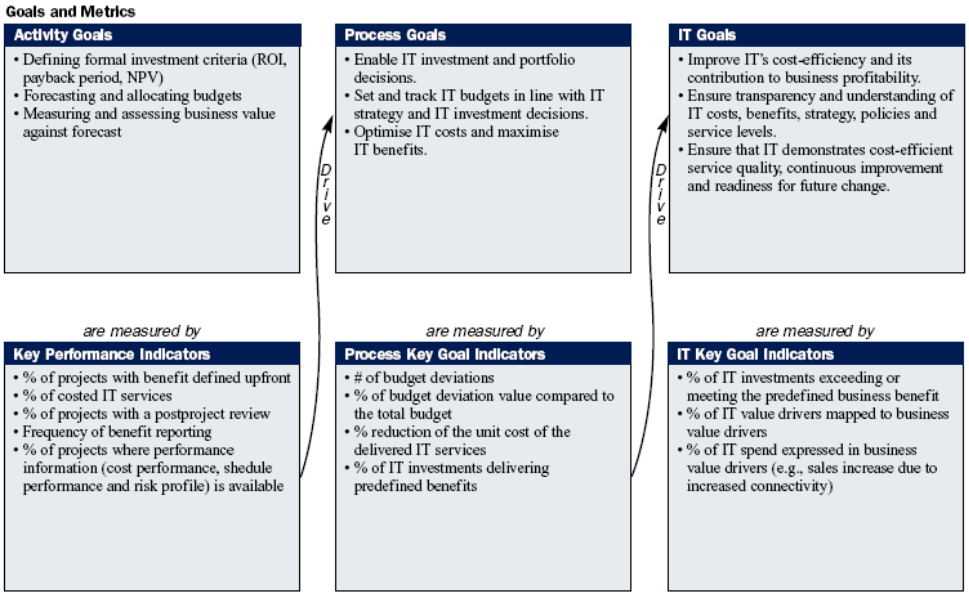

Figura 6 - Obiettivi, indicatorie metriche di COBIT: esempio relativo al processo PO5 .

3.3.4 Maturity Model

Il Modello di Maturità proposto da COBIT® per i processi di gestione dell’IT definisce i criteri per misurare il livello di strutturatezza dell’organizzazione nell’eseguire e controllare le attività di processo, su una scala da 0 – Non existent a 5 – Optimized, passando per 1 – Ad hoc, 2 – Repetable but Intuitive, 3 – Defined, 4 – Managed and Measurable.

I modelli di maturità sono strumenti ampiamente applicati per fare benchmark ed autovalutazione; la misurazione del livello di maturità si basa su questionari e tabelle di riferimento; nella misurazione del livello di maturità è importante non soffermarsi eccessivamente su questioni di precisione decimale della misurazione, quanto sulla sostanza degli aspetti che consentono, o meno, di concludere che si è raggiunto un prefissato livello di maturità.

La figura n.7 illustra in sintesi l’utilizzo del modello di maturità per la valutazione dello stato attuale e la definizione degli obiettivi da raggiungere.

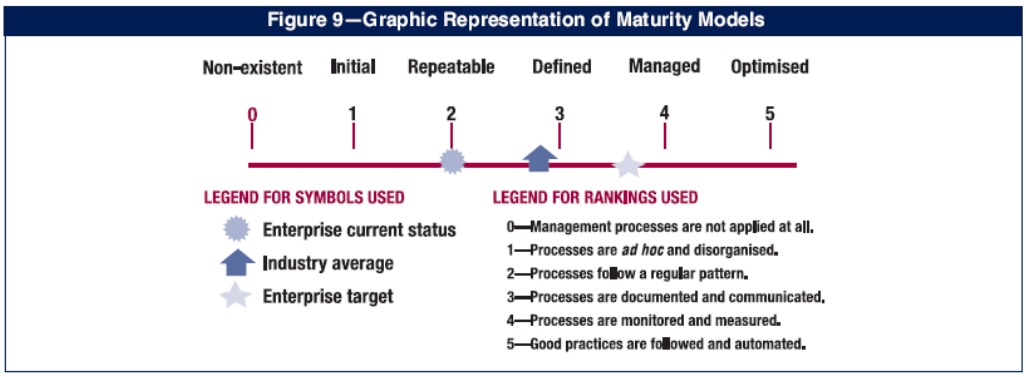

Figura 7 – Rappresentazione grafica del modello di maturità di COBIT

Vale la pena ricordare che il livello di maturità di un processo può essere interpretato anche come il livello di strutturazione del sistema di controllo e delle pratiche di gestione del processo stesso.

Oltre agli strumenti specifici per ciascun processo, l'esperienza e le ricerche maturate nell'ambito della comunità degli utilizzatori di COBIT®, ha permesso di arricchire la suite con specifici esempi o supporti per l'applicazione degli strumenti della suite.

Fra questi di particolare interesse sono ad esempio le applicazioni delle IT Balanced Scorecard multilivello nell'ambito delle quali vengono messi in relazione gli indicatori di performance e risultato concernenti l'IT con gli indicatori di performance e risultato concernenti il business.

A tale applicazione è dedicata l'Appendice I di COBIT® 4, che mette in relazione un elenco di tipici obiettivi con un elenco di tipici obiettivi di una organizzazione IT, e questi ultimi con uno o più processi che contribuiscono al conseguimento di tali obiettivi.

Ad esempio, l'obiettivo di Business "*Espansione delle quote di mercato*" è collegato, fra l'altro, a due obiettivi IT:

- **Obiettivo IT:** (25) Consegnare i progetti secondo i piani ed il budget, ottemperando agli standard qualitativi;
- **Obiettivo IT:** (28) Assicurare che l'IT dimostri: a) un servizio di qualità attraverso un uso efficiente delle risorse, b) miglioramento continuo, c) disponibilità e prontezza ai mutamenti futuri.

A loro volta, gli obiettivi IT sono messi in relazione agli obiettivi di controllo che maggiormente contribuiscono al conseguimento di tali obiettivi, come indicato nelle seguenti due tabelle:

Obiettivo IT: (25) Consegnare i progetti secondo i piani ed il budget, ottemperando agli standard qualitativi.	
Processi IT / Obiettivi di Controllo	**PO 8 Gestione della Qualità**: **PO 10 Gestione dei Progetti**:

Obiettivo IT: (28) Assicurare che l'IT dimostri: a) un servizio di qualità attraverso un uso efficiente delle risorse, b) miglioramento continuo, c) disponibilità e prontezza ai mutamenti futuri.	
Processi IT	PO 05 Gestione degli investimenti IT DS 06 Identificare e attribuire i costi ME 1 Monitoraggio e valutazione delle prestazioni IT ME 3 Assicurare la conformità ai requisiti cogenti

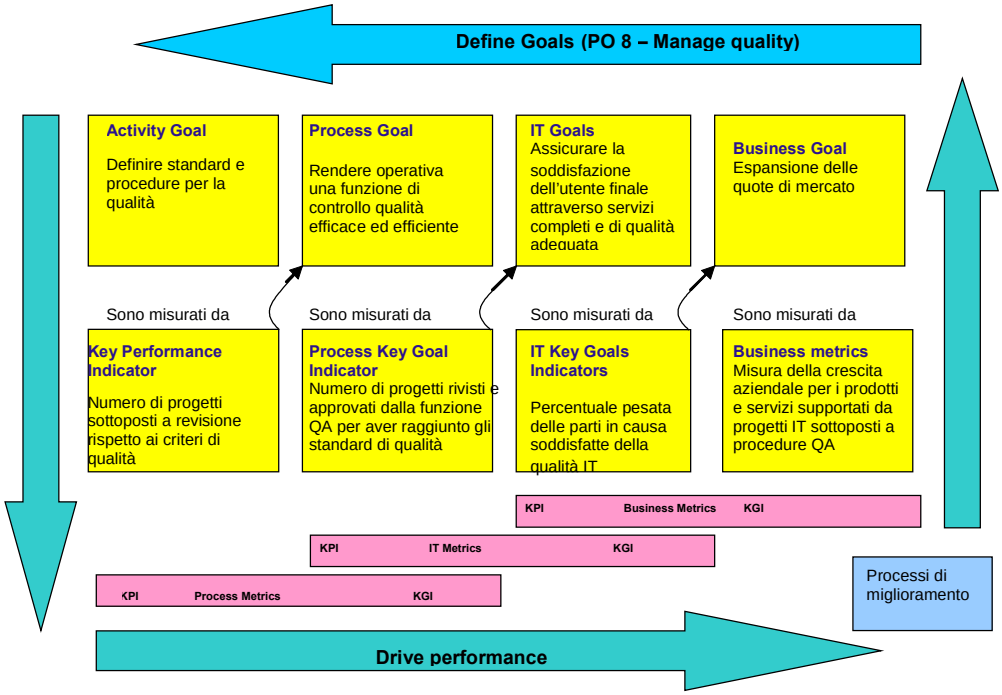

Figura 8 - Relazioni tra le attività IT, gli obiettivi IT e gli obiettivi di business

L'applicazione del modello consiste nell'individuare all'interno dei processi IT gli obiettivi di prestazione e risultato IT rilevanti, collegati ad opportuni indicatori di prestazione e risultato ai livelli processo ed attività.

Individuati tali collegamenti, il modello potrà essere implementato definendo sugli indicatori rilevanti opportuni cicli di miglioramento continuo nell'ambito dei quali il miglioramento sia misurabile sulla base delle variazioni nel valore degli indicatori oggetto di osservazione.

A titolo illustrativo, e rifacendosi all'esempio precedente, per il processo PO 8, a fronte dell'obiettivo IT di "Assicurare la soddisfazione dell'utente finale attraverso servizi completi e di qualità adeguata", collegato all'obiettivo di business "Espansione delle quote di mercato", gli obiettivi di processo e di attività proposti da COBIT® includono rispettivamente "Rendere operativa una funzione di controllo qualità efficace ed efficiente" e "Definire standard e procedure per la qualità", unitamente agli opportuni indicatori.

Sulla base di tali indicatori, potrà essere misurato il contributo dell'IT al conseguimento degli obiettivi di business, sulla base dello schema[7] presentato nella figura n.8.

3.4 Utilizzare i Control Objectives

Di norma più diretta è l'applicazione di COBIT® per le attività di progettazione e valutazione delle strutture organizzative e dei processi per lo sviluppo ed erogazione dei servizi IT. I Processi COBIT® rappresentano una traccia per progettisti e sviluppatori, utile per prevenire soprattutto per disegnare processi nell'ambito dei quali siano opportunamente presidiati sia i rischi tipici delle organizzazioni IT, sia i rischi di inefficacia/inefficienza organizzativa.

A titolo di esempio, COBIT® include specifici requisiti anche per le attività di gestione IT di servizi ottenuti da terze parti – applicabile in particolare da realtà che hanno esternalizzato in parte o in tutto la gestione dei sistemi informativi. Per tale situazione, ormai molto comune, COBIT® propone uno specifico processo: DS 2 "Manage Third-Party Services".

Il processo prevede una serie di Obiettivi di controllo dettagliati (da DS 2.1 a DS 2.4) e la catena delle attività converge verso gli obiettivi di business come indicato in figura n.9.

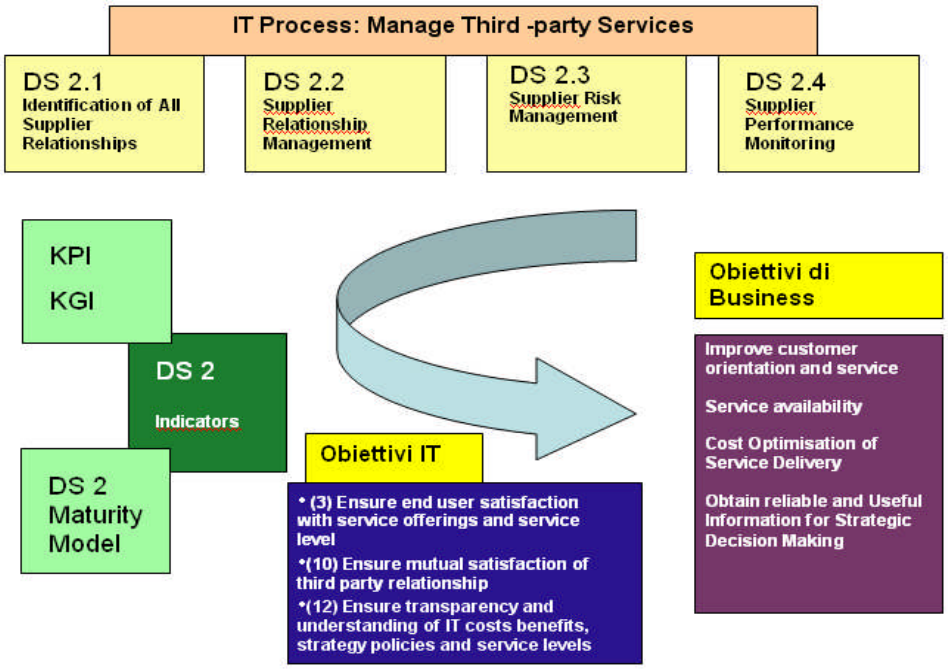

Figura 9 - Dagli obiettivi di controllo agli obiettivi di business in COBIT.

3.5 Utilizzare le IT Assurance Guidelines

COBIT® supporta in modo efficace le attività di revisione dei Sistemi Informativi: ottenuto l'incarico di svolgere una verifica in un determinato ambito aziendale, l'Auditor verificherà quali processi IT sono presenti e svolgerà le sue analisi. L'obiettivo sarà di

[7]. Per ragioni di chiarezza la figura rappresenta una situazione semplificata indicando per ogni livello solo un indicatore misurabile per tematica – la matrice completa è riportata nella Pubblicazione "COBIT 4.0" a pag.61.

formulare un giudizio in merito al grado di presidio dei rischi presenti nell'ambito esaminato.

COBIT® non propone né obiettivi di controllo né procedure di revisione per specifiche tecnologie.

3.6 Punti di forza di COBIT

Caratteristica immediatamente percepibile di COBIT® è il linguaggio semplice: è stato evitato di sviluppare un gergo specialistico, facendo invece ricorso a termini comuni, propri anche di altre metodologie.

La semplicità del linguaggio e l'esclusione di terminologia tecnica consente di stabilire una relazione importante tra IT e i "*non addetti*" dimostrando viceversa che proprio il vertice aziendale deve svolgere un ruolo di protagonista. Tramite COBIT® il vertice aziendale può finalmente ottenere visibilità sugli elementi chiave che testimoniano l'andamento dell'IT, la sua sincronia con il Business e la sua funzione di produttore di valore.

COBIT® si pone come guida efficace offrendo spunti fruibili in quasi ogni realtà nelle seguenti aree:

- Allineamento dell'IT agli obiettivi aziendali: raccordo tra le strategie e sistema di controllo sull'allineamento nel tempo tra IT e Business. (PO 1)
- Processi di comunicazione interna: attribuzione di ruoli e responsabilità (PO 4) e definizione di politiche, procedure interne (PO 6)
- Risk Assessment: COBIT® tratta in modo analitico l'attività forse più importante dopo l'ottenimento degli obiettivi di business, attraverso due processi specifici, il primo a livello di Direzione aziendale (PO 9), il secondo a livello di attuazione (DS 5).
- Monitoraggio: i 25 obiettivi di dettaglio contenuti nei processi da M1 a M4 rappresentano un insieme di elementi che si pongono come guida per una sistema di controllo dell'IT su più livelli (Controlli Interni e Audit indipendente interno e/o esterno). Considerate le difficoltà quotidiane nel controllo dell'IT, sempre alla rincorsa di obiettivi da realizzare in tempi sempre più stretti, i processi proposti da COBIT® rappresentano un riferimento molto utile.

3.7 Relazioni con altre best practice

COBIT® rimanda il "come fare" all'organizzazione dell'azienda. Tuttavia il richiamo all'adozione di standard e procedure formalizzate è costante.

COBIT® **raccomanda di non "*reinventare la ruota*" e di ricorrere alle "migliori pratiche" e / o standard riconosciuti comuni per il tipo di azienda in questione. Il sistema di indicatori di obiettivo e prestazione e "Maturity Models" è leva per questo risultato.**

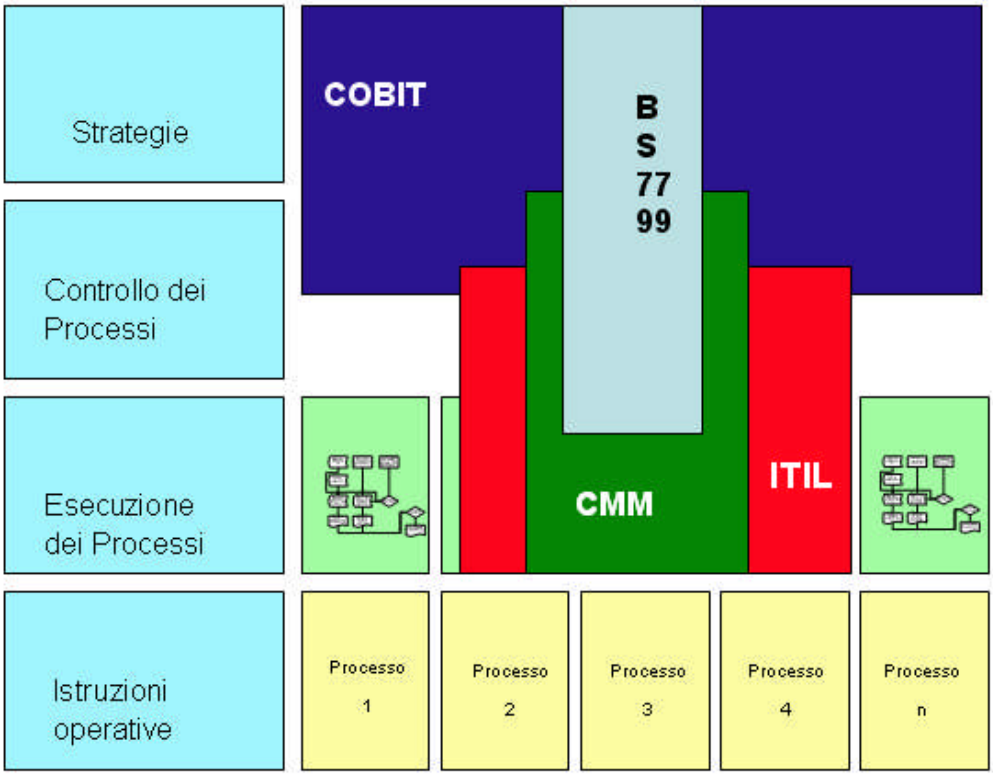

Figura 10 - Posizionamento delle diverse best practice secondo E. Guldentops

La semplicità del linguaggio aiuta anche chi si avvicina a COBIT® provenendo da ISO 17799, BS 7799, (ISO 2700x), ITIL®, COSO o altro: lo sforzo di rimappatura delle proprie conoscenze è assai ridotto.

La figura n.10 sintetizza in modo schematizzato e non quantitativo, la "copertura" di alcune best practice nei confronti dell'insieme delle attività IT. È evidente come COBIT® eviti di addentrarsi verso le aree operative: trattandosi di un modello destinato prevalentemente al management ed al controllo, COBIT® non contiene indicazioni sul "come fare" ad utilizzare la tecnologia per sfruttarla al meglio o istruzioni operative per la realizzazione di processi produttivi specifici.

4 ITIL - IT Infrastructure Library

di Annamaria Iannelli

L'attuale quadro economico richiede alle Aziende flessibilità, efficacia ed efficienza. In tale contesto è fondamentale che il dipartimento IT sia consapevole dell'importanza del proprio ruolo aziendale, conosca e condivida gli obiettivi di business e, in funzione di essi, definisca l'idonea strategia di evoluzione e gestione dell' IT. Ogni scelta effettuata, per il successo della stessa, dovrà tener presente che la qualità del servizio erogato è legato, secondo Information Technology Infrastructure Library (di seguito ITIL®), a quattro elementi fondamentali e tra loro interconnessi: Persone, Processi, Prodotti e Partner.

4.1 Origini e cenni di storia

ITIL® è stato sviluppato a partire dal 1989 nell'ambito del CCTA (Organismo tecnico del Governo inglese oggi confluito nell'OGC - Organisation for Government Commerce) come un insieme di best practice, finalizzato alla gestione ottimale dei servizi IT, ad uso e consumo della Pubblica Amministrazione Britannica.

Successivamente si è diffuso, con un ritmo sempre più rapido, in tutto il mondo e ben presto si è affermato quale standard de facto per la gestione dei servizi informatici. Le discipline di Service Support e Service Delivery che lo compongono si propongono di fornire le indicazioni necessarie affinché Persone, Processi, Prodotti e Partner assicurino il rispetto degli impegni assunti sul livello di servizio e quindi concorrano al raggiungimento degli obiettivi di business dell'Impresa.

4.2 Chi lo utilizza e perché

L'attuale quadro economico richiede ad ogni Società di rispondere tempestivamente alle richieste provenienti dal mercato e in quest'ambito il dipartimento IT viene chiamato ad assumere la responsabilità di assicurare immediatezza e sicurezza di accesso alle idonee informazioni nei tempi e nelle modalità richieste. Il dipartimento IT dunque non solo sostiene il business dell'Impresa, ma assume un ruolo di primaria importanza nella definizione e realizzazione dei processi aziendali in risposta alle sollecitazioni non solo del mercato, ma anche degli stakeholder in generale.

La tecnologia ad oggi disponibile è in grado di supportare egregiamente l'IT nel suo compito, ma non è però sufficiente ad assicurare il rispetto degli impegni assunti e soprattutto di garantire un costo adeguato rispetto al livello di servizio offerto (e/o richiesto).

Per il successo di ogni Impresa è indispensabile che il dipartimento IT sia consapevole dell'importanza del proprio ruolo aziendale, conosca e condivida gli obiettivi di business ed in funzione di essi, parallelamente:

- implementi l'idonea evoluzione tecnologica
- aggiorni i Processi coinvolti,
- modifichi ruoli e responsabilità delle Persone
- adegui il rapporto con i Partner.

Di conseguenza il dipartimento IT, o meglio il suo management, ancor prima del rinnovamento tecnologico, è tenuto ad affrontare temi di business ed organizzazione.

Il CIO è quotidianamente interpellato, a fianco dei manager degli altri dipartimenti di business, per affrontare e risolvere i seguenti problemi:

- allineamento tra obiettivi IT ed obiettivi di business aziendali
- acquisizione di vantaggi competitivi
- individuazione, razionalizzazione ed analisi dei livelli di servizio richiesti dall'utenza interna ed esterna
- analisi del livello di servizio offerto
- individuazione dell'eventuale gap in essere
- identificazione delle idonee azioni correttive e/o evolutive in termini organizzativi, procedurali, formativi e tecnologici
- sensibilizzazione, relativamente ad ogni progetto di revisione/innovazione, delle idonee strutture aziendali
- definizione del nuovo livello di servizio offerto
- disponibilità, nel rispetto dei tempi e dei costi stabiliti, di tutti gli strumenti necessari al supporto del business
- reattività e qualità di servizio rispondenti alle esigenze di mercato
- individuazione dell'idonea strategia di gestione dell'ICT: full outsourcing, outsourcing selettivo, insourcing
- definizione dell'idonea strategia di gestione dei partner
- identificazione degli opportuni Key Performances Indicator
- individuazione ed implementazione delle opportune metriche
- costante controllo del livello del servizio offerto
- implementazione della necessaria reportistica e sua diffusione ai vari livelli aziendale
- disponibilità delle idonee competenze e loro costante aggiornamento
- riduzione e controllo dei costi
- identificare potenziali rischi/criticità e definire la strategia di gestione
- identificare e incrementare il ritorno degli investimenti effettuati
- incrementare la produttività individuale

Per affrontare con successo i temi sopra citati le strutture aziendali devono condividere gli obiettivi di business, operare in partnership ed adottare un approccio strutturato ed organico basato su linee guida consolidate. A tale proposito è indispensabile che le strutture condividano lo stesso linguaggio e siano supportate da metodologie tali da consentire la definizione e l'implementazione di processi finalizzati al rispetto degli impegni assunti.

Inoltre ogni organizzazione delegata all'erogazione di servizi verso utenze interne e/o esterne deve assicurare il rilascio di servizi di “qualità”, tali da rispettare costantemente i requisiti e le aspettative dell'utenza.

In tale contesto il dipartimento IT è il primo ad essere coinvolto; ma proprio il dipartimento IT che si occupa, per missione aziendale, dell'ottimizzazione e dell'automatizzazione dei processi tipici di altre strutture aziendali è spesso il primo a trovarsi in difficoltà. Esso non dispone generalmente di processi interni formalizzati e, in molti casi, i processi informali esistenti non rispondono alle reali esigenze aziendali. E' dunque fondamentale che il dipartimento IT si ponga come obiettivo primario l'analisi dei processi interni in essere, ne verifichi il loro allineamento con le esigenze di business e provveda alla loro revisione, standardizzazione e formalizzazione.

Per raggiungere tali obiettivi un numero sempre crescente di Aziende si riferisce ad ITIL®, una raccolta di direttive e “best practice“ focalizzate sull'IT Service Management.

ITIL® costituisce, ad oggi, un “framework” di riferimento, finalizzato al miglioramento dei servizi informatici, dove vengono analizzati e descritti i Servizi fondamentali come “Processi” in cui si integrano le attività componenti, fornendo così norme di riferimento adattabili alle situazioni operative di ogni azienda..

La scalabilità e la flessibilità di ITIL® consentono la sua applicabilità ad organizzazioni di varie dimensioni e quindi favoriscono la sua diffusione.

L'introduzione e l'implementazione di tali direttive e “best practice” hanno portato all'interno di molte organizzazioni IT una serie di benefici, quali:

- flessibilità e reattività rispondenti alle esigenze di business
- razionalizzazione dei servizi offerti all'utenza interna/esterna
- razionalizzazione e formalizzazione del livello di servizio richiesto
- costante rispetto degli impegni di servizio assunti
- “ingegnerizzazione” di ogni attività periodica
- definizione chiara e formalizzata di compiti e responsabilità
- gestione efficace ed efficiente di ogni eventuale criticità
- riduzione della complessità e dei rischi operativi
- razionalizzazione, controllo e contenimento dei rischi operativi
- ottimizzazione del Return On Investement (ROI)
- team work e sinergie tra dipartimento IT ed altre strutture aziendali

4.3 Descrizione del framework

ITIL® si focalizza sul tema dell'IT Service Management e fornisce una serie di direttive e “best practice” finalizzate al miglioramento dell'efficacia e dell'efficienza del dipartimento IT e alla qualità del servizio da esso erogato.Tali direttive e best practice sono organizzate in sette moduli o chapter di seguito rappresentati e sintetizzati.

Figura 1 – Il Framework ITIL

I moduli di Service Support e Service Delivery sono il cuore della struttura. Le best practice in essi descritte forniscono le indicazioni necessarie affinchè Persone, Processi, Prodotti e Partner assicurino il rispetto degli impegni assunti sul livello di servizio e quindi concorrano al raggiungimento degli obiettivi di business dell'Impresa. Il

dipartimento IT, recependo ed applicando tali direttive, può operare in sinergia con tutte le strutture aziendali, condividendone le esigenze e fornendo il necessario supporto allo sviluppo del business.

Il modulo Service Support descrive i processi finalizzati a "supportare l'erogazione" dei servizi IT a sostegno degli obiettivi business. L'adeguatezza di tali processi costituisce un elemento fondamentale e la loro attuazione richiede il commitment manageriale. Esso include i processi di Incident Management, Problem Management, Change Management, Release Management, Configuration Management e la funzione di Service Desk che si integra con tutti gli altri processi.

Il modulo Service Delivery riguarda gli aspetti di fornitura del servizio e comprende sia processi richiesti per la pianificazione e l'erogazione di servizi IT sia i processi finalizzati al miglioramento della qualità dei servizi IT erogati, attraverso l'implementazione dei processi di Service Level Management, Financial Management, Capacity Management, IT Service Continuity e Availability Management.

4.3.1 Service Support

Abbiamo detto che il Service Desk è una funzione, a differenza delle altre tematiche di ITIL®, che sono definite come processi. Ebbene per ITIL® il **Service Desk,** è l'elemento chiave della gestione dei servizi IT, poichè costituisce l'unico punto di contatto tra i fornitori del servizio e gli utenti.

Rientra nelle sue responsabilità il controllo degli incidenti in base a quanto stabilito nel processo di Incident Management. La conoscenza degli incidenti pone il Service Desk nella condizione ideale per fornire informazioni relative alla gestione, in particolare in termini di percezione dell'erogazione del servizio da parte degli utenti. ITIL® raccomanda una stretta correlazione tra il Service Desk ed i processi di Incident Management, Problem Management e Change Mangement, raccomanda inoltre che le registrazioni degli incidenti siano conservate nello stesso database CMDB (Configuration Management Database) contenente i problemi, gli errori noti e le registrazioni degli estremi dei cambiamenti.

La prossima figura ci permette di visualizzare quale flusso segue l'incident individuato e/o segnalato, a partire dal Service Desk nell'ambito del processi definiti nel modulo di Service Support

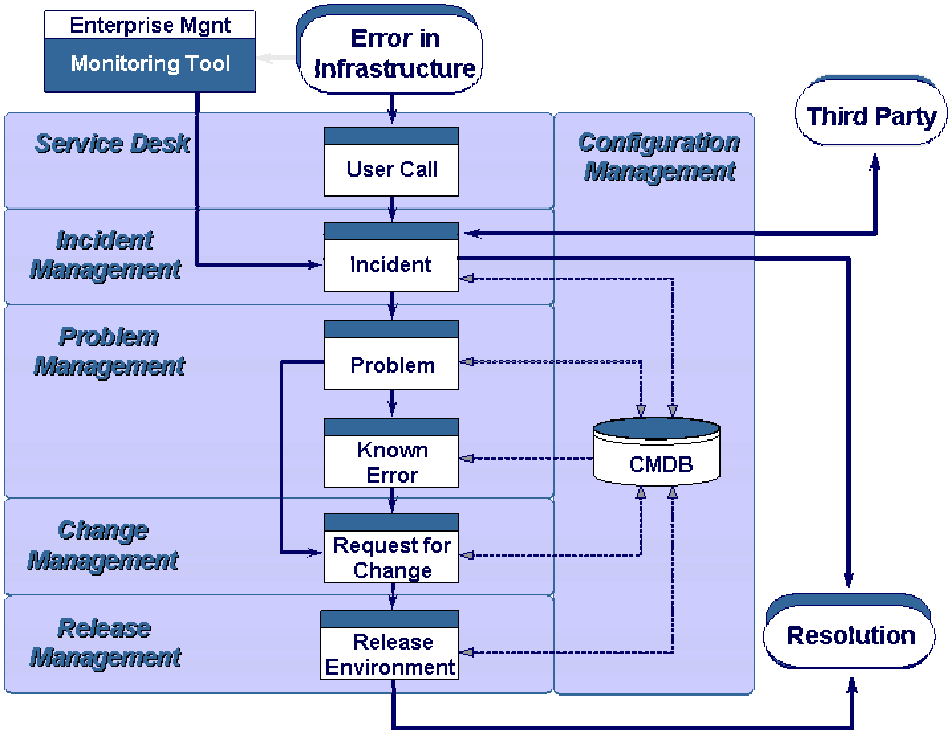

Figura 2 – Incident, il flusso seguito.

Vediamo ora più in dettaglio i singoli processi:

Incident Management, è responsabile di ripristinare le normali condizioni operative nel più breve tempo possibile e di ridurre al minimo l'impatto sulle attività business, assicurando il mantenimento dei migliori livelli possibili di disponibilità e di qualità del servizio. Nella terminologia ITIL®, un 'incidente' è definito come:

“qualsiasi evento che non fa parte del normale esercizio del servizio e che causa o può causare un'interruzione, o una riduzione di qualità, del servizio stesso,”

dove per “normale esercizio del servizio” si intende l'erogazione del servizio entro i limiti previsti dal Service Level Agreement.

Le attività di Incident Management si possono così sintetizzate:

- Rilevazione e registrazione degli incidenti
- Classificazione e supporto iniziale
- Investigazione e diagnosi
- Risoluzione e ripristino
- Chiusura dell'incidente
- Responsabilità, monitoraggio, tracciamento e comunicazione degli incidenti
- Registrazione degli incidenti e aggiornamento del CMDB

Sono fattori critici di successo per l'Incident Management:

- Risoluzione rapida degli incidenti
- Mantenimento della qualità dei servizi IT
- Miglioramento della produttività a livello IT e business
- Mantenimento della soddisfazione degli utenti

Problem Management, è responsabile di ridurre al minimo l'impatto sul business provocato da incidenti e problemi legati ad errori nell'infrastruttura IT e di prevenire il riverificarsi di incidenti legati a tali errori. Per raggiungere questo obiettivo, il Problem Management cerca di determinare la causa originaria degli incidenti e quindi di avviare azioni per migliorare o correggere la situazione. Il processo di Problem Management contiene aspetti sia reattivi che proattivi. Gli aspetti reattivi sono legati alla soluzione dei problemi in risposta a uno o più incidenti mentre quelli proattivi si occupano di identificare e risolvere i problemi e gli errori noti prima che gli incidenti si verifichino.

Nella terminologia ITIL® un "errore noto" è una condizione identificata dalla diagnosi della causa originaria di un problema e dal successivo sviluppo di un workaround.

Le attività di Problem Management possono essere così riepilogate:

- Gestione proattiva
- Identificazione e risoluzione di Problemi e Errori noti prima del verificarsi degli Incidenti (Analisi del trend)
- Analisi dei problemi
- Identificazione, classificazione e registrazione dei problemi

Sono fattori critici di successo per il Problem Management:

- Miglioramento della qualità del servizio
- Riduzione dell'impatto dei problemi
- Riduzione del costo derivante dai problemi

Change Management, assicura l'utilizzo di metodi e procedure standard finalizzati alla gestione efficace ed efficiente di tutti i cambiamenti, alla riduzione di ogni eventuale impatto sulla qualità del servizio e al miglioramento della normale operatività. Al fine di consentire, in seguito ad eventuali cambiamenti, una transizione rapida e semplice è fondamentale che il processo di Change Management abbia un'ampia visibilità e disponga di efficaci canali di comunicazione.

Le attività di Change Management si possono così sintetizzate:

- Richiesta di cambiamento RFC (Request For Change)
- Classificazione e autorizzazione del cambiamento
- Gestione dei cambiamenti
- Test, rilascio,analisi e chiusura del cambiamento

Sono fattori critici di successo per il Change Management:

- Ripetibilità dei processi di realizzazione dei cambiamenti
- Rapidità e correttezza nei cambiamenti
- Protezione dei servizi durante i cambiamenti
- Efficienza e efficacia del processo.

Configuration Management, è responsabile dell'identificazione, della registrazione all'interno del Configuration Management Database (CMDB) e del reporting di tutti gli elementi costituenti l'asset IT. Ogni elemento sarà rappresentato, all'interno del CMDB, da un Configuration Item (CI) contenente tutte le informazioni di sua pertinenza in termini di versioni, eventuali dettagli logistici o gestionali e relazioni con altri elementi dell'asset. Il processo di Configuration Management deve quindi fornire informazioni accurate sulle configurazioni e verificare l'attendibilità dei Configuration Item al fine di fornire un CMDB affidabile e consolidato per i processi di Incident Management, Problem Management e Release Management.

Le attività di Configuration Management si possono così sintetizzate:

- Definizione e gestione Configuration Management DB
- Analisi dell'impatto dei cambiamenti
- Creazione nuovi Configuration Item

Sono fattori critici di successo per il Configuration Management:

- Gestione degli asset IT
- Supporto per l'erogazione di servizi IT di qualità
- Fornitura di servizi nel rispetto dei costi e profittevole
- Supporto, integrazione e interfaccia con i processi IT Service Management

Release Management, comprende il controllo e la distribuzione del software ed è quindi strettamente connesso con il Configuration Management. Il suo obiettivo consiste nel "proteggere", a fronte dell'introduzione di nuove release hw/sw, l'ambiente di produzione ed i servizi da esso erogati. Si occupa pertanto di tutto quanto attiene ed è necessario predisporre per il rilascio e la distribuzione delle release (HW, SW, persone ecc.).

Le attività di Release Management si possono così sintetizzate:

- Verifica e/o predisposizione dei necessari prerequisiti
- Mantenimento di una consolidata Software Library

Sono fattori critici di successo per il Release Management:

- Qualità di software e hardware
- Ripetibilità dei processi di rollout di release del sw e del hw
- Rapidità e correttezza di implementazione delle release
- Economicità dell'operazione di creazione/gestione delle release

4.3.2 Service Delivery

Vediamo ora i processi di questo modulo che ha nella definizione dei Service Level Agreement la parte sicuramente più significativa anche per gli impatti immediati in ambito Service Support.

Service Level Management, rappresenta la base dei processi di Service Support e Service Delivery. I suoi obiettivi consistono nell'assicurare il rispetto dei Service Level Agreements e degli Operational Level Agreements e la mitigazione di eventuali impatti sulla qualità dei servizi. Esso comprende il processo di pianificazione, coordinamento, negoziazione, monitoraggio e reporting degli SLA. Include inoltre la revisione continua dei risultati del servizio per accertare che la qualità richiesta venga mantenuta e, ove necessario, migliorata.

Le attività del Service Level Management possono essere così sintetizzate:

- Produzione e gestione catalogo di servizi
- Negoziazione e definizione Service Level Requirement
- Individuazione, formulazione e gestione Service Level Agreement e Operational Level Agreement
- Individuazione idonee azioni manutentive/migliorative

Sono fattori critici di successo per il Service Level Management

- Quantità e qualità dei servizi IT richiesti
- Fornitura dei servizi concordati
- Fornitura di servizi a costi rispondenti alle esigenze aziendali
- Gestione dell'interfaccia tra business e utenti

Financial Management for IT Services, è responsabile della contabilità dei costi IT, del ritorno degli investimenti (ROI) e di tutti gli aspetti che concernono l'addebito all'utenza dei servizi IT. Al fine di identificare il costo reale dei servizi opera in stretta collaborazione con il Capacity Management, il Configuration Management ed il Service Level Management. Esso collabora inoltre con le strutture di business e con l'organizzazione IT per la negoziazione del budget e dei servizi.

Le attività del Financial Management for IT Services possono essere così sintetizzate:

- Comprensione ed allocazione costi
- Definizione Budget

Sono fattori critici di successo per il Financial Management for IT Services:

- Amministrazione efficace delle finanze IT
- Efficacia globale del processo
- Soddisfazione dei clienti in relazione a costi e addebiti dei servizi

Capacity Management, ha la responsabilità di assicurare la disponibilità delle capacità IT adeguate alle esigenze del business. Ogni Capacity Plan rilasciato è strettamente legato alle strategie ed ai piani di business. E' inoltre coinvolto nella risoluzione degli incidenti e nell'identificazione dei problemi.
Le attività del Capacity Management possono essere così sintetizzate:

- Gestione della richiesta
- Memorizzazione dei dati sulle capacità
- Modellazione e dimensionamento delle applicazioni
- Produzione del Capacity Plan

Sono fattori critici di successo per il Capacity Management:

- Conoscenza esigenze di business
- Conoscenza tecnologie attuali e future
- Dimostrazione dell'opportunità dell'investimento
- Pianificazione e disponibilità delle risorse appropriate

IT Service Continuity, ha la responsabilità di assicurare, in caso di indisponibilità parziale o totale di una risorsa,, un livello predeterminato e concordato di servizio a supporto dei requisiti minimi del business.

Le attività dell'IT Service Continuity possono essere così sintetizzate:

- Analisi dell'impatto sul business
- Valutazione dei rischi
- Strategia di continuità del business
- Riduzione dei rischi di minacce e delle vulnerabilità
- Piano di realizzazione e organizzazione

Sono fattori critici di successo per l'IT Service Continuity:

- Erogazione e ripristino dei servizi IT coerentemente agli obiettivi business
- Sensibilizzazione dell'intera organizzazione relativamente ai piani di continuità

Availability Management, si occupa della progettazione, dell'implementazione, della misurazione e della gestione dei servizi IT al fine di assicurare il costante rispetto dei livelli di disponibilità richiesti dalle esigenze di business. Richiede una comprensione delle ragioni per cui si verificano i guasti IT e del tempo necessario per ripristinare il servizio e, a tale proposito, interagisce con l'Incident Management ed il Problem Management.

Le attività di Availability Management possono essere così sintetizzate:

- Definizione degli obiettivi di disponibilità, affidabilità e manutenibilità
- Definizione e gestione del piano di disponibilità
- Misurazione e reporting in funzione del business
- Monitoraggio e analisi dei trend

Sono fattori critici di successo per l' Availability Management:

- Gestione della disponibilità e affidabilità dei servizi IT
- Soddisfazione delle esigenze business
- Disponibilità, a un costo ottimale, dell'infrastruttura IT

Altri temi sono trattati, in modo però meno completo rispetto a quelli di Service Support e Service Delivery, all'interno del framework. I restanti cinque moduli sono di seguito sintetizzati.

ICT Infrastructure Management: comprende tutti gli aspetti della gestione dell'infrastruttura ICT (Information & Tecnology Infrastructure) , dall'identificazione delle esigenze di business alla definizione dell'idoneo adeguamento infrastrutturale ed alla sua realizzazione, amministrazione e supporto.

Planning to Implement Service Management: esamina i problemi e le attività relative alla pianificazione, implementazione e miglioramento dei processi di Service Management all'interno di una organizzazione. Esso indirizza inoltre anche i problemi associati con i cambiamenti culturali ed organizzativi, lo sviluppo di una strategia ed il più appropriato metodo di approccio.

Application Management: descrive come gestire le applicazioni partendo dalle necessità di business, attraverso tutte le fasi del ciclo di vita fino alla loro “fine vita”. Pone enfasi sull'assicurare che progetti e strategie IT siano costantemente allineate con le esigenze di business in ogni momento del ciclo di vita dell'applicazione.

The Business Perspective: si rivolge al personale IT e fornisce consigli finalizzati a facilitare la comprensione e la condivisione degli obiettivi di business, a migliorare il contributo offerto dall'IT nel contesto aziendale mediante l'allineamento di ruoli e servizi.

Security Management: dettaglia, relativamente all'ambiente IT, il processo di pianificazione e gestione di un predefinito livello di sicurezza. Include la valutazione e la gestione dei rischi e delle vulnerabilità e l'implementazione delle contromisure nel rispetto del contenimento dei costi.

4.4 Come si applica

In molti contesti aziendali si riscontra che le reali necessità dell'utenza, cioè i Service Level Requirement, non sono mai stati chiaramente identificati e di conseguenza non sono stati definiti e formalizzati i relativi Service Level Agreement.

In tali realtà la struttura IT effettua sovente attività, sia preventive che reattive, la cui esecuzione avviene senza alcuna responsabilità e procedura definita. L'IT, in questo contesto, deve concentrare i suoi sforzi nella risoluzione o gestione delle criticità. Il dispendio di risorse, sia umane che economiche, è notevole ed i risultati in termini di

soddisfazione dell'utenza e quindi di business sono modesti e non proporzionali all'impegno prestato.

Nell'attuale contesto economico situazioni analoghe a quelle sopra citate pregiudicano il successo dell'impresa stessa e richiedono l'individuazione e la tempestiva implementazione dell'idonea strategia evolutiva.

Per definire ed implementare il percorso ottimale è indispensabile disporre delle necessarie competenze ed avvalersi di modelli/metodologie. Questi ultimi devono essere in grado di offrire le linee guida necessarie per l'identificazione delle esigenze aziendali, la definizione dei relativi Service Level Requirement e dei corrispondenti Service Level Agreement, l'identificazione delle capacità attuali e di quelle invece richieste, l'individuazione e la pianificazione delle idonee attività.

ITIL® costituisce un modello di riferimento, ad oggi standard de facto, a cui ispirarsi al fine di fornire servizi rispondenti alle effettive richieste dell'utenza nel rispetto degli obiettivi di costi e business prefissati dall' azienda.

Esso non impone regole, ma propone best practice a cui riferirsi al fine di soddisfare le necessità della propria utenza.

L'azienda e la sua organizzazione non devono quindi modificarsi in funzione del modello, ma devono cogliere da quest'ultimo quanto serve per razionalizzare, ottimizzare, formalizzare i processi già esistenti ed introdurre quanto necessario anche se mai formalmente implementato ed ingegnerizzato, ma solo effettuato occasionalmente o a fronte di criticità.

L'introduzione di ITIL® esige una serie di prerequisiti/modalità ed un rigoroso approccio progettuale.

Prerequisiti e modalità

- **Commitment del management** – Costituisce un presupposto dal quale non si può prescindere. L'introduzione di ITIL® coinvolge l'intera azienda in quanto ogni struttura è, direttamente o indirettamente, responsabile del successo dell'iniziativa.
  Alcune strutture aziendali sono infatti coinvolte in qualità di utenti finali e quindi in base alle loro esigenze sono definiti i Service Level Requirement. Altre strutture sono responsabili della formalizzazione dei corrispondenti Service Level Agreement ed altre ancora sono responsabili della definizione di processi tali da assicurare il costante rispetto dei Service Level Agreement definiti. Infine l'attuazione e il rispetto delle procedure e delle responsabilità definite è affidata ad altri settori dell'azienda.
- **Informazione, sensibilizzazione e formazione** – L'introduzione di ITIL® comporta un cambiamento culturale.

  Ogni settore aziendale, coerentemente con le proprie attività e responsabilità, deve essere correttamente informato e sensibilizzato relativamente al progetto in corso ed agli obiettivi che l'azienda, con esso, si è prefissata. Inoltre occorre ricordare che non si possono trarre benefici da ciò che non si conosce dunque, in funzione del livello e del tipo di coinvolgimento, ogni settore aziendale dovrà poter disporre dell'idonea formazione.

  I processi nuovi e/o aggiornati dovranno diventare, dopo la loro implementazione o revisione, operativi. Le varie strutture aziendali, coerentemente con il loro coinvolgimento e la loro responsabilità, dovranno regolamentare le loro attività quotidiane secondo i nuovi processi e dovranno essere in grado di trarre da essi il massimo vantaggio. E' quindi indispensabile

che ogni struttura sia consapevole dei potenziali benefici, condivida il cambiamento in atto e collabori fattivamente per il suo successo.

- **Consapevolezza della situazione attuale –** Non si può certo identificare l'idoneo obiettivo e definire il giusto cammino senza conoscere le reali esigenze dell'utenza, le capacità e le potenzialità della struttura in essere. Occorre dunque conoscere e razionalizzare le richieste dell'utenza, identificare tutti i servizi attualmente offerti, verificare la loro rispondenza a quanto richiesto e l'adeguatezza dei processi a loro supporto, identificare ogni eventuale vincolo e rischio, individuare i fattori critici di successo e definire le opportune metriche. Tutto questo richiede un'analisi approfondita dell'ambiente in essere e delle necessità aziendali a medio e lungo termine ed occorre inoltre tener presente che la qualità dei dati di tale analisi influenzerà pesantemente il risultato del progetto ITIL®.
- **Definizione dell'area di azione** – Come si è detto l'introduzione di ITIL® coinvolge, anche se a livelli diversi, la maggior parte dei settori aziendali. Affrontare un progetto ITIL® in tutta la sua globalità è estremamente rischioso. L'esperienza, ad oggi acquisita, conferma che l'assenza di risultati nel breve tempo porta a demotivazione, dispersione di energie, perdita di entusiasmo e sfiducia nel perseguire gli obiettivi. È dunque fortemente consigliato individuare una prima area di azione (un particolare processo o servizio) chiaramente delimitata e scelta in funzione delle priorità e dell'attenzione aziendale. Questo consentirà di ottenere il maggior risultato con il minor sforzo e sarà così possibile usufruire dei benefici di ITIL®, per l'area prescelta, nel breve termine. Il risultato ottenuto permetterà inoltre di consolidare le competenze, acquisire confidenza per il conseguimento dei successivi obietti e ottenere credibilità aziendale.

In conclusione, da un lato, l'introduzione di ITIL® passa per un coinvolgimento dell'intera azienda, quantomeno per la definizione dei Service Level Agreement, ma dall'altro lato il Service Desk è l'elemento chiave nell'applicazione di ITIL® per l'erogazione e gestione dei servizi IT.

La prossima figura ci permette di vedere schematicamente tutti gli elementi e le relazioni fondamentali che permettono una corretta applicazione delle best practice ITIL®

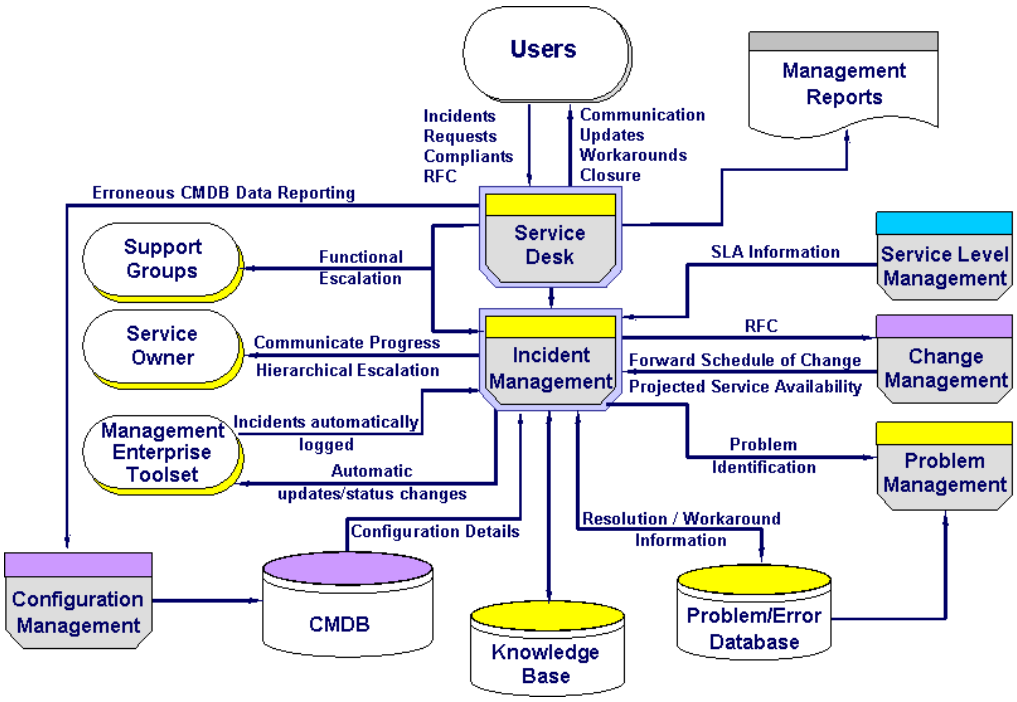

Figura 3 – Elementi e relazioni fondamentali.

I benefici apportati dall'introduzione e applicazione delle best practice ITIL® sono testimoniati dalle ormai innumerevoli realtà aziendali che si sono ispirate a tale modello e che hanno conseguito risultati positivi sia quantitativi (riduzione degli incidenti e dei problemi, minori tempi di attesa per le soluzioni, ..) che qualitativi (miglior percezione degli utenti, miglior organizzazione delle attività all'interno del dipartimento IT).

L'approccio

Il costante rispetto dei prerequisiti sopra citati ed il raggiungimento degli obiettivi prefissati sarà assicurato da un approccio progettuale in grado di guidare l'azienda dalla fase preliminare di comprensione delle tematiche di IT Service Management, a quella successiva di introduzione delle direttive ITIL® fino a quella finale di implementazione e attuazione dei processi ottimali per la specifica realtà.

La fase preliminare di progetto dovrà quindi rivolgersi a tutti i manager e responsabili di processo che, per posizione e ruolo, contribuiscono al raggiungimento degli obiettivi aziendali al fine di:

- consentire la comprensione e razionalizzazione delle specifiche esigenze
- trattare i temi principali dell'IT Service Management riferendosi alla specifica realtà
- fornire un primo livello informativo su ITIL®
- individuare i vantaggi più evidenti per i vari contesti aziendali
- individuare ed analizzare il catalogo dei servizi offerti
- identificare i processi in essere ed il loro livello di maturità
- definire le aree prioritarie, le eventuali interrelazioni e le responsabilità
- concordare il possibile percorso evolutivo con le prime ipotesi in termini di tempi ed aree di coinvolgimento

Tale attività di informazione, presa di conoscenza e sensibilizzazione dovrà essere ripetuta, con i necessari approfondimenti all'interno del progetto di implementazione ITIL®, coerentemente con le esigenze aziendali. In funzione dell'avanzamento del progetto essa dovrà anche fornire e documentare i risultati ottenuti al fine di verificare costantemente l'adeguatezza e la correttezza di quanto effettuato.

Le successive fasi, denominate "assessment" si focalizzeranno, secondo le priorità precedentemente concordate, su aree ben definite e saranno finalizzate a determinare la capacità d

ella realtà in essere. Si dovrà cioè identificare l'eventuale GAP esistente tra quanto in essere e quanto effettivamente richiesto dalle esigenze aziendali.

A tal fine verranno esaminati tutti gli elementi fondamentali - Persone, Processi, Prodotti e Partner - che condizionano il livello di servizio offerto. In base a quanto rilevato verrà identificato il gap esistente tra capacità attuali e quelle effettivamente necessarie e verranno individuate tutte le azioni correttive ed implementative corredate delle opportune metriche. Generalmente tale fase prevede un report finale nel quale sono dettagliate tutte le necessarie competenze, le idonee componenti tecnologiche, le attività richieste, la pianificazione di quest'ultime e le relative responsabilità.

I risultati della fase di assessment richiederanno, per la corretta prosecuzione del progetto, l'approvazione e la condivisione dei responsabili designati da tutte le strutture

coinvolte, il commitment del management e la formalizzazione di quest'ultimo a procedere.

Questa fase, particolarmente delicata, richiede spesso un nuovo ciclo di informazione e sensibilizzazione.

Ottenuto il consenso aziendale si potrà quindi proseguire nella implementazione effettiva di quanto definito nella precedente fase di assessment. Tale fase comporta la revisione/introduzione di Processi, l'adeguamento di ruoli e responsabilità delle Persone, l'evoluzione delle modalità di gestione dei Partner, l'adeguamento tecnologico dei Prodotti a supporto dei Processi.

Tale fase realizzativa dovrà prevedere parallelamente ad ogni rilascio il relativo allineamento operativo. Sarà infatti indispensabile verificare che ogni modifica all'esistente e/o ogni “novità” introdotta sia correttamente recepita ed utilizzata secondo modalità tali da consentire i massimi benefici. Ogni risultato ottenuto dovrà essere documentato e trasmesso alle varie strutture con l'idoneo dettaglio.

E' inoltre indispensabile ricordare che un “progetto ITIL®” è dotato, come ogni soluzione tecnologica, di un suo ciclo di vita. In altri termini la conclusione della fase di implementazione coincide con l'inizio della fase di gestione finalizzata alla verifica dell'idoneo utilizzo di quanto rilasciato e all'individuazione di ogni nuova esigenza.

Senza una corretta ed attenta gestione, al sorgere di un cambiamento organizzativo o di una nuova richiesta quanto implementato diventerebbe inadeguato e, nel breve termine, i servizi rilasciati dal dipartimento IT non sarebbero più in grado di sostenere gli obiettivi di business.

5 Confronto COBIT - ITIL

di Andrea Pederiva, Maxime Sottini

5.1 Introduzione

Dopo aver introdotto entrambi i framework, COBIT® nel capitolo 3 e ITIL® nel capitolo 4, questo capitolo ha come obiettivo quello di metterli a confronto. Il confronto verrà portato a livello complessivo degli approcci, senza entrare in dettaglio nelle singole parti del modello (ovvero, ad esempio, nei singoli processi).

Per un confronto ad un maggior livello di dettaglio, si rimanda ai capitoli 6 e 7, ove alcuni processi specifici, trattati in entrambi i modelli, sono esaminati e confrontati nel dettaglio, al fine di riscontrare differenze e analogie.

Una delle analisi più significative effettuate in letteratura è senza dubbio quella descritta nel white paper "Aligning COBIT®, ITIL® and ISO 17799 for Business Benefit" pubblicato congiuntamente dai medesimi organismi che hanno creato COBIT® e ITIL®, ovvero ITGI e OGC.

Tale documento non vuole essere propriamente un "confronto" ma piuttosto una guida per l'allineamento e l'utilizzo congiunto dei due framework. Questo perché COBIT® e ITIL® non sono approcci concorrenti ma complementari, in grado di completarsi l'un l'altro.

Il white paper offre quindi preziosi "puntatori", ovvero collegamenti tra i processi (e la documentazione), da un framework verso l'altro, in entrambe le direzioni. Nel seguito, tali puntatori verranno spesso utilizzati e citati.

Un esempio del contenuto del documento è riportato in figura 1 per quanto concerne la lettura da COBIT® verso ITIL® ed in figura 2, per la lettura in senso inverso.

COBIT Domain: Plan and Organise PO3 Determine Technological Direction			
Determining technological direction satisfies the business requirement of taking advantage of available and emerging technology to drive and make possible the business strategy. It is enabled by the creation and maintenance of a technological infrastructure plan that sets and manages clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms.			
COBIT Control Objective	**Key Areas**	**ITIL Supporting Information**	**ISO 17799 Supporting Information**
PO3.1 Technological infrastructure planning	Technological infrastructure plan, systems architecture, technological direction, migration strategies	*Applications Management*, The Application Management Lifecycle, 5.5 Deploy *ICT Infrastructure Management*, Design and Planning, 2.5 The processes and deliverables of strategic planning	3.1 Information security policy 4.1 Information security infrastructure 8.5 Network management
PO3.2 Monitor future trends and regulations	Technological infrastructure plan maintenance	*ICT Infrastructure Management*, Technical Support, 5.4 The technical support processes	4.1 Information security infrastructure
PO3.3 Technological infrastructure contingency	Systematic assessment, redundancy, resilience and evolutionary capability	***Service Delivery*, Capacity Management, 6.3 Activities in capacity management** ***Service Delivery*, Availability Management, 8.5 Availability planning** *ICT Infrastructure Management*, 3 Deployment	5.2 Information classification 11.1 Aspects of business continuity management

Figura 1. Collegamenti da COBIT verso ITIL. Tratto da "Aligning COBIT, ITIL and ISO 17799 for Business Benefit".

Si osservi che nella definizione dei collegamenti da COBIT® verso ITIL® in figura 1 sono riportati in grassetto gli argomenti ove le organizzazioni, ITGI e OGC, ritengono che ITIL® possa offrire un supporto più avanzato. E' vera l'osservazione opposta, ovvero un contributo più contenuto di ITIL® nelle aree non riportate in grassetto.

Mapping ITIL to COBIT			
ITIL Process	COBIT Process	COBIT Detailed Control Objective	
3. ICT Infrastructure Management *cont.*			
Establish ICT standards and policies	PO3	PO3.5	Technology standards
Maintain ICT architectural blueprints	PO3	PO3.1	Technological infrastructure planning
Design and implement technical migration plans	PO3	PO3.1	Technological infrastructure planning
Review programme against strategy and business plans	PO4	PO4.1	IT planning or steering committee
Develop and ratify ICT solutions	AI	AII	Acquire and implement
Build appropriate working environments	AI5	AI5.12	Promotion to production
Test ICT solutions	AI5	AI5.6	Testing strategies and plans
Define appropriate roll-out strategy	AI5	AI5.3	Implementation plan
Roll-out ICT solutions	AI5	AI5.12	Promotion to production

Figura 2. Contenuto del white paper "Aligning COBIT, ITIL and ISO 17799 for Business Benefit". Collegamenti da ITIL verso COBIT.

Il white paper si riferisce alla versione 3 di COBIT® ed alla versione 2 di ITIL®.

Il risultato dello studio, condiviso dagli autori, è che mentre COBIT® è uno strumento di Governance che fornisce supporto per stabilire **che cosa fare** (in termini di obiettivi e processi da attivare) in ambito IT e **come controllare il raggiungimento degli obiettivi**, ITIL® fornisce le **indicazioni e gli strumenti per implementare i requisiti espressi** da COBIT®.

5.2 Destinatari

Destinatario di COBIT® è principalmente il Management delle Organizzazioni, che include ovviamente quello della funzione IT.

Nella pratica i fruitori concreti della metodologia sono i Direttori IT, che la possono applicare ai fini della Governance e dell'Organizzazione della funzione, e gli auditor, interni e/o esterni, che la utilizzano per la loro attività nell'ambito della gestione dell'IT.

La Sarbanes-Oxley è stata uno dei driver più rilevanti per l'adozione del framework, e tra i principali destinatari compaiono ovviamente anche gli attori coinvolti in essa per quanto concerne l'IT. Di COBIT® si occupano generalmente anche tutte le società ed i consulenti che offrono servizi di impostazione della governance e/o di auditing.

Rispetto a COBIT®, il target di destinatari di ITIL® è più ampio. Tutti coloro che si occupano di COBIT® infatti sono interessati al framework ITIL®, la cui adozione assicura un'implementazione consistente, efficace ed efficiente dei processi.

In aggiunta però, destinatari di ITIL® sono le funzioni IT che quotidianamente contribuiscono ad erogare i processi IT descritti nel framework, come pure le società fornitrici che erogano servizi IT e numerosi attori fornitori di strumenti a supporto dell'esecuzione dei processi IT.

L'adozione massiva e world-wide di ITIL®, a livello di aziende di dimensioni medio/grandi, testimonia l'interesse per il modello da parte di tutti coloro che si occupano di servizi di gestione delle infrastrutture IT (il mondo applicativo risulta, sino ad ora, meno interessato).

5.3 Obiettivi

Cominciamo quindi il confronto dagli obiettivi dei due approcci.

COBIT® ha l'obiettivo primario di fornire un framework ed il supporto per la Governance dell'IT, ove quest'ultima è parte della Governance più generale dell'azienda. L'obbiettivo della Governance IT, a sua volta, è quello dell'allineamento, controllato e misurato, della gestione dell'IT ai fini del raggiungimento degli obiettivi di business.

ITIL® è un approccio, o best practice, finalizzato ad offrire indicazioni e supporto operativi per l'erogazione di Servizi IT di qualità, allineati con le necessità del business. Nonostante la diversità di fondo degli obiettivi, è però possibile riscontrare che entrambi gli approcci riconoscono:

- l'importanza del contributo dell'IT per il business;
- la necessità di allineare l'IT con il business;
- l'importanza di un corretto bilanciamento tra livelli di servizio e costi di erogazione.

5.4 Ampiezza

Non è semplice confrontare l'ampiezza della copertura dei due approcci in termini di ambito dei processi di gestione IT.

Partendo dal concetto che COBIT®, essendo uno strumento di Governance, dovrebbe coprire totalmente tale ambito, il citato white paper OGC/ ITIL® evidenzia, esaminando i puntatori o collegamenti segnalati, una buona corrispondenza tra i due modelli e, conseguentemente, una buona copertura teorica anche da parte di ITIL®.

In particolare, nell'area Planning & Optimise, i soli processi su cui non vi è alcuna copertura ITIL® sono:

PO7 - Manage IT Human Resources
PO8 - Manage Quality

Nelle aree Acquire and Implement e Deliver and Support non risultano scoperture di ITIL®, mentre nell'area Monitor and Evaluate risultano scoperti (con riferimento a COBIT® 3) i processi:

M2 - Assess Internal Control Adequacy
M3 - Obtain Independent Assurance
M4 - Provide for Independent Audit

5.5 Struttura e contenuti

Su questo punto, COBIT® e ITIL® evidenziano molte diversità. Entrambi i modelli sono infatti orientati ai processi, tuttavia COBIT® li organizza con una logica più tradizionale, ispirata al ciclo di vita dei sistemi (plan, build, run, monitor), mentre ITIL® non offre una visione altrettanto intuitiva e non fornisce uno schema sintetico di lettura complessiva se non in alcune aree (Service Support e Service Delivery).

Passando ai contenuti, COBIT® è un modello estremamente regolare e omogeneo.

Per ciascun processo riporta infatti sempre la medesima struttura e contenuti (con riferimento a COBIT® versione 4):

- High Level Objectives, dettagliati come in figura 3;
- Detailed Control Objectives;
- Management Guidelines (inputs/outputs, RACI chart, Goals and Metrics, Maturity Model).

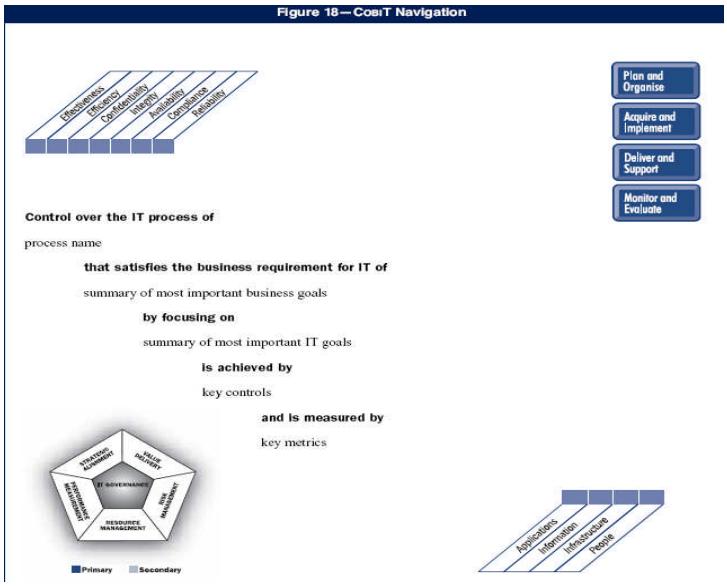

FIgura 3. Struttura degli High Level Objectives di un processo in COBIT versione 4.

ITIL® non è così omogeneo. Tra le diverse pubblicazioni che costituiscono il modello, si riconosce il tentativo di impostare una struttura simile per quanto concerne i processi, tentativo riuscito solo parzialmente e comunque soprattutto nelle due pubblicazioni (Service Support e Service Delivery) che, come avremo modo di vedere, sono le pubblicazioni "core" ed utilizzate più estesamente.

La struttura ricercata per ogni processo è la seguente:

- Obiettivi
- Ambito
- Benefici
- Pianificazione e implementazione
- Attività
- Ruoli
- KPIs
- Strumentazione
- Appendici

Tuttavia, come si è già evidenziato, alcuni processi non riportano tutte le sezioni oppure, in alcune parti, possono avere una strutturazione diversa da quella riportata.

Se si osservano, oltre al contenuto vero e proprio degli approcci, anche gli aspetti complementari, si scopre che COBIT® offre importanti contenuti quali una guida all'implementazione e delle linee guida per l'audit e per l'implementazione dei controlli.

In ITIL® versione 2, tali pubblicazioni non sono presenti nel core anche se è possibile riscontrare numerosi lavori di parti esterne ad OGC volte a colmare tale carenza.

5.6 Utilizzo

Entrambe le metodologie raccomandano e richiedono di essere contestualizzate e, quindi, un approccio all'utilizzo adattato agli obiettivi e al dominio di applicazione.

Tuttavia, mentre COBIT® può essere utilizzato con pari efficacia in tutte le aree di processo, ITIL® è prevalentemente utilizzato nelle aree di Service Support e Service Delivery.

L'utilizzo di COBIT® è strutturato con un approccio top-down, ovvero partendo dagli obiettivi di business si determinano quelli per l'IT, e da essi gli obiettivi di controllo significativi da implementare e controllare. ITIL® è invece utilizzato con diverse modalità.

In generale, è scelto come modello a tendere per l'erogazione dei Servizi, in particolare in quelle organizzazioni in cui il Servizio IT è un elemento importante oppure è esso stesso il core business. In molti casi, tuttavia, si riscontrano utilizzi focalizzati di specifici processi del framework, es. Incident Management, spesso in risposta ad esigenze o criticità specifiche.

Per queste ragioni, COBIT® è sempre richiesto o imposto dalla Direzione, molto spesso dal Management del Business o, comunque da quello IT, ed ha in generale un ampio ambito di utilizzo, ad esempio in termini di assessment dei processi. ITIL® invece, può anche essere supportato e promosso da specifiche aree del management IT, oltre che dalla sua Direzione, in particolare dal management che si occupa delle infrastrutture, anche con finalità "tattiche".

5.7 Aree di complementarietà

Ci addentriamo ora nel cuore di questo Capitolo per analizzare le aree in cui COBIT® e ITIL® risultano essere effettivamente complementari, anticipando che tale ambito non coincide con quello complessivo dei framework.

Se infatti è vero che le due metodologie si sovrappongono con poche differenze per copertura dei processi di gestione IT - come il white paper di ITGI e OGC mette in evidenzia e come precedentemente sottolineato, se si entra nel merito dei contenuti la situazione cambia considerevolmente, come si mostrerà nel seguito.

Ciò avviene perché mentre COBIT® fornisce, ai fini della Governance e dell'audit, il medesimo supporto per tutti i processi, ITIL® non fornisce indicazioni operative su come implementare con il medesimo livello di dettaglio tutti i processi.

E' quindi molto importante comprendere in quali aree, o ambiti di processo, ITIL® è un buon complemento a COBIT® ed in quali aree questo non avviene. Per tale scopo, si è partiti ancora una volta dal white paper ITGI/OGC.

Infatti, in tale documento è espressa una valutazione dettagliata (per COBIT® 3) delle aree in cui ITIL® è in grado di supportare significativamente l'implementazione degli obiettivi di controllo.

Il problema principale del documento è che l'analisi è effettuata ad un elevato livello di dettaglio che non consente una sintesi e comprensione immediata del quadro complessivo. Tale sintesi è l'obbiettivo che ci prefiggiamo di raggiungere nel seguito di questo paragrafo.

Per costruire la sintesi è stato adottato l'approccio nel seguito descritto. Per tutti gli High Level Control Objectives sono stati eseguiti i seguenti passi:

- evidenziate in una matrice le aree in cui le pubblicazioni di ITIL® forniscono supporto (per pubblicazione);
- contati i Detailed Control Objectives per cui ITIL® non fornisce alcun supporto (valutazione ITGI/OGC);
- contati i Control Objectives per cui ITIL® fornisce un buon livello di supporto (valutazione OGC/ ITIL®);
- calcolato il livello di supporto degli High Level Objectives complessiva da parte di ITIL®, espresso come percentuale (1 – numero di Detailed Control Objectives non coperti/numero di Detailed Control Objectives);
- calcolato il livello di supporto degli High Level Objectives con buon supporto da parte di ITIL® (numero di Detailed Control Objectives con supporto significativo dichiarato da OGC/ ITIL® / numero di Detailed Control Objectives) in percentuale.

L'analisi è stata effettuata per tutte le aree e gli High Level Control Objectives del modello ITIL®.

Nel seguito, quattro tabelle sintetizzano i risultati costruiti con il seguente metodo:

- % totale di copertura del High Level Control Objective compresa tra 0 e 33%, valutazione bassa (colore rosso);
- % totale di copertura del High Level Control Objective compresa tra 34% e 66%, valutazione media (colore giallo);
- % totale di copertura del High Level Control Objective compresa tra 67% e 100%, valutazione alta (colore verde);
- % di copertura con buon supporto del High Level Control Objective compresa tra 0 e 33%, valutazione bassa (colore rosso);
- % di copertura con buon supporto del High Level Control Objective compresa tra 34% e 66%, valutazione media (colore giallo);
- % di copertura con buon livello di supporto del High Level Control Objectives compresa tra 67% e 100%, valutazione alta (colore verde);

Ai fini della valutazione complessiva del supporto ITIL® ad un area di processo, High Level Control Objective, si è tenuto conto sia della copertura totale dei Detailed Control Objectives corrispondenti (in tabella colonna "% cop. CO") che di quella con buon livello di supporto (in tabella colonna "% cop. CO-OK").

Combinando entrambe, si ottiene:

- buon supporto di ITIL® se **copertura totale alta** e **livello di supporto alto**,
- medio supporto di ITIL® se **copertura totale media** e **livello di supporto medio**, oppure se **copertura totale alta** e **livello di supporto medio o basso**, oppure se **copertura totale medio o bassa** e **livello di supporto alto**.

I risultati sono sintetizzati nelle 4 tabelle sottostanti, una per ciascuna area dei processi COBIT®.

PLAN AND ORGANIZE	Planning to Implement Service Management	The Business Perspective	ICT Infrastructure Management	Application Management	Service Support	Service Delivery	Security Management	Software Asset Management	# GAPs	# CO	% cop. CO	% cop. CO-OK
PO1 - Define a strategic IT plan									0	8	100%	0%
PO2 - Define the information architecture									2	4	50%	0%
PO3 - Determine Technology Direction						1		1	0	5	100%	40%
PO4 - Define the IT Processes, Organisation and Relationships	1		1					1	4	15	73%	20%
PO5 - Manage IT Investment						3			0	3	100%	100%
PO6 - Communicate Management Aims and Direction									6	11	45%	0%
PO7 - Manage IT Human Resources									8	8	0%	0%
PO8 - Manage Quality									6	6	0%	0%
PO9 - Assess and Manage IT risks									2	8	75%	0%
PO10 - Manage Projects									15	19	21%	0%

Tabella 1 – Sintesi livello di supporto di ITIL v2 a COBIT v3 per l'area PLAN & ORGANIZE

Dalla tabella 1, si evince che ITIL® non supporta adeguatamente l'area di processi PLAN & ORGANIZE, fatta eccezione per **PO5 – Manage IT Investement**, ove in particolare il processo ITIL® di IT Financial Management fornisce indicazioni adeguate.

Qualche forma di supporto, anche se migliorabile, si può trovare per:

PO1 - Define a strategic IT plan
PO3 - Determine Technology Direction
PO4 - Define the IT Processes, Organisation and Relationships
PO9 - Assess and Manage IT risks

AQUIRE AND IMPLEMENT	Planning to Implement Service Management	The Business Perspective	ICT Infrastructure Management	Application Management	Service Support	Service Delivery	Security Management	Software Asset Management	#
AI1 - Identify Automated Solutions			2						
AI2 - Acquire and maintain application software						1			
AI3 - Acquire and maintain technology infrastructure			1						
AI4 - Enable Operation and Use	1	1							
AI5 - Procure IT resources					2				
AI6 - Manage Changes					7				

Tabella 2 – Sintesi livello di supporto di ITIL v2 a COBIT v3 per l'area ACQUIRE & IMPLEMENT

Dalla tabella 2, si evince che ITIL® non supporta adeguatamente l'area di processi ACQUIRE & IMPLEMENT, fatta eccezione per **AI6 – Manage Changes**, ove in particolare il processo ITIL® di **Change Management** fornisce indicazioni adeguate.

Qualche forma di supporto, anche se non adeguato, si può trovare per:

AI2 - Acquire and maintain application software
AI3 - Acquire and maintain technology infrastructure

DELIVER AND SUPPORT	Planning to Implement Service Management	The Business Perspective	ICT Infrastructure Management	Application Management	Service Support	Service Delivery	Security Management	Software Asset Management	# GAPs	# CO	% cop. CO	% cop. CO-OK
DS1 - Define and manage Service Levels						7			0	7	100%	100%
DS2 - Manage third parties services						1			1	8	88%	13%
DS3 - Manage Performance and Capacity					1	7			1	9	89%	89%
DS4 - Ensure continuous service		1				9			2	13	85%	77%
DS5 - Ensure System security									0	21	100%	0%
DS6 - Identify and allocate costs						3			0	3	100%	100%
DS7 - Educate and train users									1	3	67%	0%
DS8 - Manage Service Desk and Incidents					4				1	5	80%	80%
DS9 - Manage the Configuration					7	1			0	8	100%	100%
DS10 - Manage Problems					3				2	5	60%	60%
DS11 - Manage Data									24	30	20%	0%
DS12 - Manage the physical environment									5	6	17%	0%
DS13 - Manage Operations			5						3	8	63%	63%

Tabella 3 - Sintesi livello di supporto di ITIL v2 a COBIT v3 per l'area DELIVER & SUPPORT

Dalla tabella 3, si evince che ITIL® supporta adeguatamente in molti casi i processi dell'area DELIVER & SUPPORT; in particolare si possono stabilire le seguenti relazioni:

DS1 - Define and manage Service Levels	**Service Level Management**
DS3 - Manage Performance and Capacity	**Capacity Management**
DS4 - Ensure continuous service	**IT Continuity Management**
DS6 - Identify and allocate costs	**IT Financial Managemnet**
DS8 - Manage Service Desk and Incidents	**Incident Management**
DS9 - Manage the Configuration	**Configuration Management**

In altri casi il supporto è minore, ma comunque significativo:

DS5 - Ensure System security
DS7 - Educate and train users
DS10 - Manage Problems
DS13 - Manage Operations

MONITOR AND EVALUATE	Planning to Implement Service Management	The Business Perspective	ICT Infrastructure Management	Application Management	Service Support	Service Delivery	Security Management	Software Asset Management	# GAPs	# CO	% cop. CO	% cop. CO-OK
M1 Monitor the Process					1				0	4	100%	25%
M2 - Assess Internal Control Adequacy									4	4	0%	0%
M3 - Obtain Independent Assurance									8	8	0%	0%
M4 - Provide for Independent Audit									8	8	0%	0%

Tabella 4 - Sintesi livello di supporto di ITIL v2 a CobiT v3 per l'area MONITOR & EVALUATE

Infine, Dalla tabella 4, si evince che ITIL® non supporta adeguatamente l'area di processi MONITOR & EVALUATE; qualche indicazione è fornita in relazione a **M1 – Monitor the Process**.

Queste indicazioni numericamente espresse e sintetizzate in figura 4, sono apparse agli autori un ritratto sufficientemente fedele alla realtà ed in linea con le esperienze maturate sul campo.

Unica eccezione potrebbe essere il processo ITIL® di **Problem Management** che, seppur valutato con un livello di supporto medio con il metodo utilizzato, parrebbe agli autori dover essere posizionato ad un livello di supporto elevato, nei confronti dell'obbiettivo di controllo **DS10 – Manage the problems** di COBIT®.

Per questo motivo, tale obiettivo è riportato in giallo in figura 4.

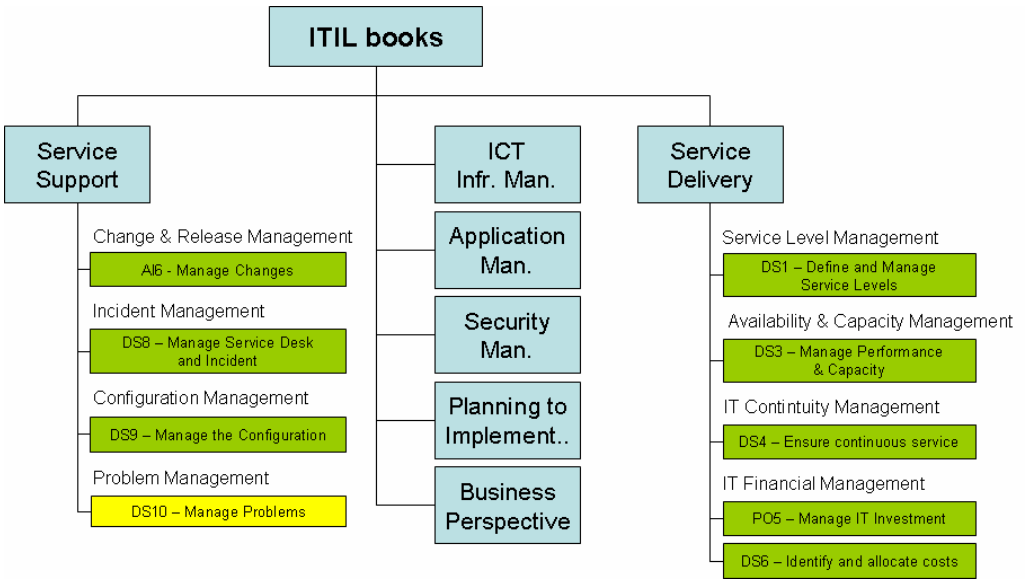

Figura 4 - Sintesi delle aree di supporto effettivo di ITIL v2 agli obiettivi di controllo CobiT v3

5.8 Conclusioni

COBIT® e ITIL® sono due modelli complementari che lavorano bene insieme: combinati forniscono governance (dove intervenire e che obiettivi porre), processi, linee guida di implementazione, soluzioni, strumenti di audit per l'IT. Non in tutte le aree, però.

ITIL® è utilizzato prevalentemente nell'ambito dei processi di Service Support e Service Delivery. Forse per questo si dimostra un buon compagno di COBIT® in particolare per queste aree di processi.

Una volta affrontato in questo capitolo il tema del confronto a livello complessivo tra COBIT® e ITIL® i Capitoli 6 e 7 si porranno l'obiettivo di approfondire e verificare in dettaglio, per alcune aree ad elevata complementarietà, le sinergie ottenibili dall'utilizzo congiunto dei due modelli.

6 Caso di applicazione congiunta: Configuration Management

di Federico Corradi, Orillo Narduzzo,

6.1 Introduzione

Anche in questo caso l'argomento è trattato strutturando il capitolo in due parti. La prima ha come obiettivo quello di tracciare un confronto dettagliato tra i due framework in relazione al processo. Questa analisi completa ed integra quella operata ad un livello più alto nel Capitolo 5.

La seconda parte consiste in un confronto sintetico sulla complementarietà dei due framework nel caso del Configuration Management.

Il caso di applicazione congiunta dei framework viene riportato in coda alla descrizione di questo processo, identificando i contributi specifici di COBIT® e ITIL®.

6.2 Prima parte: confronto Configuration Management

6.2.1 Il processo di Configuration Management: confronto tra i due framework

Nel seguito il processo di Configuration Management è esaminato ponendo a confronto i framework COBIT® e ITIL® con riferimento a diverse prospettive di analisi, in particolare:

- definizione e posizionamento del processo nei framework;
- contenuto e struttura del processo;
- obiettivi del e metriche del processo;
- supporto all'implementazione del processo;
- supporto all'implementazione dei controlli del processo e alla misura della strutturazione del processo
- organizzazione e ruoli previsti a supporto del processo.

6.2.2 Definizione e posizionamento del processo nei framework

In COBIT® il Configuration Management è trattato principalmente nel processo "DS 9 – Manage the Configuration" collocato nel dominio "Deliver and Support".

Ogni processo di COBIT® è sinteticamente descritto all'inizio dell'esposizione specifica, riportando le caratteristiche essenziali del processo e la motivazione.

Contenuti del Processo

"Assicurare l'integrità della configurazione hardware e software richiede di definire e mantenere aggiornata un'accurata e completa repository delle configurazioni. Questo processo comprende la raccolta delle informazioni sulla configurazione iniziale, la formalizzazione della baseline, la verifica e l'audit delle informazioni sulla configurazione e l'aggiornamento della documentazione ogniqualvolta sia necessario."

Obiettivo

"Un'efficace gestione della configurazione facilita il perseguimento di una maggiore disponibilità dei sistemi, minimizza i problemi per le aree produttive e permette di risolverli più rapidamente."

Il processo DS9 è rilevante per assicurare l'efficacia dei sistemi, ma anche la loro efficienza e disponibilità, oltre all'affidabilità dei dati. Le risorse trattate sono: le applicazioni, i dati, l'infrastruttura. Per quanto riguarda l'IT Governance, questo processo facilita principalmente la creazione di valore e secondariamente aiuta a mitigare i rischi.

Come già evidenziato nel capitolo 3, nel modello COBIT® ogni singolo Processo IT contribuisce al raggiungimento di obiettivi specifici. E' quindi possibile che attività collegate al Configuration Management possano trovare collocazione in altri processi perché ritenute più strettamente collegate agli obiettivi ed al sistema di controllo di questi altri processi. I principali collegamenti sono esposti nella tabella 1 che riepiloga gli input e gli output (referenziati come documenti) del processo DS9 ed i codici dei processi (esempio DS10) dove sono usati questi documenti.

In altre parole il Configuration Management è strettamente connesso con i seguenti processi a monte: Documentazione (AI4), Approvazione delle nuove relase (AI7), Continuità del servizio (DS4); con la Gestione degli incidenti e del service desk (DS8), la Gestione dei problemi (DS10), Gestione delle attività operative (DS13), Gestione delle modifiche (AI6), Valutazione delle performance (ME1). In generale l'analisi di un processo aziendale di gestione della configurazione deve fare riferimento anche a questi processi per quanto opportuno.

From	Inputs
AI4	User, operational, support, technical and administration manuals
AI7	Released configuration items
DS4	Criticality of IT configuration items

Outputs	To						
IT configuration/asset details	DS8	DS10	DS13				
Request for change (where and how to apply the fix)	AI6						
Process performance reports	ME1						

Tabella 1. Relazioni Configuration Management con altri processi – Fonte COBIT 4.0

In ITIL® il processo di Configuration Management è posizionato nell'ambito dei processi di Service Support ed è di particolare rilevanza per il framework. La sua definizione è la seguente: "Il processo che identifica e definisce i Configuration Item di un sistema, registra e riporta sullo stato dei Configuration Item e delle Requests for Change e verifica la completezza e correttezza dei Configuration Items" ove i Configuration Items sono "componenti di una infrastruttura o elementi, ad esempio una Request for Change, associati ad una infrastruttura che si trovano (o si troveranno) sotto il controllo del processo di Configuration Management; i Configuration Items possono variare molto in termini di complessità, dimensione e tipologia, spaziando da un intero sistema (incluso tutto l'hardware, il software e la documentazione) sino ad un singolo modulo o sub componente hardware". Secondo ITIL®, le configurazioni gestite devono essere conservate nel Configuration Management Data Base, o CMDB, l'elemento centrale del Configuration Management ma non solo.

Si può osservare che la definizione di ITIL® del processo è più operativa e che, nel contempo, COBIT® si riferisce ad un processo che può sostanzialmente coincidere con essa.

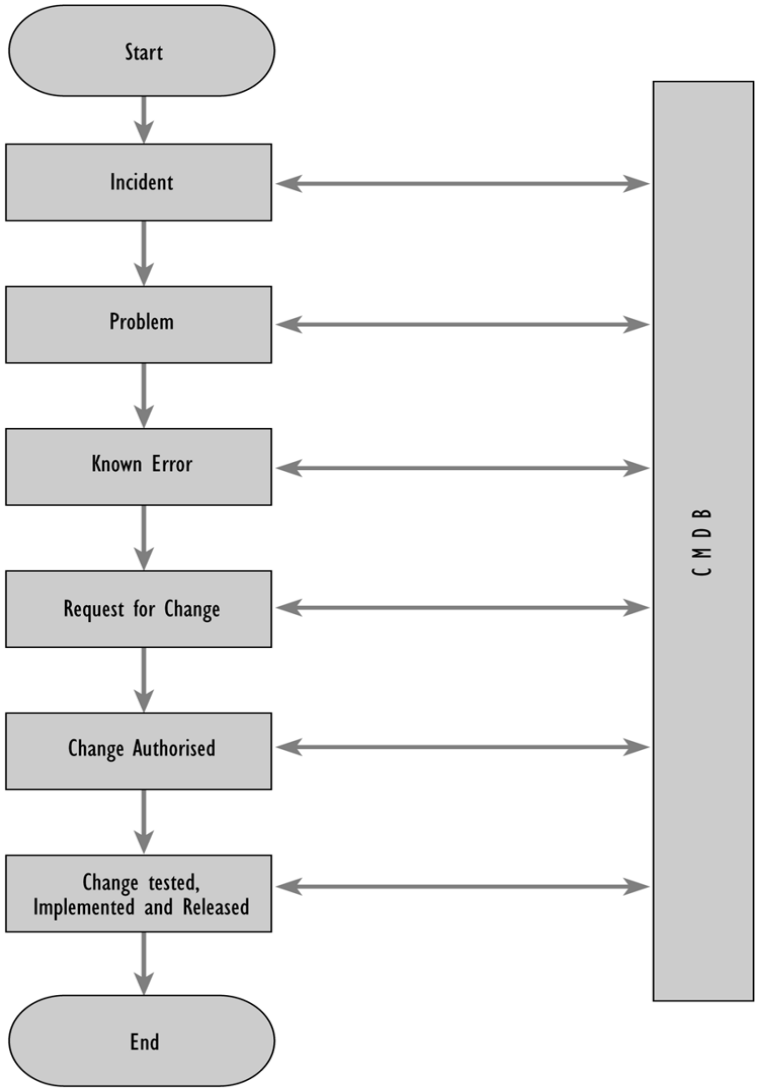

Figura 1. Interfaccia tra Incident, Change, Problem, Release Management ed il CMDB. Fonte: ITIL v2

La relazione del Configuration Management con gli altri processi ITIL®, in particolare con gli altri processi di Service Support (Incident, Change, Release e Problem Management), è di grande rilevanza ed è illustrata nella Figura 1. Il CMDB è fonte di conoscenza per valutazioni nell'ambito dell'Incident, Problem e Release Management, ed è aggiornato grazie al processo di Change Management. Ma il CMDB è anche di grande rilevanza per i processi di Service Delivery, un elemento centrale di tutto il modello ITIL®, da cui anche l'importanza del processo di Configuration Management che contribuisce alla sua creazione e mantenimento.

In ITIL® questo processo ha una collocazione centrale, infatti il CMDB contribuisce fortemente all'efficacia dell'intera practice.

6.2.3 Contenuto e struttura del processo

ITIL® identifica le attività che costituiscono il processo di Configuration Management:

- Configuration management planning (predispone un piano per l'introduzione del processo di Configuration Management);
- Configuration identification (definisce la struttura, granularità e contenuti del CMDB tra cui le baseline);
- Control of CIs (assicura che solamente che i Configuration Item autorizzati siano registrati nel CMDB);
- Configuration status accounting (reporting relativamente allo stato del CMDB e dei Configuration Items);
- Configuration verification and audit (controlla periodicamente lo stato del CMDB attraverso audit focalizzati o complessivi);
- CMDB back-ups, archives and housekeeping (manutenzione del CMDB);
- Providing a Configuration Management Service (organizzazione ed erogazione di servizi inerenti il Configuration Management, ad esempio informazioni, suggerimenti o policies).

COBIT®, con riferimento al contesto individuato nella descrizione del processo, indica quali sono i controlli che dovrebbero essere presenti in un processo di Configuration Management perché tale processo persegua efficacemente il proprio obiettivo:

DS9.1 Configuration Repository and Baseline (costruire un repository di configurazioni ed identificare le baseline o configurazioni di riferimento);

DS9.2 Identification and Maintenance of Configuration Items (assicurare che i Configuration Item siano identificati, registrati, e aggiornati);

DS9.3 Configuration Integrity Review (verificare periodicamente lo stato dei Configuration Items).

Le attività corrispondenti ai controlli sono riportate nella RACI Chart che ne attribuisce anche la responsabilità alle figure professionali tipiche dell'ambito IT.

6.2.4 Obiettivi e metriche del processo

Le finalità del processo di Configuration Management in COBIT® sono essenzialmente due: permettere all'IT di ottimizzare l'utilizzo tecnico delle risorse al fine di ridurre i costi dei processi aziendali, gestire accuratamente e proteggere i beni IT al fine di gestire i rischi dell'impresa e ottimizzare l'utilizzo dei beni aziendali.(vedere la Figura 2, combinazione degli obiettivi aziendali ed IT estratti dall'appendice I e dal processo DS9). Si precisa che il processo DS9 non è l'unico a contribuire al raggiungimento degli obiettivi indicati.

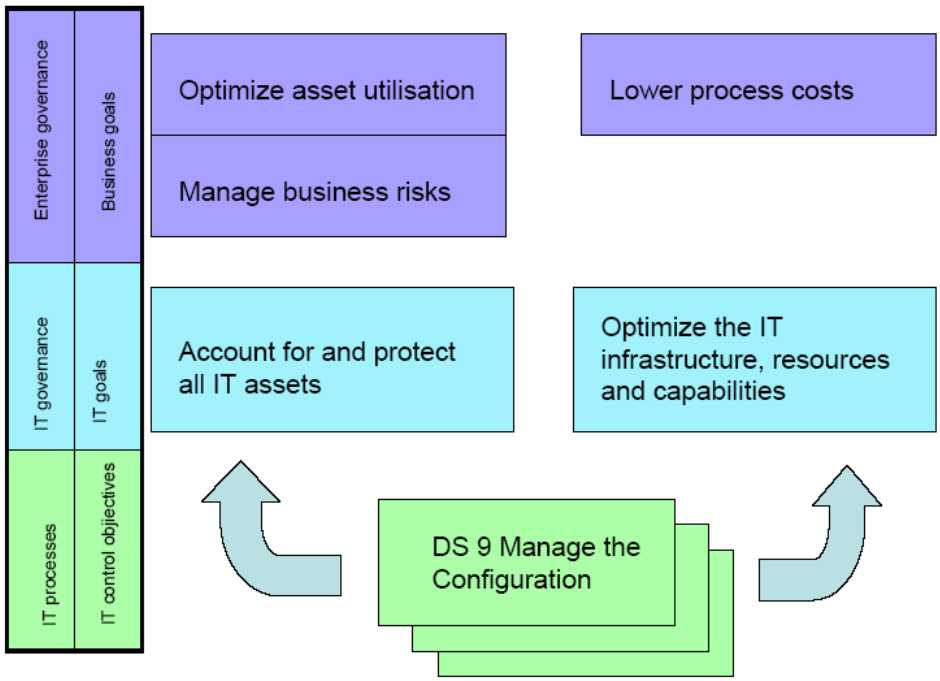

Figura 2. Obiettivi aziendali ed IT ai quali contribuisce il processo DS 9.

In ITIL® l'obiettivo del processo è quello di fornire un modello logico dell'infrastruttura/servizi, e processi in grado di identificare, controllare, mantenere e verificare i componenti, Configuration Items, che lo compongono al fine di meglio controllare infrastrutture e servizi e migliorare così l'efficienza.

Gli obiettivi di dettaglio del Configuration Management sono:

- account for all the IT assets and configurations within the organisation and its services;
- provide accurate information on configurations and their documentation to support all the other Service Management processes;
- provide a sound basis for Incident Management, Problem Management, Change Management and Release Management;
- verify the configuration records against the infrastructure and correct any exceptions.

Per quanto concerne le metriche per la misurazione del processo, ITIL® identifica un insieme di rilevazioni che riguardano il Configuration Management ma anche altri processi, ad esempio il : **Change Management**.

COBIT® fornisce un gruppo di metriche specifiche e focalizzate sul processo, illustrate in Tabella 2. Le metriche indicate da COBIT® e ITIL® appaiono diverse e complementari.

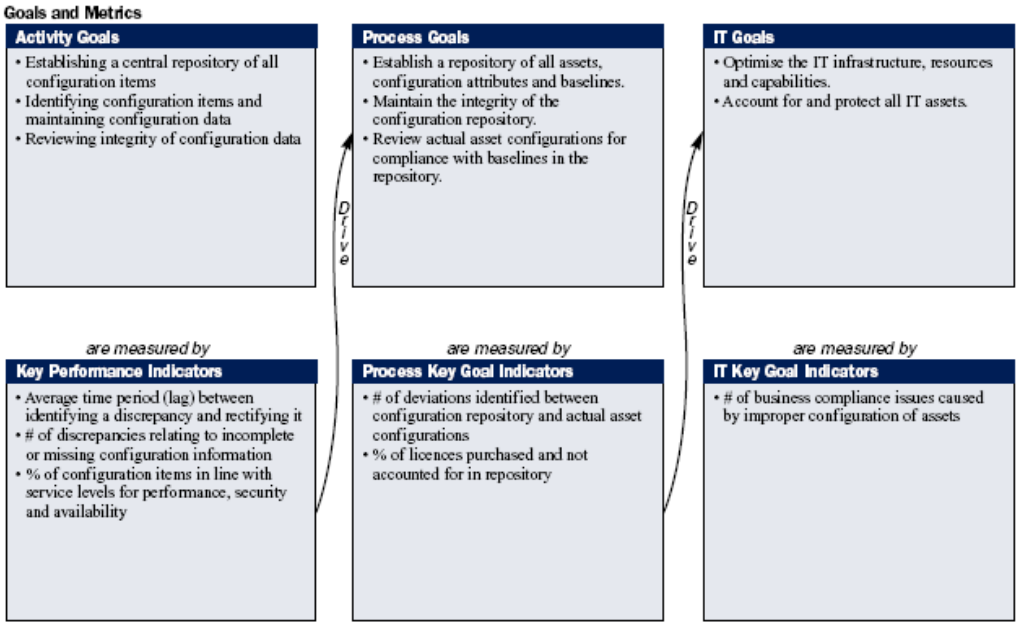

Tabella 2. Obiettivi e metriche del DS9 in CobiT – Fonte CobiT 4.0.

6.2.5 Supporto all'implementazione del processo

ITIL® offre numerose indicazioni.

Suggerimenti generali:

- che cosa si deve intendere per Configuration Management (concetti base);
- come approcciare il processo;
- i benefici del processo;
- i principali problemi che si possono incontrare nella realizzazione dei processi e le cause di fallimento più comuni;
- relazioni con altri processi.

Pianificazione ed implementazione:

- l'illustrazione delle fasi e attività che costituiscono il processo di introduzione del Configuration Management;
- caratteristiche della strumentazione a supporto da utilizzare;
- fonti e natura dei costi da prevedere;
- strutturazione del CMDB;
- natura e ciclo di vita dei Configuration Items;
- attributi dei Configuration Items;
- suggerimenti su come identificare le baseline;
- suggerimenti sulle naming conventions;
- suggerimenti sull'etichettatura degli asset;
- ecc…

Esecuzione del processo:

- fasi ed attività del processo on-going;
- suggerimenti sulla reportistica.

6.2.6 Supporto all'implementazione dei controlli del processo e alla misura della strutturazione del processo

COBIT® offre specifiche indicazioni sulle tecniche da adottare per realizzare il sistema di controllo descritto dal framework. Il fascicolo *IT Control Practice* descrive i metodi e le procedure più adatti per implementare ciascuno dei tre controlli individuati per il processo DS9.

Con quale impegno economico ed organizzativo?

COBIT® aiuta a rispondere a questa domanda con due paragrafi del processo DS9: le Audit Guidelines ed il Maturity Model.

Le *Audit Guidelines* descrivono le attività da svolgere per l'audit del processo DS9. Elencati i principali rischi del processo sono poi indicati: i ruoli aziendali da contattare e intervistare, quali documenti esaminare, quali analisi effettuare, quali test eseguire per misurare il rischio residuo.

Il *Maturity Model*, o Modello di Maturità, del processo permette di misurare – con una attività di self assessment ovvero utilizzando il precedente audit - il posizionamento as-is e determinare quello atteso secondo un paradigma che prevede le dimensioni: consapevolezza e comunicazione, politiche e procedure, competenze ed esperienze, responsabilità ed organizzazione, obiettivi e misure.

Sulla base delle misure effettuate è possibile suggerire gli interventi più opportuni al sistema di controllo per aumentare l'affidabilità del processo DS9.

6.2.7 Organizzazione e ruoli

ITIL® identifica e descrive in dettaglio le responsabilità e attività di due figure principali impegnate nel processo: il Configuration Manager ed il Configuration Librarian.

COBIT® riepiloga le responsabilità ed i ruoli ricoperti dalle tipiche figure professionali IT nel caso specifico del processo DS9.

RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security	Configuration Manager
Develop configuration management planning procedures.					C	A	C	I	C		C	R
Collect initial configuration information and establish baselines.						C	C	C			I	A/R
Verify and audit configuration information (includes detection of unauthorised software).		I				A			I		I	A/R
Update configuration repository.						R	R	R			I	A/R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Tabella 3. RACI chart dei ruoli coinvolti nel processo di Configuration Management in COBIT – Fonte COBIT 4.0.

6.2.8 Conclusioni

In questo Capitolo si sono analizzato COBIT® ed ITIL® in relazione al processo di Configuration Management e si è potuta apprezzare la complementarietà dei due framework rispetto a vari elementi importanti. Riportiamo il confronto e la complementarietà di alcuni di questi aspetti nella tabella seguente:

Definizione e posizionamento nei framework	Le definizioni sono simili. In COBIT® il processo "DS 9 – Manage the Configuration" è collocato nel dominio "Deliver and Support"; in ITIL® è posizionato nell'ambito dei processi di Service Support ed è di particolare rilevanza per il framework a causa del ruolo del suo elemento centrale: il Configuration Management Data Base (CMDB).
Contenuti e struttura	In COBIT®: DS9.1 Configuration Repository and Baseline;DS9.2 Identification and Maintenance of Configuration Items; DS9.3 Configuration Integrity Review. In ITIL®: Pianificazione del Configuration Mgmt; Identificazione Configurazioni; Controllo dei CI; Resoconto della situazione delle Configurazioni; Verifica e audit delle configurazioni; Back-up, archiviazione e custodia sicura del CMDB; Fornitura di Servizi per il Configuration Mgmt.
Metriche e KPI	Le metriche indicate da COBIT® e ITIL® appaiono diverse e complementari. In ITIL® alcune metriche riguardano anche altri processi , ad es. il Change Mgmt. In COBIT® sono proposte metriche specifiche e focalizzate sul processo suddivise tra KPI e KGI (Key Goal Indicator), oltre a un modello per misurare la strutturazione del processo.
Organizzazione e ruoli	ITIL® identifica e descrive in dettaglio le responsabilità e attività delle due figure principali impegnate nel processo: il Configuration Manager e il Configuration Librarian. COBIT® mappa le responsabilità ed i ruoli del processo sulle tipiche figure professionali di una organizzazione IT.
Supporto alla implementazione.	ITIL® offre numerosi aiuti: come approcciare il processo; i principali problemi che si possono incontrare nella realizzazione e le cause dei fallimenti più comuni; relazioni con altri processi. COBIT® supporta l'individuazione di priorità sostenibili attraverso il Maturity Model e la progettazione dei controlli (IT Control Practice).

In generale si sottolinea che esiste una chiara interrelazione e potenziale sinergia fra i due framework: COBIT® definisce i controlli per l'IT in relazione ai processi aziendali e ITIL®, a sua volta, mediante la definizione dei processi di servizio, suggerisce la miglior strutturazione dei processi affinché possano perseguire gli scopi specifici e soddisfarne i controlli.

6.3 Seconda parte: il caso

Di Federico Corradi, Stefano Niccolini

Questo caso è relativo ad una parte di un Progetto per il conseguimento della conformità alla Sarbanes- Oxley da parte di una Società multinazionale che opera nel settore dei servizi e che intende quotarsi alla Borsa di New York.

Si è introdotto questo esempio centrato sulla Sarbanes-Oxley (Sarbox) per il fatto che il meccanismo per raggiungere la conformità comporta una combinazione congiunta di

COBIT® e ITIL®.

Il Progetto che si descrive in questo caso è quello sviluppato nella Consociata italiana della Società, in allineamento alle politiche decise dalla Direzione Corporate.

6.3.1 Premessa sulla Sarbanes-Oxley e sua applicazione a questo Progetto

Il "Public Company Accounting Reform and Investor Protection Act", meglio conosciuto con il nome di "Sarbanes-Oxley Act" dal nome dei parlamentari proponenti, conosciuto con diverse abbreviazioni, fra cui SOX, SOXA, SOA e Sarbox, è una legge entrata in vigore nel 2002 negli Stati Uniti in risposta ad alcuni scandali finanziari di vaste proporzioni connessi alla sfera della Corporate Governance.

Contiene un insieme di norme che regolamentano il comportamento delle Società quotate sul mercato statunitense, nonché dell'Alta Direzione e dei revisori esterni delle stesse Società.

Si compone di molteplici sezioni, alcune delle quali introducono specifici requisiti ed obblighi delle Società in relazione al sistema di controllo interno sul processo di predisposizione del bilancio (*Internal Controls over Financial Reporting – di seguito "ICFR"*).

Le principali sezioni che introducono tali obblighi sono due:

- Section 302, Corporate Responsibility for Financial Reports (title III – Corporate Responsibility);
- Section 404, Management Assessment of Internal Controls (title IV – Enhanced Financial Disclosures).

In particolare, la Sezione 404 della Sarbox è quella per la quale una società deve attestare l'adeguatezza e l'efficacia dei controlli interni sul reporting contabile e di bilancio, e tale attestazione deve essere accompagnata da un'analoga attestazione rilasciata da un revisore terzo.

Tale sezione è quella i cui adempimenti hanno maggiore impatto sull'IT; infatti, l'attestazione del revisore terzo deve essere rilasciata sulla base di un'attività di revisione condotta in conformità alle previsioni dello standard di revisione n° 2 del PCAOB[8], il quale include espressamente i controlli generali sull'IT ed i controlli applicativi fra i controlli rilevanti nell'ambito dei controlli sul Financial Reporting[9].

Pertanto, le Società soggette a SOXA sono anche chiamate a documentare e valutare l'efficacia dei propri controlli generali sull'IT – con particolare focus, in relazione alle previsioni dell'Audit Standard 2 del PCAOB, sui controlli generali concernenti il change management e la gestione della sicurezza.

[8] Organismo USA di controllo sui revisori, introdotto da Sarbox.

[9] Secondo la solita logica per cui i controlli generali supportano l'affidabilità di altri controlli – fra i quali ad esempio i controlli applicativi e/o i controlli di segregazione dei compiti, etc. – mentre i controlli applicativi vanno inclusi fra i controlli di processo.

Per ottenere tale risultato è essenziale esaminare, contestualmente all'analisi dei processi di business, anche anche le applicazioni ed i sistemi e processi IT a supporto.

A tale scopo, ed al fine di indirizzare le analisi da condurre, all'inizio del Progetto è stato esaminato il documento "IT Control Objectives for Sarbanes-Oxley" pubblicato dall'IT Governance Institute (ITGI), specificamente indirizzato a rispondere ai requisiti della Sezione 404.

"IT Control Objectives for Sarbanes-Oxley" inquadra gli obiettivi di controllo COBIT® per l'IT nel contesto del COSO Framework, modello di riferimento per i sistemi di controllo interno di cui l'Audit Standard 2 del PCAOB fa esplicita menzione quale modello di riferimento accettabile ai fini SOXA.

In particolare, l'IT Governance Institute (ITGI) ha individuato un sotto insieme di COBIT® per l'Audit Sarbox, che prevede obiettivi di controllo in 27 diverse aree di processo (Appendice C del documento ITGI citato). Gli obiettivi di controllo COBIT® selezionato ai fini SOXA sono stati inoltre contestualizzati nell'ambito delle componenti previste dal COSO framework[10].

Quanto sopra è rappresentato nella tabella contenuta nella figura 3 a pagina seguente tratta dal documento ITGI citato. In essa le 27 aree di Processo sono quelle elencate nelle righe marcate con dei pallini nelle prime due colonne di sinistra e di questi processi il Progetto in oggetto ha scelto di concentrarsi sui 15 contraddistinti da frecce sulla sinistra della tabella.

Le due frecce più spesse (verdi) segnalano il processo di Configuration Management.

Inoltre a causa del collegamento operativo tra i processi aziendali che impattano sui rapporti finanziari e i Processi IT, ITIL® è stato preso in considerazione come insieme di linee guida a cui si devono adeguare i processi IT.

Infatti esiste una chiara interrelazione tra ITIL® e COBIT®: quest'ultimo definisce i controlli per IT in relazione ai processi aziendali e ITIL® suggerisce la migliore strutturazione dei processi IT. L'applicazione congiunta dei due modelli di fatto facilita la conformità alla Sarbox.

[10] Control Environment, Risk Assessment, Control Activities, Information & Communication, Monitoring.

Figure 10—CobiT Areas/COSO Components

Company Level	Activity Level	CobiT Area	COSO Component: Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring
		Plan and Organize (IT Environment)					
●		IT strategic planning	●	●		●	●
●		Information architecture			●	●	
		Determine technological direction					
●		IT organization and relationships	●			●	
		Manage the IT investment					
●		Communication of management aims and direction	●			●	●
●		Management of human resources	●			●	
●		Compliance with external requirements				●	●
●		Assessment of risks		●			
		Manage projects					
●		Management of quality	●		●	●	●
		Acquire and Implement (Program Development and Program Change)					
		Identify automated solutions					
	●	Acquire or develop application software			●		
	●	Acquire technology infrastructure			●		
	●	Develop and maintain policies and procedures			●	●	
	●	Install and test application software and technology infrastructure			●		
	●	Manage changes			●		●
		Deliver and Support (Computer Operations and Access to Programs and Data)					
	●	Define and manage service levels	●		●		●
	●	Manage third-party services	●	●	●		●
●		Manage performance and capacity			●		●
		Ensure continuous service					
	●	Ensure systems security			●	●	●
		Identify and allocate costs					
●		Educate and train users	●			●	
		Assist and advise customers					
	●	Manage the configuration			●	●	
	●	Manage problems and incidents			●	●	●
	●	Manage data			●	●	
●		Manage facilities		●			
	●	Manage operations			●	●	
		Monitor and Evaluate (IT Environment)					
●		Monitoring				●	●
●		Adequacy of internal controls					●
●		Independent assurance	●				●
●		Internal audit					●

(*) Processi CobiT che fanno parte del Progetto

Figura 3 - Processi del Progetto in esame rispetto ai Processi di CobiT e alle Componenti di COSO per Sarbanes-Oxley, la figura 10 interna è tratta da "IT Control Objectives for Sarbanes-Oxley" pubblicato da ITGI.

Nel presente documento non si potrà coprire tutti gli aspetti di questo tipo di Progetto, che è complesso, ma si descriveranno alcune sue fasi che daranno un'idea dell'applicazione coordinata di CobiT® ed ITIL®.

Per aderire all'approccio del Progetto impostato dalla Direzione Corporate, le fasi principali da eseguire da parte di ogni Consociata - prima dell'Audit conclusivo - sono le seguenti:

- Documentazione dei Processi
- Documentazione dei Rischi e dei Controlli per mitigarli
- Esecuzione dei Controlli
- Valutazione periodica dei Controlli
- Valutazione dell'impatto e della probabilità dei Rischi

Questo Caso, dopo un cenno alla fase A, illustra la fase B (quali controlli fare e dove inserirli) che costituisce un esempio significativo di applicazione congiunta di COBIT® e ITIL®.

6.3.2 Fase A

La base di partenza è stata la documentazione prodotta dalla Corporate della Società, completamente allineata ad ITIL®.

La Consociata italiana ha esaminato i *gap* esistenti tra i Processi attualmente utilizzati e le indicazioni ricevute e ha definito un percorso per ottenere progressivamente la conformità.

6.3.3 Fase B

Il seguito di questo paragrafo è dedicato alla Fase B il cui obiettivo è quello di identificare i Controlli necessari per coprire i Rischi definiti dal Progetto per i due Processi oggetto del Caso.

Controlli per mitigare i Rischi del Configuration Management
Il Rischio è stato sinteticamente espresso come segue.

I componenti dei Servizi ICT non sono configurati in modo appropriato per fornire un'elaborazione delle informazioni accurata, completa e sicura.

Esempi di rischi aggiuntivi definiti dalle specifiche di Progetto sono:

- Le componenti ICT non sono configurate in modo appropriato per consentire accessi basati su richieste del Management
- Le componenti ICT non forniscono un supporto adeguato per la verifica/registrazione delle configurazioni correnti.

La guida ai controlli è stata tratta dal documento citato "IT Control Objectives for Sarbanes-Oxley", Appendice C, e si collega ai rischi sopra nominati nel modo seguente:

- Obiettivo dei Controlli: fornire una ragionevole assicurazione che le componenti ICT, per quello che riguarda le loro relazioni con la sicurezza, l'elaborazione e la disponibilità, sono ben protette, in quanto sono in grado di prevenire ogni modifica non autorizzata e di dare supporto alla verifica e registrazione delle Configurazioni correnti.
- Ragioni alla base dei Controlli: Il Configuration Management assicura che i controlli su sicurezza, disponibilità e completezza delle elaborazioni siano definiti nei sistemi e mantenuti operanti durante il loro intero ciclo di vita. Controlli insufficienti sulle configurazioni possono causare esposizioni a rischi di sicurezza e disponibilità, concretamente possono permettere accessi non autorizzati ai sistemi e ai dati e avere impatti sui dati finanziari prodotti.

Un estratto delle linee guida di maggior dettaglio per i controlli e per i test del processo di Configuration Management sono riepilogati nella seguente tabella:

Linee guida dei Controlli e dei relativi Test per il Configuration Management	
Controlli	**Test sui Controlli**
a) L'infrastruttura sistemi, inclusi Firewall, Router, Switch, Sistemi Operativi di Rete, Server e altri simili dispositivi, deve essere configurata opportunamente per prevenire accessi non autorizzati	**a')** Determinare se le Policy dellasocietà richiedono la documentazione delle Configurazioni correnti, così come le impostazioni di configurazione della sicurezza da realizzare. Rivedere un campione di server, firewall, router, ecc. per esaminare se essi siano stati configurati in accordo con la politica dell'Azienda
b) Il Software applicativo e i sistemi di archiviazione dati devono essere correttamente configurati per permettere accessi basati sulle esigenze dimostrabili dei singoli individui per consultare, aggiungere, modificare o cancellare dati	**b')** Condurre una valutazione della frequenza e tempestività delle revisioni dei record di Configurazione da parte dei Responsabili. Valutare se esiste la documentazione delle procedure di Gestione delle Configurazioni Rivedere un campione di Modifiche, Aggiunte o Cancellazioni delle Configurazioni, per valutare se esse siano state correttamente approvate, sulla base di esigenze dimostrate
c) Test e valutazioni devono essere effettuati periodicamente per confermare che il software e l'infrastruttura di rete siano correttamente configurati (in relazione ad un insieme di Configurazioni base di riferimento)	**c')** Rivedere l'infrastruttura Software e di Rete per verificare che essa sia stata correttamente configurata e mantenuta, secondo un Processo aziendale documentato

Responsabilità dei Controlli e dei Test

Affinché il processo di Configuration Management funzioni correttamente deve anzitutto essere definito il Responsabile del Processo, secondo ITIL®: il "Configuration Manager".

Egli deve definire il Processo stesso e mantenerlo aggiornato e dovrà essere coinvolto nei Controlli e dei relativi test da parte dello specifico Responsabile, che denominiamo "Esecutore dei Controlli".

Dove inserire i Controlli

Per poter posizionare con precisione i Controlli che mitigano i Rischi, è necessario definire il Processo di Configuration Management in modo strutturato, documentato, allineato a quanto definito dalla Direzione Corporate.

Tra le fasi principali finalizzate alla gestione ci sono quelle relative al Configuration Management Data Base:

- Identificazione dei CI e dei relativi attributi
- Loro controllo/verifica

Queste due fasi si debbono mappare sul Processo definito dalla Corporate e costituiscono il presupposto base per alcuni dei Controlli e dei Test previsti per questo Processo, indicati nella tabella della pagina precedente.

Nel diagramma di flusso del Processo predisposto dalla Direzione Corporate si prendono in considerazione i seguenti sotto-Processi:

"Aggiornamento dei CI e di quelli collegati:

- "Validazione dei requisiti": ricevere e controllare le richieste di nuove Configurazioni.
- "Aggiornamento CMDB": aggiornare il CMDB con i nuovi componenti (creazione di nuovi CI), o modificare i CI esistenti in seguito ad un Change.

"Incongruenze delle Configurazioni" e in cascata i suoi componenti:

- "Soglia di incongruenza Configurazioni" ed il suo sotto-processo
- "Esame e risoluzione delle incongruenze" : si propongono di rilevare discordanze tra i dati delle Configurazioni (nei CI) e l'infrastruttura esistente e di risolvere le incongruenze riscontrate.

I Test sui Controlli vanno effettuati nell'ambito degli stessi sotto-Processi, con la periodicità opportuna. Inoltre i test devono verificare se le Procedure sono correttamente documentate e se esistono Policy aziendali formalizzate.

In base a quanto sopra specificato su dove inserire i Controlli e considerando i Controlli da fare, contenuti nella tabella a pagina 97, di questi ultimi si commentano ulteriormente quelli contraddistinti come "**b**" e "**c**":

b: I relativi flussi prevedono che:

- le richieste di creazione di record nel CMDB (CI) vengano effettuate dopo opportuna validazione
- vengano verificate le incoerenze tra richieste e registrazioni preesistenti sul CMDB
- vengano analizzate e risolte eventuali situazioni dubbiose

c: Le valutazioni e i test di questo tipo di Controllo possono iniziare:

- nel sotto processo "Incongruenze delle Configurazioni", per proseguire per approfondimenti nei sotto-processi "Soglia di incongruenza Configurazioni" ed "Esame e risoluzione delle incongruenze".
- e qualora vengano riscontrate delle situazioni anomale, saranno avanzate richieste di correzioni di singoli elementi (CI) del CMDB, tramite i flussi "Validazione dei requirement" e "Aggiornamento CMDB".

La Consociata italiana a fronte di queste norme emesse dalla Direzione Corporate ha individuato il gap esistente fra i controlli e e test previsti e quelli in essere ed ha definito un progetto per la riduzione di questi gap.

Inoltre, poiché non disponeva di un CMDB - come previsto dalle best practice e richiesto dalla Direzione Corporate – ha avviato un progetto di analisi di fattibilità.

Le modalità di esecuzione dei Test sui Controlli, la valutazione periodica dei Controlli e la Valutazione dell'impatto e della probabilità dei Rischi, sono al di fuori degli obiettivi del presente documento.

7 Caso di applicazione congiunta: Service Level Management

di Andrea Pederiva, Maxime Sottini

7.1 Introduzione

L'argomento è trattato strutturando il capitolo in due parti. La prima ha come obiettivo quello di tracciare un confronto specifico tra i due framework in relazione al processo di Service Level Management. Questa analisi completa ed integra quella operata ad un livello più alto nel capitolo 5.

La seconda parte illustra invece un caso di applicazione congiunta dei framework, ripercorrendo le attività svolte, identificando i contributi specifici di COBIT® e ITIL®, per poi concludere con un'opninione in merito alla complementarietà nel caso del Service Level Management.

7.2 Prima parte: confronto Service Level Management

Nel seguito il processo di Service Level Management è esaminato ponendo a confronto i framework COBIT® e ITIL®, con riferimento a diverse prospettive di analisi, in particolare:

- definizione e posizionamento del processo nei framework;
- contenuto e struttura del processo;
- obiettivi del e metriche del processo;
- organizzazione e ruoli previsti a supporto del processo;
- supporto all'implementazione del processo;
- supporto all'implementazione dei controlli del processo e alla misura della strutturazione del processo.

7.2.1 Definizione e posizionamento del processo nei framework

Il Service Level Management è uno dei processi di maggior importanza sia per COBIT®, sia per ITIL®. In particolare per quest'ultimo che, essendo una "practice" per la gestione ottimale dei servizi IT trova nel Service Level Management un punto di partenza (definizione di servizio, di catalogo dei servizi, di criteri di misurazione della loro erogazione e definizione dei valori target) ma anche di arrivo (misurazione della qualità effettiva del servizio erogato). In ITIL®, il processo è posizionato nell'ambito del Service Delivery ed ha numerose interazioni con gli altri processi dello stesso ambito, come è possibile osservare in figura 1, ma non solo.

Esso può fornire i requisiti e misurare le performance di tutti i processi per cui sono definiti obiettivi, ad esempio anche quelli di Incident Management, Change Management, Problem Management, Release Management.

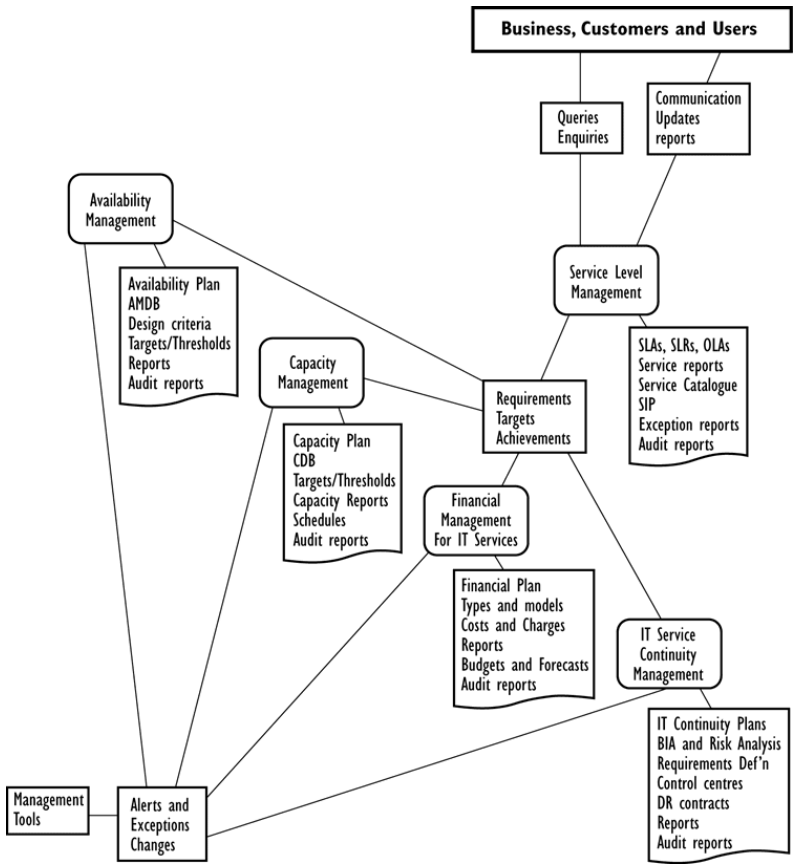

Figura 1. Le principali relazioni tra i processi di Service Delivery – Fonte ITIL Service Delivery.

Per ITIL® la definizione di "Service Level Management" è la seguente: Service Level Management è il processo di pianificazione, coordinamento, predisposizione, definizione, monitoraggio, reporting e revisione dei Service Level Agreements, ovvero degli accordi tra un IT Service Provider - (interno o esterno) ed il cliente (non necessariamente un contratto). I Service Level Agreements o, più semplicemente, SLAs definiscono gli obiettivi per i servizi e le responsabilità di entrambe le parti. Il processo ha come finalità anche quella di assicurare che la qualità richiesta sia giustificabile in relazione ai costi e che, oltre ad essere raggiunta, venga gradualmente e continuamente incrementata.

In COBIT® il processo "DS1 – Definire e gestire i livelli di servizio" è posizionato nell'ambito dei processi di "Deliver and Support", ovvero dell'insieme dei processi focalizzati sull'erogazione e supporto dei servizi IT, ed è così sintetizzato: "Per facilitare l'allineamento tra i servizi IT e i relativi requisiti aziendali è necessario istituire efficaci comunicazioni tra l'IT ed i clienti interni relativamente alla richiesta di servizi. Tali comunicazioni sono rese possibili da una definizione ben documentata e un accordo sui servizi IT e sui livelli di servizio. Questo processo comprende anche il monitoraggio ed il reporting tempestivo agli enti interessati, del raggiungimento dei livelli di servizio."

Le relazioni con altri processi del framework sono molteplici, ben identificate e mappate come si evince in figura 2.

From	Inputs
PO1	Strategic and tactical IT plans, IT service portfolio
PO2	Assigned data classifications
PO5	Updated IT service portfolio
AI2	Initial planned SLAs
AI3	Initial planned OLAs
DS4	Disaster service requirements including roles and responsibilities
ME1	Performance input to IT planning

Outputs	To						
Contract review report	DS2						
Process performance reports	ME1						
New/updated service requirements	PO1						
SLAs	AI1	DS2	DS3	DS4	DS6	DS8	DS13
OLAs	DS4	DS5	DS6	DS7	DS8	DS11	DS13
Updated IT service portfolio	PO1						

Figura 2. Relazioni del Service Level Management in COBIT con altri processi – Fonte COBIT 4.0

7.2.2 Contenuto e struttura del processo

Per il processo di Service Level Management COBIT® e ITIL® sono, come ci accingiamo ad illustrare, fortemente complementari. In primo luogo esaminiamo il contenuto e la struttura del processo secondo i due framework. In ITIL® si ritrova lo schema di figura 3, ripreso ed approfondito in forma discorsiva nell'ambito della trattazione del processo (capitolo Service Level Management del libro Service Delivery). COBIT® classifica il processo secondo dei criteri di valutazione delle informazioni, delle risorse interessate, dell'ambito di contribuzione all'IT Governance ed espone sinteticamente gli obiettivi del processo, le caratteristiche del suo sistema di controllo e le principali metriche. La parte centrale è costituita dalla descrizione del sistema di controllo attraverso l'elencazione degli obiettivi di controllo.

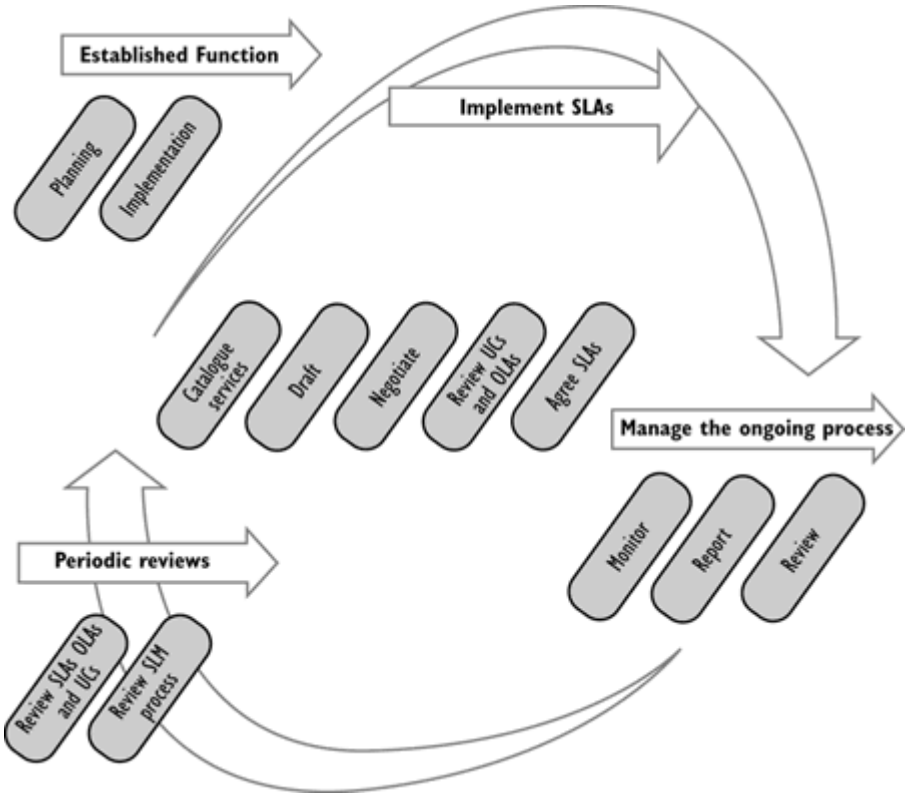

Figura 3. Il processo di Service Level Managmeent secondo ITIL –Fonte ITIL Service Delivery.

DS1 Define and Manage Service Levels

DS1.1 Service Level Management Framework
Define a framework that provides a formalised service level management process between the customer and service provider. The framework maintains continuous alignment with business requirements and priorities and facilitates common understanding between the customer and provider(s). The framework includes processes for creating service requirements, service definitions, service level agreements (SLAs), operating level agreements (OLAs) and funding sources. These attributes are organised in a service catalogue. The framework defines the organisational structure for service level management, covering the roles, tasks and responsibilities of internal and external service providers and customers.

DS1.2 Definition of Services
Base definitions of IT services on service characteristics and business requirements, organised and stored centrally via the implementation of a service catalogue/portfolio approach.

DS1.3 Service Level Agreements
Define and agree to service level agreements for all critical IT services based on customer requirements and IT capabilities. This covers customer commitments, service support requirements, quantitative and qualitative metrics for measuring the service signed off on by the stakeholders, funding and commercial arrangements if applicable, and roles and responsibilities, including oversight of the SLA. Items to consider are availability, reliability, performance, capacity for growth, levels of support, continuity planning, security and demand constraints.

DS1.4 Operating Level Agreements
Ensure that operating level agreements explain how the services will be technically delivered to support the SLA(s) in an optimal manner. The OLAs specify the technical processes in terms meaningful to the provider and may support several SLAs.

DS1.5 Monitoring and Reporting of Service Level Achievements
Continuously monitor specified service level performance criteria. Reports are provided in a format meaningful to the stakeholders on achievement of service levels. The monitoring statistics are analysed and acted upon to identify negative and positive trends for individual services as well as for services overall.

DS1.6 Review of Service Level Agreements and Contracts
Regularly review service level agreements and underpinning contracts with internal and external service providers to ensure that they are effective, up to date, and that changes in requirements have been accounted for.

Tabella 1. Obiettivi di controllo per il Service Level Management in CobiT – Fonte CobiT 4.0

Una tra le più importanti differenze tra le due best practice è che COBIT® descrive i controlli (sistema dei controlli) e ITIL® descrive le attività (organizzazione e workflow). Tale complementarietà è ben rappresentata in figura 4 dove sono mappati sia i controlli che le attività.

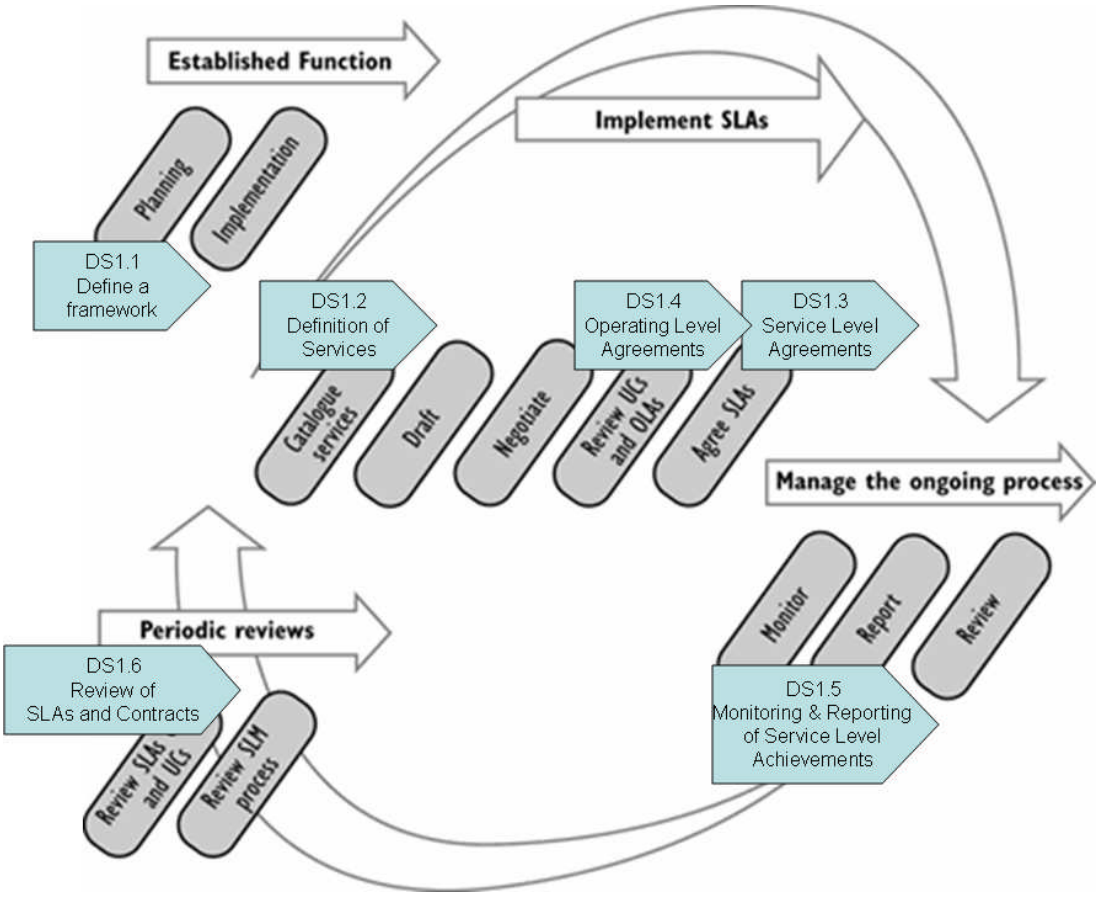

Figura 4. Raffronto COBIT/ITIL che illustra la sovrapposizione delle attività.

7.2.3 Obiettivi e metriche del processo

In merito agli obiettivi del processo ITIL® esprime quello di "mantenere e migliorare la qualità del servizio IT", tramite l'esecuzione in continuo delle attività che lo costituiscono. COBIT® ha come obbiettivo di alto livello, High-level Control Objective, la definizione e gestione dei livelli di servizio finalizzata ad una migliore comunicazione tra IT e Business ed all'allineamento dei Servizi IT con i requisiti dei processi di business. La materia è approfondita e gli obiettivi sono dettagliati a livello di attività, processo e business e sono individuate le metriche con cui la misurazione del raggiungimento degli obiettivi deve essere determinata (Tabella 2). E' questo un aspetto complementare di COBIT® rispetto ad ITIL® poiché, anche se quest'ultimo indica alcune metriche e KPI, quelle previste in COBIT® risultano più complete, dettagliate ed applicabili. In ITIL® infatti, la maggioranza delle metriche non individuano chiaramente misuratori ma risultano, piuttosto, suggerimenti su cosa misurare. In altre parole ITIL® individua principalmente l'aspetto o l'ambito su cui introdurre metriche, mentre COBIT® le precisa meglio.

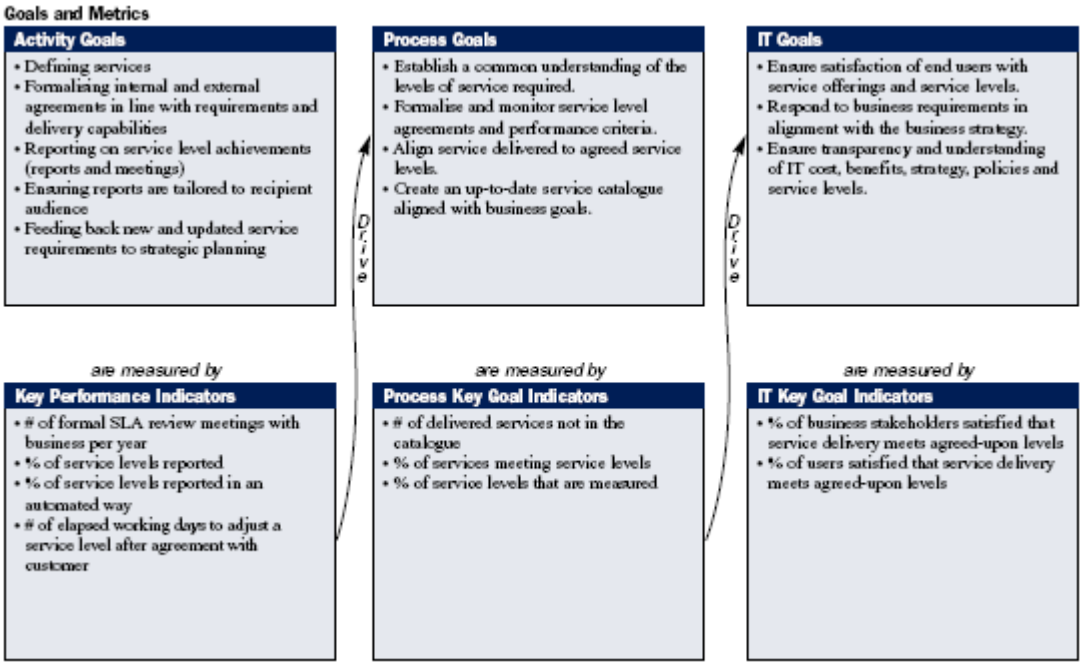

Tabella 2. Metriche per il Service Level Management in COBIT – Fonte COBIT 4.0.

7.2.4 Organizzazione e ruoli

Infine, un aspetto di fondamentale importanza per la progettazione e l'implementazione del Service Level Management: l'organizzazione ed i ruoli coinvolti. ITIL® raccomanda un "owner" per il processo, il Service Level Manager, di cui fornisce in dettaglio responsabilità, principali skill richiesti e per cui fornisce suggerimenti per il posizionamento organizzativo. COBIT® prevede diversi ruoli nell'ambito del Service Level Management, come illustrato in tabella 3. Il Service Manager è il ruolo che coincide con quello ITIL® di Service Level Manager.

RACI Chart — **Functions**

Activities	CEO	CFO	Business	CIO	Business	Head O	Chief A	Head D	Head I	PMO	Compl. Risk & Security	Service Manager
Create a framework for defining IT services.			C	A	C	C	I	C	C	I	C	R
Build an IT service catalogue.			I	A	C	C	I	C	C	I	I	R
Define service level agreements (SLAs) for critical IT services.		I	I	C	C	R	I	R	R	C	C	A/R
Define operating level agreements (OLAs) for meeting SLAs.				I	C	R	I	R	R	C	C	A/R
Monitor and report end-to-end service level performance.				I	I	R		I	I		I	A/R
Review SLAs and underpinning contracts.		I		I	C	R		R	R		C	A/R
Review and update IT service catalogue.			I	A	C	C	I	C	C	I	I	R
Create service improvement plan.			I	A	I	R	I	R	C	C	I	R

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.

Tabella 3. RACI chart dei ruoli coinvolti nel processo di Service Level Management in COBIT – Fonte COBIT 4.0.

La complementarietà di ITIL® e COBIT® emerge ancora una volta poiché si osserva che:

- ITIL® approfondisce responsabilità e skill del Service Level Manager (Annex 4A del Service Delivery ITIL) mentre COBIT® mappa tutti i ruoli sulle tipiche figure professionali dell'IT;
- ITIL non approfondisce né identifica altri ruoli coinvolti nel processo al contrario di COBIT® (tabella 3).

7.2.5 Supporto all'implementazione del processo

E' quando si decide di implementare il processo che ITIL torna nuovamente ad essere il framework di riferimento. Nel seguito si illustrano le aree di approfondimento per le quali la best practice offre suggerimenti operativi e raccomandazioni.

Suggerimenti generali:

- che cosa si deve intendere per Service Level Agreement;
- i benefici del Service Level Management;
- le voci di costo più rilevanti per l'implementazione dei processi di Service Level Management; ITIL®
- i principali problemi che si possono incontrare nella realizzazione dei processi e le cause di fallimento più comuni.
- Pianificazione del processo:
- le attività che costituiscono questa fase;
- come misurare la percezione del livello di servizio prima dell'implmentazione del processo;
- l'importanza ed il ruolo dei contratti con le terze parti;
- Key Performance Indicator (KPI) e metriche per il processo di SLM.

Implementazione del processo:

- cosa intendere per Catalogo dei Servizi;
- che cosa è un Servizio;
- come gestire le aspettative dei fruitori del processo (i "clienti") durante l'implementazione;
- come strutturare gli SLA (per servizio vs. per cliente o multi livello) e come definire i requisiti inizialmente;
- come formulare gli SLA (contenuti, suggerimenti per la redazione, esempi);
- come gestire la ricerca di consenso sugli SLA;
- come realizzare le capacità di monitoraggio del Servizio;
- il ruolo dei contratti con terze parti (underpinning contracts) con ricadute sul servizio e come gestirli;
- il ruolo del reporting e dei meccanismi di rivisitazione periodica;
- l'importanza e le modalità per diffondere la conoscenza sull'esistenza degli SLA;

- ruoli, responsabilità, skill richiesti e suggerimenti per posizionare in modo ottimale nell'organizzazione la figura del Service Level Manager, centrale per il processo.

Esecuzione del processo:

- con che frequenza, cosa comprendere nelle attività periodiche di reporting e monitoraggio e a chi divulgare i risultati;
- con quale frequenza e su cosa focalizzare gli incontri di revisione periodica dei Servizi;
- in che cosa consiste un Service Improvement Programme (SIP);
- ogni quanto e con quali modalità rivedere gli SLA e OLA;
- punti di attenzione per l'introduzione di nuovi Servizi.

7.2.6 Supporto all'implementazione dei controlli del processo e alla misura della strutturazione del processo

COBIT® offre specifiche indicazioni sulle tecniche da adottare per realizzare il sistema di controllo descritto dal framework. Il fascicolo *IT Control Practice* descrive i metodi e le procedure più adatti per implementare ciascuno dei controlli individuati per il processo DS1.

Con quale impegno economico ed organizzativo?

COBIT® aiuta a rispondere a questa domanda tramite due paragrafi del processo DS1: le Audit Guidelines ed il Maturity Model. .

Le *Audit Guidelines* descrivono le attività da svolgere per l'audit del processo DS1. Elenca i principali rischi del processo e quindi indica: i ruoli aziendali da contattare e intervistare, quali documenti esaminare, quali analisi effettuare, quali test eseguire per misurare il rischio residuo.

Il *Maturity Model*, o Modello di sostenibilità del processo, permette di misurare – con una attività di self assessment ovvero utilizzando il precedente audit - il posizionamento as-is e determinare quello atteso secondo uno schema che prevede diverse dimensioni di analisi: consapevolezza e comunicazione, politiche e procedure, competenze ed esperienze, responsabilità ed organizzazione, obiettivi e misure.

Sulla base delle misure effettuate è possibile suggerire gli interventi più opportuni al sistema di controllo per aumentare l'affidabilità del processo DS1.

7.3 Seconda parte: il caso

Conclusa la comparazione dei due framework ci focalizziamo sulla loro applicazione congiunta ad un caso. L'esempio è finalizzato ad illustrare la complementarietà pratica dei due Framework. Si riferisce all'introduzione del processo di Service Level Management con il supporto congiunto dei due framework, COBIT® e ITIL®, presso un'ipotetica azienda. Quanto illustrato potrebbe verificarsi ma non corrisponde ad un case history effettivamente verificatasi.

Dopo aver introdotto ed illustrato il contesto, il caso approfondisce gli aspetti progettuali dell'introduzione del processo, utili al fine di evidenziare le modalità di utilizzo dei due framework e la loro complementarietà. A tal fine saranno esaminati:

- Pianificazione delle attività

- Definizione dell'organizzazione e dei ruoli per la gestione del processo
- Definizione del Service Catalogue
- Definizione di Service Level Agreements e Operational Level Agreements
- Predisposizione delle Monitoring Capabilities
- Analisi degli Underpinning Contracts
- Definizione dei processi di Service Level Management "on-going"
- Metriche per la misurazione del processo

7.3.1 Introduzione ed illustrazione del contesto

Il caso aziendale prescelto è quello di un primario Gruppo Assicurativo, nel seguito Gruppo, articolato in diverse società operative, Compagnie, su diverse linee di business (es. vita, danni). Il Gruppo ha creato una società specifica responsabile dell'erogazione dei Servizi IT, nel seguito denominata Internal Sourcer o più semplicemente Sourcer. Le esigenze del Gruppo, delle Compagnie e del Sourcer sono diverse anche se gli obiettivi sono sinergici. Le Compagnie hanno come obbiettivo primario quello di allineare i Servizi IT alle esigenze di business, focalizzandosi sulle attività core e delegando la gestione dell'IT all'esterno, anche se inizialmente esclusivamente tramite un Sourcer di Gruppo, alla ricerca di maggior efficienza ed efficacia. Il Sourcer, dal canto suo, ha come obbiettivo quello di offrire Servizi IT ottimali alle Compagnie con gli unici vincoli rappresentati dal budget e dagli accordi con esse. Il Gruppo ha infine il ruolo di rendere sinergici e finalizzati al disegno di business complessivo le attività, delle singole Compagnie, inclusi gli investimenti IT.

In questo scenario generale, al fine di raggiungere i propri obiettivi e quelli delle Compagnie, il Gruppo, in coordinamento con le Compagnie, ha avviato un programma di IT Governance e, a tal fine, ha scelto COBIT® come framework di riferimento. Dal canto suo, il Sourcer avverte l'esigenza di massimizzare la propria efficacia/efficienza nell'erogazione dei Servizi IT, sia per far fronte alle esigenze delle Compagnie che per prepararsi, in un eventuale scenario futuro, ad operare sul mercato dei fornitori di Servizi IT anche per società di Assicurazione esterne al Gruppo. Per migliorare ha dunque scelto di ottimizzare i propri processi adottando il framework di riferimento ITIL® per l'IT Service Management.

In questo contesto, risulta evidente come uno dei punti centrali per Compagnie e Sourcer sia rappresentato dai Servizi e dal Service Level Management, traguardato dalle prime in ottica di allineamento dei Servizi IT con le esigenze di business e di processo rilevante ai fini della governance IT. Nell'ambito di questa convergenza di interessi, il Sourcer decide di ottimizzare il processo di Service Level Management con due obiettivi: da un lato l'ottimizzazione del processo sfruttando le best practice ITIL®, dall'altro la conformità e l'allineamento alle esigenze delle Compagnie, misurabile utilizzando COBIT®. Le iniziative sono dunque sinergiche Compagnie/Sourcer e si decide di affrontare la revisione dei processi ed il tema della loro governance con l'ausilio di COBIT® e ITIL® congiuntamente.

La decisione iniziale è quella di progettare il processo, identificando immediatamente i principali attori, secondo quanto previsto da ITIL® e COBIT®. E' così selezionato il Service Level Manager, previsto da entrambi i framework, che assume anche il ruolo di responsabile del processo e della sua progettazione. Per la sua identificazione si utilizzano gli skill e la definizione di responsabilità contenuti in ITIL®. Le altre figure previste dalla RACI COBIT® per il processo, vd. precedente tabella 3, sono pure identificate e coinvolte nel progetto secondo i ruoli previsti in COBIT®. Le funzioni di Business sono identificate nel Gruppo e nelle Compagnie, mentre le altre presso il Sourcer.

Una volta definito il team ed i ruoli in seno ad esso, è avviato il progetto di revisione del processo di Service Level Management. Il primo passo è la comprensione della situazione di partenza e la definizione degli obiettivi per il processo. A questo fine, sia COBIT® che ITIL® suggeriscono di utilizzare l'approccio basato sul Capability Maturity Model. In questo caso però, COBIT® è più analitico e fornisce una definizione dei diversi livelli di maturità specifici per il processo, come riportato in tabella 4.

Tramite un'analisi condotta con il metodo delle interviste, il team di progetto determina che lo stato di maturità iniziale dei processi è compreso tra 1 e 2. In particolare, per Servizi critici di alcune Compagnie del Gruppo sono definiti dei Livelli di Servizio o SLA (il livello di maturità applicabile è 2) ma questo non avviene per la maggioranza dei Servizi erogati dal Sourcer. Spesso il concetto stesso di Servizio non è percepito e comunemente interpretato.

MATURITY MODEL

DS1 Define and Manage Service Levels

Management of the process of *Define and manage service levels* that satisfies the business requirement for IT of *ensuring the alignment of key IT services with business strategy* is:

0 Non-existent when
Management has not recognised the need for a process for defining service levels. Accountabilities and responsibilities for monitoring them are not assigned.

1 Initial/*Ad Hoc* when
There is awareness of the need to manage service levels, but the process is informal and reactive. The responsibility and accountability for defining and managing services are not defined. If performance measurements exist, they are qualitative only with imprecisely defined goals. Reporting is informal, infrequent and inconsistent.

2 Repeatable but Intuitive when
There are agreed-upon service levels, but they are informal and not reviewed. Service level reporting is incomplete and may be irrelevant or misleading for customers. Service level reporting is dependent on the skills and initiative of individual managers. A service level co-ordinator is appointed with defined responsibilities, but limited authority. If a process for compliance to service level agreements exists, it is voluntary and not enforced.

3 Defined Process when
Responsibilities are well defined, but with discretionary authority. The service level agreement development process is in place with checkpoints for reassessing service levels and customer satisfaction. Services and service levels are defined, documented and agreed-upon using a standard process. Service level shortfalls are identified, but procedures on how to resolve shortfalls are informal. There is a clear linkage between expected service level achievement and the funding provided. Service levels are agreed to but they may not address business needs.

4 Managed and Measurable when
Service levels are increasingly defined in the system requirements definition phase and incorporated into the design of the application and operational environments. Customer satisfaction is routinely measured and assessed. Performance measures reflect customer needs, rather than IT goals. The measures for assessing service levels are becoming standardised and reflect industry norms. The criteria for defining service levels are based on business criticality and include availability, reliability, performance, growth capacity, user support, continuity planning and security considerations. Root cause analysis is routinely performed when service levels are not met. The reporting process for monitoring service levels is becoming increasingly automated. Operational and financial risks associated with not meeting agreed-upon service levels are defined and clearly understood. A formal system of measurement of KPIs and KGIs is instituted and maintained.

5 Optimised when
Service levels are continuously re-evaluated to ensure alignment of IT and business objectives, while taking advantage of technology including the cost-benefit ratio. All service level management processes are subject to continuous improvement. Customer satisfaction levels are continuously monitored and managed. Expected service levels reflect strategic goals of business units and are evaluated against industry norms. IT management has the resources and accountability needed to meet service level targets and compensation is structured to provide incentives for meeting these targets. Senior management monitors KPIs and KGIs as part of a continuous improvement process.

Tabella 4. Maturity model per il processo di Service Level Management in COBIT – Fonte COBIT 4.0.

La decisione presa da Sourcer e Gruppo, in accordo con i suggerimenti di ITIL® e di COBIT® e per la quale è calibrato l'investimento iniziale di progetto, è quella di non puntare immediatamente al massimo livello di maturità possibile per il processo di Service Level Management ma ad un livello variabile tra il tre ed il quattro, a seconda dei Servizi. Per tutti i Servizi si prevede: un processo di gestione dei livelli di servizio ben formalizzato, responsabilità ben assegnate, Servizi e relativi livelli di servizio definiti, documentati e concordati. Per i Servizi maggiormente critici, si decide anche che i

livelli di servizio vengano misurati e che il charging tenga conto delle performance raggiunte in relazione alle attese delle Compagnie (customer satisfaction, misurazione end-to-end dei livelli di servizio). Di conseguenza, il Sourcer dovrà anche operare al fine di identificare repentinamente eventuali problemi legati al Servizio ed attivare le necessarie contromisure, nonchè gestire un Service Improvement Program, come previsto da ITIL®.

Per i nuovi Servizi, la gestione dei Livelli di Servizio dovrà essere affrontata sin dalle prime fasi di progettazione. Per tutti i Servizi critici, il reporting deve essere automatizzato.

Con questi obiettivi, individuati grazie all'utilizzo congiunto di COBIT® e ITIL® applicati al contesto delle Compagnie/Sourcer, è ora possibile affrontare la fase di progettazione dei processi. I processi di dettaglio sono definiti tenendo conto delle indicazioni fornite da ITIL® e sono articolati, quando necessario, in due varianti per i Servizi critici e non. I processi sono identificati ed illustrati mediante appositi diagrammi grafici che illustrano eventi, attività, attori, sistemi informativi utilizzati a supporto, input e output, condizioni logiche per l'attivazione di flussi. I processi definiti sono quelli ricorsivi, ovvero quelli appartenenti alle categorie illustrate in figura 4 "Manage the ongoing process" e "Periodic reviews", nonché quelli di introduzione di nuovi Servizi. I rimanenti processi di introduzione del Service Level Management, "Established Function" e "Implement SLAs", sono invece semplicemente eseguiti una tantum, in ottica progettuale, senza una definizione formale come per i precedenti.

Nel seguito si ripercorrono alcuni passaggi fondamentali ed importanti decisioni maturate con il contributo di ITIL® e COBIT® che possono prevedere anche interpretazioni e adattamenti in logica "adopt and adapt", come raccomandato dai framework medesimi.

7.3.2 Pianificazione delle attività

Come si è già detto è nominato il Service Level Manager, definita la struttura del Team di implementazione, i suoi ruoli e responsabilità. Si predispone un piano di lavoro ed adotta una metodologia di Project Management (PRINCE2). Il progetto si articola in diverse fasi, come è possibile osservare nella tabella 5. Le prime tre sono la declinazione della fase di "Implement SLAs" prevista da ITIL® (si veda anche la precedente Figura 4).

La gestione della comunicazione ed il coinvolgimento di tutti gli attori previsti, vd. precedente tabella 3, è assicurata dall'esecuzione del progetto secondo quanto suggerito dalla metodologia PRINCE2 e soddisfa l'esigenza espressa in ITIL®.

Fase	Durata	Contenuti
Progettazione	3 mesi	Esecuzione delle attività di progettazione dei processi "on-going", dei sistemi di monitoraggio degli SLA; costruzione del catalogo dei Servizi, individuazione degli SLAs e OLAs iniziali; valutazione dello stato iniziale degli SLAs, contrattazione iniziale degli SLAs con i clienti dei Servizi.
Implementazione	3 mesi	Implementazione del sistema di monitoraggio e reporting di SLAs e OLAs. Interventi sugli "Underpinning Contracts".
Osservazione	3 mesi	Valutazione degli SLAs e OLAs effettivi ottenuti nel periodo di Osservazione. Valutazione interventi e definizione degli SLAs definitivi con i clienti.

On-going	n/a	Avvio dei processi on-going di Service Level Management.

Tabella 5. Fasi del progetto di adozione del processo di SLM in ottica COBIT /ITIL.

7.3.3 Definizione dell'organizzazione e dei ruoli per la gestione del processo

Per la numerosità dei Servizi previsti, la figura del Service Level Manager, così come individuata da ITIL®, è ritagliata verso l'alto (compiti e responsabilità di controllo del processo di SLM e supporto alla individuazione e definizione di SLAs e OLAs). Un ruolo operativo nel processo è assegnato ai Service Manager, più di uno e ciascuno responsabile di uno o più Servizi. Nel complesso, l'insieme delle responsabilità previste da ITIL® per il Service Level Manager è articolato su due ruoli, Service Level Manager e Service Manager, preesistente al progetto e punto di riferimento operativo per il Servizio, con responsabilità in relazione ad altri processi (es. Incident Management, Problem Management, ecc.).

7.3.4 Definizione del Service Catalogue

Le Compagnie avevano già definito un certo numero di Servizi prima dell'avvio del progetto che rappresenta l'occasione per razionalizzare e completare il lavoro già svolto. Il contributo di ITIL® è importante per comprendere come identificare e classificare i Servizi e così strutturare il Catalogo. Il risultato sono più di 100 Servizi, ognuno descritto tramite una scheda che prevede, tra l'altro, le seguenti informazioni: Service Manager, descrizione del Servizio, configurazione del Servizio (in termini di CIs e loro relazioni), clienti che usufruiscono del Servizio, referenti per il Servizio, presenza di SLAs ed eventuale indicazione del documento. I Servizi identificati possono essere multi Compagnia o mono Compagnia. La struttura del Catalogo Servizi che ne consegue è quindi fondamentalmente Service Based, con la possibilità di SLAs specifici per Compagnia. I Servizi sono raggruppati in categorie, tra cui ad esempio i Business Services (percepiti direttamente dai Clienti) e Infrastructural Services (indispensabili per il funzionamento di altri Servizi).

Nell'ambito del Catalogo Servizi, in accordo con le Compagnie, sono individuati quelli critici per cui devono essere identificati SLAs.

7.3.5 Definizione di Service Level Agreements e Operational Level Agreements

Si adottano le definizioni di ITIL®. In particolare si decide di concentrarsi sugli SLA end-to-end, percepiti dall'utenza dei Servizi per i Servizi che sono individuati come critici. Sono comunque individuati, ogni qual volta possibile, OLA end-to-end per i Servizi non critici e OLA "tecnici" per il funzionamento delle componenti tecnologiche. Sono assegnate le responsabilità di monitoraggio e intervento di tutti i livelli di Servizio identificati.

In particolare, per la definizione degli SLAs end-to-end dei Servizi critici, si adotta la struttura proposta da ITIL® (paragrafo 4.6 di ITIL®, Service Delivery) che prevede le seguenti informazioni: introduzione, orario di servizio, availability, reliability, supporto, troughput, transaction response time, batch turnaround time, etc.

7.3.6 Predisposizione delle Monitoring Capabilities

Nell'ambito della progettazione e implementazione è realizzato un sistema automatico di monitoraggio e reporting degli SLAs, come suggerito da ITIL®, presupposto indispensabile per un processo di Service Level Management sostenibile. Il sistema di monitoraggio SLAs attinge informazioni ma non coincide con quello di monitoraggio dei sistemi. In effetti deve essere in grado di

elaborare i dati forniti da quest'ultimo per elaborare report sugli SLAs che tengano conto delle finestre di servizio, illustrino gli andamenti rispetto ai target e diano spiegazioni (es. dettaglio degli eventi) di deviazioni rispetto agli SLAs. Il sistema è interfacciato anche con quello di Service Desk e Incident Management, dal momento che per essi sono definiti SLAs.

Non tutti gli SLAs sono monitorati automaticamente sin dall'inizio; si stabilisce un percorso progressivo che prevede diversi momenti: dapprima un sottoinsieme dei Servizi Critici, quindi tutti i Servizi Critici, successivamente una percentuale consistente dei Servizi non Critici ed infine tutti i Servizi.

7.3.7 Analisi degli Underpinning Contracts

Come suggerito da ITIL® e da COBIT®, sin dalla fase di definizione dei draft di SLAs sono presi in considerazioni i contratti con terze parti che possono influenzare in qualche modo l'erogazione dei Servizi.

L'approccio è il seguente:

- verificare l'adeguatezza degli accordi in essere (SLAs);
- verificare la possibilità e disponibilità a modificare gli accordi in caso di inadeguatezza.

Queste attività sono eseguite durante la fase di progettazione con i seguenti esiti:

- modifica dei contratti con terze parti quando possibile (caso raro);
- evidenziazione delle modifiche da apportare alla scadenza dei contratti (caso ricorrente).

I processi on-going di Service Level Management si preoccuperanno di prendere in carico tali segnalazioni, gestirle e quindi migliorare gli SLAs nel tempo.

7.3.8 Definizione dei processi di Service Level Management "on-going"

Sono processi semplici, come previsti da ITIL®: "Monitoring and Reporting", "Service Review Meetings", "Service Improvement Programme", "Maintenance of SLAs, contract and OLAs". In aggiunta a quelli espressamente indicate da ITIL® si sono definiti anche quelli di "Create new Service"; "Close Service"; "Review Service" per la gestione di nuovi Servizi, la terminazione di Servizi non più richiesti o la gestione di importanti modifiche a Servizi esistenti.

7.3.9 Metriche per la misurazione del processo

Per il controllo del processo si decide di attivare tutte le misure previste da COBIT®, vd. precedente figura 2. Gli indicatori suggeriti da COBIT® sono misurabili in seguito al completamento delle attività precedentemente illustrate tranne che per la verifica della soddisfazione dell'utenza dei Servizi (IT goals) per la quale si decide di svolgere, oltre a Service Review Meetings previsti dai processi on-going, survey di Customer Satisfaction annuali, per Compagnia (cliente). Al Service Level Manager è affidato l'incarico di predisporre il reporting relativo al controllo del processo che non richiede particolare automazione. La relazione annuale prevista da parte del Service Level Manager è strutturata sviluppando tutti i punti suggeriti da ITIL® (vd. paragrafo 4.7 di ITIL® Service Delivery).

7.4 Conclusioni

Nella prima parte di questo capitolo abbiamo analizzato COBIT® e ITIL® in riferimento al processo di Service Level Management. Abbiamo così avuto modo di comprendere la notevole sinergia ottenibile

dall'adozione di entrambi i framework. In particolare la vicinanza in termini di contenuto del processo con complementarietà per quanto concerne gli obiettivi (cosa controllare, quali ruoli prevedere, che percorso compiere in COBIT®, come fare operativamente in ITIL®) ed il punto di vista da cui vengono traguardati (l'allineamento del business all'IT in un caso, COBIT®, il miglioramento dei Servizi IT nell'altro).

La tabella 6 sintetizza quanto emerso.

Elemento di analisi	COBIT	ITIL
Ambito e contenuto del processo	Il contenuto del processo è sostanzialmente equivalente per i due framework	
Rilevanza nel framework	**Standard**, è uno dei processi che contribuiscono al raggiungimento degli obiettivi	**Molto elevata**, è un elemento centrale del Service Management
Obiettivi del processo	Migliorare la **comunicazione e l'allineamento** Business e IT	Raggiungere e migliorare la **qualità del Servizio IT** concordata con il cliente
Metriche	**Complete e dettagliate**	Da integrare
Contributo per chi desidera implementare	Fuori ambito	**Elevato**; ricco di suggerimenti e casi pratici
Contributo per progettare i controlli	Specifico e dettagliato	Fuori ambito
Organizzazione e ruoli per il processo	**Visione complessiva** e sintetica del contributo da parte di tutti i ruoli aziendali ma **minor profondità sui ruoli specifici**	**Elevato dettaglio su ruoli specifici per il processo**; impatto su altri ruoli aziendali non esaminato

Tabella 6. Comparazione sintetica di COBIT e ITIL.

Abbiamo quindi esaminato un caso di applicazione, non reale ma realizzabile, in cui tale complementarietà è stata evidenziata. Un Sourcer di un Gruppo Assicurativo ha trovato in ITIL® una valida guida per progettare il processo di Service Level Management ottimizzandolo ai fini dell'efficienza e dell'efficacia e garantendo, nel contempo, il raggiungimento degli obiettivi di allineamento IT/Business e di controllo che il Gruppo e, in seno ad esso le diverse Compagnie, ricercano adottando il framework COBIT®.Nell'applicazione dei principi di ITIL® da parte del Sourcer non sono emerse incompatibilità ma anzi, al termine del progetto, sono risultati facilmente implementabili tutti i controlli previsti da COBIT® ai fini degli obiettivi di Attività, Processo e, più in generale IT, previsti dal framework stesso.

8 L'evoluzione di COBIT e ITIL

di Federico Corradi, Andrea Pederiva

8.1 Il futuro di COBIT

Con la versione 4 la suite COBIT® ha raggiunto un notevole livello di complessità in termini di sofisticazione degli strumenti proposti e di copertura dei temi dell'IT Governance, dell'IT Management, e del Controllo Interno sull'IT.

La suite COBIT® si compone oggi di più pubblicazioni, inclusive di specifici supporti per l'implementazione e per la formazione, pensati per diversi destinatari ed accessibili in parte liberamente dal sito di ISACA, in parte a pagamento, come indicato in figura 1.

		Top management	IT Management	IT Staff	Internal Auditor	IS Auditor	
Pubblicazioni	• Board Briefing on IT Governance	✓	✓	✓	✓	✓	●
	• Val IT	✓	✓	✓	✓	✓	●
	• Management Guidelines		✓	✓	✓	✓	●
	• Framework	✓	✓	✓	✓	✓	●
	• Control Objectives		✓	✓	✓	✓	●
	• Control Practices			✓		✓	$
	• IT Assurance Guide				✓	✓	●
	• CobiT Quickstart		✓	✓		✓	$ *
	• IT Control Objectives for Sarbanes-Oxley		✓	✓	✓	✓	●
	• CobiT Security Baseline			✓		✓	●
Ausili per l'implementazione	• IT Governance Implementation Guide			✓		✓	$
	• CobiT Online			✓		✓	$ *, **
Ausili per il Training	• CobiT Foundation Course			✓	✓	✓	$

Figura 1 - La suite COBIT: destinatari e modalità di accesso

Il presente capitolo discute l'evoluzione futura di COBIT® prendendo in esame gli sviluppi previsti per COBIT® con riferimento a due ambiti: l'arricchimento dei contenuti e delle pubblicazioni per un verso, e l'organizzazione del lavoro di ricerca per l'altro.

Sotto il profilo dei contenuti, la presenza nella suite COBIT® di più pubblicazioni e strumenti fa sì che la suite si sviluppi secondo due linee principali di evoluzione:

- lo sviluppo ed arricchimento dei contenuti in senso stretto, incluso l'adeguamento nel tempo rispetto all'evoluzione delle conoscenze e della tecnica nell'ambito dell'IT, del management dell'IT e dei relativi standard di riferimento;
- il mantenimento nel tempo della coerenza interna fra le diverse pubblicazioni e strumenti che compongono la suite.

Di fatto, la pubblicazione di COBIT® 4.0 ha interessato tre principali pubblicazioni: il Framework, i Control Objectives e le Management Guidelines; sotto numerosi profili COBIT® 4.0 ha innovato in modo significativo il nucleo dei contenuti della suite COBIT®.

In considerazione della numerosità e della rilevanza delle modifiche apportate nei contenuti da COBIT® 4.0 rispetto a COBIT® 3.0, appare possibile associare la pubblicazione di COBIT® 4.0 alla prima delle due linee evolutive indicate in precedenza; infatti, COBIT® 4.0 ha rappresentato per tali pubblicazioni un significativo elemento di discontinuità nei contenuti rispetto alle precedenti edizioni della suite.

Appare ragionevole pertanto attendersi che sotto il profilo dei contenuti l'evoluzione nel prossimo futuro sia prevalentemente orientata ad allineare le altre componenti della suite alle innovazioni già introdotte nei contenuti da COBIT® 4.0, adottando invece per le componenti interessate da COBIT® 4.0 una strategia di miglioramento più graduale.

Tale aspettativa è in linea con gli indirizzi sull'evoluzione di COBIT® forniti da alcuni fra i principali esponenti del COBIT® Steering Committee e dei gruppi di ricerca che hanno contribuito all'evoluzione dei contenuti della suite, nonché con le informazioni sugli sviluppi previsti per COBIT® fornite da ISACA (si veda www.isaca.org).

La strategia complessivamente seguita allo stato attuale da ISACA prevede come principali obiettivi il consolidamento dei contenuti introdotti da COBIT® 4.0 e l'allineamento rispetto a tali contenuti di tutti i componenti della suite.

Più specificamente, gli sviluppi previsti per COBIT® nel prossimo futuro in termini di contenuti sono quelli descritti nei seguenti paragrafi.

8.2 Pubblicazione di COBIT 4.1

Lo sviluppo di CobiT 4.1 si è concluso con il maggio 2007. I principali miglioramenti apportati rispetto a COBIT® 4.0 includono:

- il miglioramento del testo degli obiettivi di controllo, anche a seguito del lavoro di revisione ed allineamento delle pratiche di controllo (attualmente in corso);
- i miglioramenti al testo degli obiettivi di controllo derivanti dal lavoro di ricerca per lo sviluppo di "ValIT";
- l'arricchimento del framework per la parte concernente i modelli teorico-pratici a supporto della struttura di indicatori e delle metriche proposta da COBIT® 4.0.

Inoltre, saranno riorganizzati sulla base di criteri di efficacia ed efficienza del reporting, ed in particolare del reporting contabile, i controlli applicativi che in COBIT® 4.0 sono stati portati all'interno del framework; è altresì previsto che di tali controlli sia ridotta la numerosità complessiva.

8.3 Aggiornamento del mapping fra COBIT 4.1 e gli altri standard

COBIT® è stato mappato da ISACA rispetto a tutti i principali standard disponibili sul mercato per il controllo, gestione e governo dell'IT, inclusi gli standard di sicurezza. Tali mappature saranno riviste ed aggiornate con riferimento a COBIT® 4.1.

Rispetto a COBIT® 4.0 risultava già pubblicata da ISACA a Novembre 2005 un'analisi dei principali standard citati, orientata ad individuare le caratteristiche salienti di ciascuno standard e ad invididuare se nell'ambito di ciascuno standard i processi / contenuti trattati da COBIT® fossero discussi.

Tale mappatura consente pertanto di verificare rispetto ai contenuti trattati da COBIT® 4.0 se altri standard trattino lo stesso argomento, anche al fine di permettere all'utente di COBIT® di arricchire i propri riferimenti con altre fonti[11].

[11] I titolo di tale pubblicazione è "Aligning COBIT®, ITIL® and ISO 17799 for Business Benefit", sottotitolo "A Management Briefing from ITGI and OGC", ©2005, ISACA .

8.4 Aggiornamento delle Audit Guidelines

La principale pubblicazione COBIT® di utilizzo per gli IS Auditor è il volume "Audit Guidelines"; tale volume sarà pubblicato da ISACA allineato a COBIT® 4.1 con il titolo "IT Assurance Guide".

La struttura e le finalità rimarranno invariate, mentre i principali cambiamenti riguarderanno l'allineamento a COBIT® 4.1 per quanto riguarda il modello dei processi; inoltre, il dettaglio delle attività per il processo per la revisione dei sistemi informativi sarà rivisto al fine di descrivere con maggiore precisione le modalità di intervento per le fasi di Evaluation, Compliance Testing e Substantive Testing.

La terminologia sarà inoltre allineata con la terminologia invalsa in seguito alle novità regolamentari introdotte dalla normativa Sarbanes-Oxley ed alla conseguente emanazione di nuovi standard di revisione per l'audit delle società quotate negli Stati Uniti.

In particolare: la fase di Evaluation sarà denominata Test Of Design (TOD, consistente nella sostanza ad una valutazione del disegno dei controlli); la fase di Compliance Testing sarà denominata Test Of Effectiveness (TOE, o test dell'efficacia operativa dei controlli); la fase di Substantive Testing diventa "assessing the impact of control weaknesses", sulla scorta del fatto che la valutazione dei controlli inefficaci dovrebbe essere di norma supportata dalla esecuzione di opportuni test di sostanza.

Le nuove IT Assurance Guide conterranno inoltre linee guida per la revisione dei controlli automatici o semi-automatici (application controls), ed ulteriori linee guida sull'utilizzo di altre componenti di COBIT® – ulteriori rispetto agli obiettivi di controllo ed alle IT Assurance Guide – a supporto delle attività dell'IS Auditor.

8.5 Aggiornamento delle altre pubblicazioni della suite

E' previsto nella prima metà del 2007 l'allineamento a COBIT® 4 delle pubblicazioni "COBIT® Security Baseline" e "COBIT® Quickstart".

8.6 Aggiornamento dei sussidi all'implementazione

Il principale strumento di supporto all'implementazione di COBIT® è la pubblicazione "IT Governance Implementation Guide"; tale pubblicazione consiste di una raccolta di strumenti che includono piani di lavoro per l'implementazione dell'IT Governance utilizzando COBIT®, template, strumenti di diagnostica, casi di studio, mappature di COBIT® con COSO, ITIL®, BS17799, Frequently Asked Questions, esempi di IT Balanced Scorecard, linee guida per l'IT Risk Analysis, linee guida e strumenti per l'applicazione dei Maturity Model e altro ancora.

La versione allineata a COBIT® 4.1 includerà nuovo materiale proveniente anche da ValIT a copertura delle pratiche e dei modelli teorici per la creazione di valore con il supporto e/o mediante l'IT.

Infine, sarà allineato a COBIT® 4.1 anche "COBIT® Online", l'applicativo che ISACA ha reso disponibile con accesso internet per l'accesso e la personalizzazione dei contenuti della suite COBIT®, comprese le funzionalità di benchmarking del sistema di controllo interno e del livello di maturità dei processi.

In aggiunta al lavoro dei gruppi di ricerca dedicati a tali progetti specifici, continua nel tempo la raccolta dei contributi allo sviluppo di COBIT® costituito dalle osservazioni che gli utenti della suite in tutto il mondo inviano ad ISACA.

Sotto il profilo organizzativo, nel prossimo futuro le attività di ricerca concernenti COBIT® continueranno ad essere guidate dal COBIT® Steering Committee e supportate da alcuni centri di ricerca e da molteplici contributori coordinati dallo stesso Steering Committee.

Il COBIT® Steering Committee ha il compito di pianificare, coordinare e implementare lo sviluppo delle componenti della suite COBIT®, contribuendo anche alla raccolta dei fondi necessari. Il Committee si

compone di membri provenienti da Europa, Stati Uniti, Canada, Uruguay e nel suo complesso rappresenta esperienze provenienti da diverse industry unitamente a competenze di tipo accademico.

I gruppi di lavoro guidati dallo Steering Committee si compongono di volontari provenienti dai cinque continenti; complessivamente allo sviluppo di COBIT® partecipano centinaia di esperti il cui contributo, sia per le attività di sviluppo che per le attività di verifica della qualità, è rivisto e sistematizzato da gruppi di lavoro più ristretti.

L'attuale editore di COBIT®, ed il detentore dei diritti d'autore sul relativo materiale, è l'IT Governance Institute, filiazione di ISACA.

Un ulteriore aspetto notevole dell'evoluzione futura di COBIT®, non tanto nei contenuti, quanto rispetto alla diffusione prevista per tale standard, è rappresentato dall'adozione o dal riconoscimento di COBIT® come standard di riferimento per il controllo dell'IT da parte di organismi governativi o enti regolatori.

In particolare, COBIT® è stato adottato dalla Commissione Europea a Marzo 2005 come standard di riferimento per l'audit delle componenti IT dei sistemi di controllo interno delle Agenzie di Pagamento per gli interventi di politica agricola (come noto, la Politica Agricola Comune dell'UE assorbe circa il 50% del bilancio dell'Unione). Gli altri due standard sono ISO17799 e il Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch (IT Baseline Protection Manual).

Numerose altre istituzioni ed enti governativi hanno adottato COBIT® come standard di riferimento per il controllo ed il governo dell'IT, spesso come standard di riferimento per la stesura dei testi regolamentari di propria competenza.

Allo stato attuale, mentre non appare probabile che COBIT® diventi uno standard istituzionalizzato nell'ambito ISO, appare piuttosto possibile che altri organismi governativi in futuro facciano esplicito riferimento a COBIT® per le proprie esigenze regolamentari e di controllo nell'ambito della gestione dell'IT, probabilmente insieme ad altri standard di maggiore dettaglio tecnico per gli interventi concernenti i prodotti IT (come ad esempio i Common Criteria).

8.7 Il futuro di ITIL

L'evoluzione di estremo rilievo di ITIL® è costituita dal Progetto attualmente in corso denominato "Refresh Project" che produrrà una nuova versione di ITIL® (ITIL® v3) destinata a sostituire quelle attualmente in uso (v2).

La Versione 3 di ITIL® è parte del processo teso a perfezionare le "best practice" di ITIL®. Queste ultime infatti devono continuamente evolvere ed essere migliorate per essere in fase con le evoluzioni delle Aziende, che cambiano per aderire ai cambiamenti del mercato e dei loro Clienti. Quindi ITIL® v3 aiuterà i fornitori di Servizi a restare efficaci nel generare valore per i loro Clienti.

Tuttavia una parte significativa dei contenuti della Versione 2, sarà perfezionata ed inclusa in ITIL® v3.

Le informazioni che seguono sono basate:

- sulla storia del Progetto sin dal suo inizio;
- sui più recenti documenti resi disponibili dai Responsabili del Progetto e da OGC (Office for Government Commerce – UK), che ha la proprietà di ITIL® ed ha preso l'iniziativa di lanciare la nuova versione: questi ultimi documenti, insieme alle presentazioni più recenti sull'argomento, sono elencati in bibliografia.

Nel Novembre 2004 OGC ha lanciato un progetto per definire l'ambito e i piani generali di sviluppo di una versione aggiornata ("Refresh") di ITIL®; successivamente, nel primo trimestre 2005 OGC, con il supporto di varie Organizzazioni di Servizi, tra cui itSMF e la relativa Associazione Italiana, ha

effettuato una vasta consultazione a livello mondiale, per capire quali fossero le opinioni degli utenti di ITIL® e di tutta la comunità di operatori dei servizi sulle evoluzioni necessarie per ITIL®.

La risposta è stata entusiasta e sostanzialmente coerente rispetto alle linee consigliate e ciò ha fornito al Gruppo di Progetto, che aveva già cominciato a lavorare, input aggiuntivi molto preziosi.

Quindi il progetto è iniziato già da due anni - con l'attività di produzione cominciata ad Ottobre 2005 - e sta procedendo secondo i piani: il primo blocco importante della documentazione (denominato "Core Guidance -Tranche B)" sarà pubblicato a fine Maggio 2007 e sarà seguito dal grosso dei libri restanti nel corso del 2007.

Non ci sarà una sostituzione uno ad uno per ognuno degli attuali libri/CD: l'architettura dei volumi è diversa e anche se gli aspetti fondamentali resteranno, essi saranno distribuiti in modo diverso nei documenti. L'insieme delle pubblicazioni costituirà un set integrato.

Una differenza sensibile di impostazione è costituita dal fatto che nella nuova Versione sono state introdotte come elementi di riferimento le fasi del Ciclo di vita dei Servizi, invece dell'elenco e dei raggruppamenti dei Processi dell'attuale versione. Ciò sarà meglio illustrato in una Tabella riportata nel seguito di questo paragrafo.

Le parti componenti di ITIL® v3, che saranno pubblicate in sequenza di date successive, sono elencate di seguito:

➢ **Supporting Guidance – Tranche A** – Questa parte - che in parte ha cominciato ad essere pubblicata - è anche indicata come Web Offerings, poiché sarà disponibile sul Web in modo gratuito. Essa comprende:

- Mappe integrate dei Processi ITIL®: consisterà in un modello integrato per il nuovo ITIL®, che mostrerà anche i punti di interfacciamento possibile con le altre best practice esistenti sul mercato; tali mappe saranno pubblicate alla fine dello sviluppo di ITIL® Refresh;
- Glossario dei termini e delle definizioni standard: esso è già stato pubblicato, ma sarà aggiornato per corrispondere ai contenuti dei volumi "core" dopo il loro completamento;
- Introduzione di alto livello: sarà focalizzata sulla nuova struttura, sui Processi e sui contenuti, sulla proposta di Valore e sui benefici derivanti dall'adottare ITIL®;
- Cosa c'è di nuovo: informazione sulla nuova struttura, sui contenuti e le modifiche introdotti nella nuova versione di ITIL®; è indirizzata soprattutto agli operatori che siano già utenti di ITIL®.

➢ **Titoli della Core Guidance - Tranche B** – La pubblicazione di questa parte è attesa nel periodo Aprile - Maggio 2007, da confermare, e sarà composta da 5 volumi per un totale di circa 1000 pagine. Essa comprende:

- Service Strategy (SS)**:** è relativo ad una visione di ITIL® focalizzata all'allineamento tra business e IT che include la prospettiva e il valore della Gestione Servizi; sviluppa i concetti e la guida per Definizione dei Servizi, la Governance dei Servizi, i collegamenti tra i Piani e gli obiettivi del Business e le Strategie dei Servizi IT, Ruoli e Responsabilità, Misurazioni e Controllo, Critical Success Factor e Rischi; ogni libro successivo dell'insieme v3 collegherà i suoi argomenti base ai concetti del SS per soddisfare gli obiettivi di business, le esigenze e i principi della Gestione dei Servizi;

- Service Design (SD): fornisce la guida per la produzione e aggiornamento dei Processi IT, sulle politiche, le architetture e la documentazione per il progetto di servizi infrastrutturali corretti e innovativi atti a soddisfare le esigenze attuali e prevedibili del business. Include anche gli aspetti del Sourcing : Insourcing, Outsourcing e Co-sourcing;

- Service Transition (ST): fornisce la guida e le attività di Processo per la migrazione e attuazione dei Servizi nell'ambiente aziendale; sviluppa il ruolo del Change Management in senso ampio e a lungo termine e le pratiche di Release Management, considerando i rischi, i benefici e i meccanismi di erogazione; include gli aspetti di cambiamenti organizzativi e di mutamenti culturali e anche il Knowledge Management;

- Service Operation (SO): dedicato al Processo di erogazione e controllo; gli elementi di controllo dei Processi del Service Support e del Service Delivery dell'attuale v2 costituiscono una parte preponderante di questo volume, che include anche aspetti dell'Application Management e dell'Infrastructure Management;

- Continual Service Improvement (CSI): focalizzato sugli elementi di Processo coinvolti nella identificazione e nello sviluppo dei miglioramenti delle gestione Servizi.

➢ **Complementary products – Tranche C** (date di disponibilità da definire), che comprenderà Pocket Guides, Case studies, Moduli di lavoro delle pratiche ITIL® (es. SLM, …), Metodi di Governance, aiuti allo studio per le Certificazioni.

➢ **Executive Introduction to Service Management – Tranche D** (disponibilità prevista: entro l'estate del 2007). Questa pubblicazione è parte del Core dal punto di vista logico ma sarà sviluppata dopo il completamento dei 5 volumi base poiché riassumerà i concetti del nuovo ITIL® ed i benefici della sua adozione.

Nella tabella seguente viene riportata la Sintesi delle caratteristiche salienti di ITIL® v3 poste in relazione alle esigenze espresse dagli Utenti nella Consultazione del 2005.

Esigenze principali espresse dagli Utenti di ITIL	Come sono indirizzate nel Refresh Project
Struttura, stile scrittura e "navigazione" coerenti per tutti i libri/CD	Tutte le Pubblicazioni base avranno un'impostazione e una struttura di consultazione simile e in ogni volume ci saranno collegamenti con i principali criteri di guida.
Conservazione dei concetti chiave di Service Support e Service Delivery	Nella nuova Versione sono state introdotte le fasi del ciclo di vita Servizi invece della lista di Processi dell'attuale versione. I concetti base del Service Support e del Service Delivery attuali saranno incorporati nella Service Operation. Gli aspetti di Strategia e Pianificazione saranno trattati nei volumi Service Strategy e Service Design in cui si adattano meglio ad ogni fase della vita dei Servizi.
Definire il Ciclo di vita dei Servizi - dagli aspetti strategici a quelli operativi - come una struttura di gestione Servizi	Le fasi del Ciclo di vita sono: quella strategica (Service Strategies), quella tattica (Design e Introduction) e quella operativa (Service Operation). Il miglioramento dei Servizi si tradurrà in una guida di perfezionamento di tutte le fasi. Tutte le pratiche più importanti nei sette volumi di ITIL della versione attuale (v2) saranno incorporate nella nuova architettura.
Guida alla strutture organizzative ottimali per ITIL	Tutti i nuovi volumi principali includeranno la guida sui modelli di erogazione e sulle strutture organizzative per raggiungerli. Ciò perché la struttura organizzativa dà un forte contributo al raggiungimento delle best practice e

Esigenze principali espresse dagli Utenti di ITIL	Come sono indirizzate nel Refresh Project
	questo aspetto era stato trascurato nell v2.
Maggiore copertura degli aspetti dei cambiamenti culturali legati all'adozione di ITIL	Tutti i volumi base svilupperanno gli argomenti legati all'adozione, alle tecniche e ai benefici dei mutamenti culturali necessari per una soddisfacente realizzazione di ITIL.
Riferimenti alle altre best practice	E' utile riferirsi alle altre best practice quando si può supporre un beneficio nell'applicarle o nel capirle in relazione all'utilizzo di ITIL. Il volume del Service Design esaminerà le altre best practice o metodologie nella prospettiva dei benefici di allineamento con ITIL.
Interfacce e allineamento con gli altri framework	ITIL deve identificare le interfacce con CobiT, CMM, Six Sigma, eTom, ecc. Una mappatura formale dell'ITIL attuale (v2) e di CobiT v3 e sarà aggiornato per ITIL v3 e CobiT v4 e anche altri framework saranno mappati su ITIL.
Esempi di Business Case, Studi di Casi, Modulistica, Soluzioni per supportare le Organizzazioni nello sviluppo di uno o più Processi	Informazioni generali sui Business Case saranno contenute nelle Pubblicazioni Core. Esempi effettivi di Business Case, di Case Studies, di Moduli e di sviluppi significativi saranno forniti nell'ambito della Complementary Guidance
ITIL in ambienti "multisource" (Insourcing, Outsourcing, Co-sourcing)	Ogni volume Core (ad es. Service Strategies, Service Design, Service Transition) tratterà: le best practice e le linee guida per usare ITIL in ambienti multi-sourced, i fattori di decisione e strutture organizzative relativi al multi-sourcing, ecc.
Scalabilità	ITIL svilupperà questo argomento nelle guide Core, e inoltre pubblicherà un libro complementare su questo argomento: il libro "ITIL – small scale implementation" sarà aggiornato per riflettere le novità introdotte dal Refresh e costituirà un titolo complementare.
Mantenere l'approccio non prescrittivo	La struttura di ITIL Refresh nel Core contiene guide generiche e una suite complementare con argomenti più specifici e aree con guide ad hoc: cioè saranno prodotte guide complementari prescrittive dove giudicate necessarie.
Indicazioni di Prestazioni e informazioni sul Return on Investment (ROI) per i Processi, per valutare i benefici dei miglioramenti	Le pubblicazioni Core affronteranno argomenti come: Indicatori di prestazioni più precisi e di ROI riferiti ai Processi per facilitare l'accettazione da parte delle Direzioni aziendali.Produzione di Valore, Benchmark di prestazioni Servizi, efficienze di Costi, analisi di Prestazioni, pratiche di miglioramento.
Qualità della produzione delle pubblicazioni	ITIL v3 viene scritto in un modo coerente dai vari Autori che stanno producendo le pubblicazioni nello stesso periodo e sotto un controllo che verifica anche la coerenza dello stile espositivo.
Terminologia e definizioni standard	La prima pubblicazione delRefresh Project è stata il rifacimento del Glossary precedente, che è un insieme di termini e definizioni standard ITIL. Esso sarà anche seguito dagli Autori dei vari volumi per ottenere una completa omogeneità di linguaggio.
Indirizzare la Governance IT	In ognuna delle pubblicazioni Core in cui le pratiche ITIL devono considerare aspetti e argomenti di Governance questi verranno discussi e dove necessario i lettori saranno indirizzati a metodi formalizzati di Governance esterni ad ITIL.
Informazioni per le Direzioni aziendali e Marketing	Una visione di insieme sintetica di ITIL con i suoi benefici per l'Azienda e per l'IT che sia di interesse per la dirigenza, è stata ritenuta molto importante per facilitare la comprensione del modello e per favorirne l'adozione. Una pubblicazione di tipo strategico orientata al business farà parte del nucleo base di ITIL.
Guida alla valutazione degli strumenti di supporto	Questo argomento sarà sviluppato in modo parziale: ITIL come insieme di pratiche indipendente dai Fornitori, non può scendere nella valutazione degli strumenti ad es. confrontando le funzionalità dei vari prodotti commerciali. Tuttavia identificherà opportunità di automatizzare le attività dei Processi e criteri di guida su quali funzionalità gli Utenti dovrebbero esigere per soddisfare tali opportunità.

Esigenze principali espresse dagli Utenti di ITIL	Come sono indirizzate nel Refresh Project
Metriche per le prestazioni chiave	Ognuna delle pubblicazioni del nucleo base conterrà metriche di misura della prestazioni (KPI) con esempi del loro significato e della loro applicazione.
Miglioramento dell'auto valutazione	La Survey di auto valutazione verrà aggiornata come parte della Complementary Guidance una volta che le Core publications saranno state completate.
Modello di Processi integrato	E' stato prodotto un modello di alto livello per documentare le pratiche correnti di ITIL: esso servirà da punto di partenza per gli Autori di ITIL v3 per i loro sviluppi e sarà successivamente aggiornato.
Elementi di successo e benefici immediati di ogni Processo	La nuova Versione indicherà esempi di benefici immediatamente percepibili (quick wins)

Nella seguente Figura 2 si riporta la struttura fondamentale di ITIL® v3.

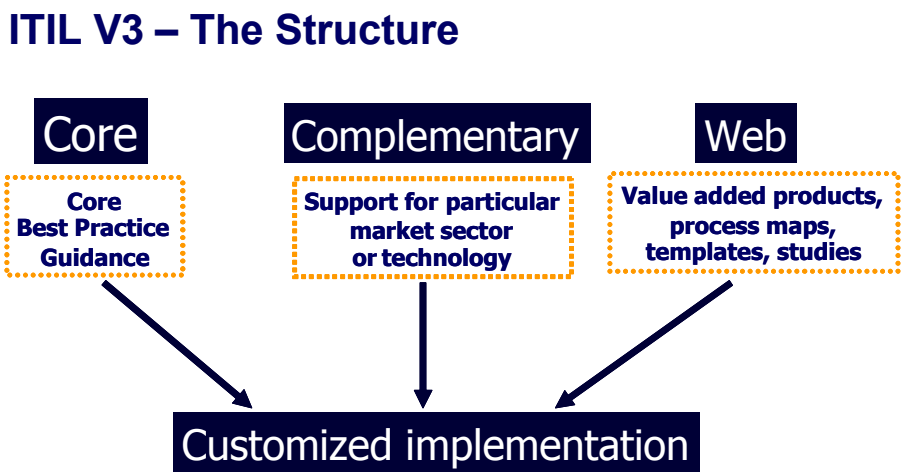

Figura 2 - Macro-componenti di ITIL v3

Nella Figura 3 a pagina seguente si riporta uno schema di insieme di ITIL® v3 (tratto dalla Presentazione di Sharon Taylor a Birmingham il 30/11/06); al centro sono evidenziati i Processi Core (Service Strategies, Service Design, Service Transition, Service Operation, Continual Service Improvement) e ai due lati sono messi in evidenza i framework e gli Standard con cui ITIL® v3 comunicherà o che sono stati comunque esaminati nel corso del suo progetto.

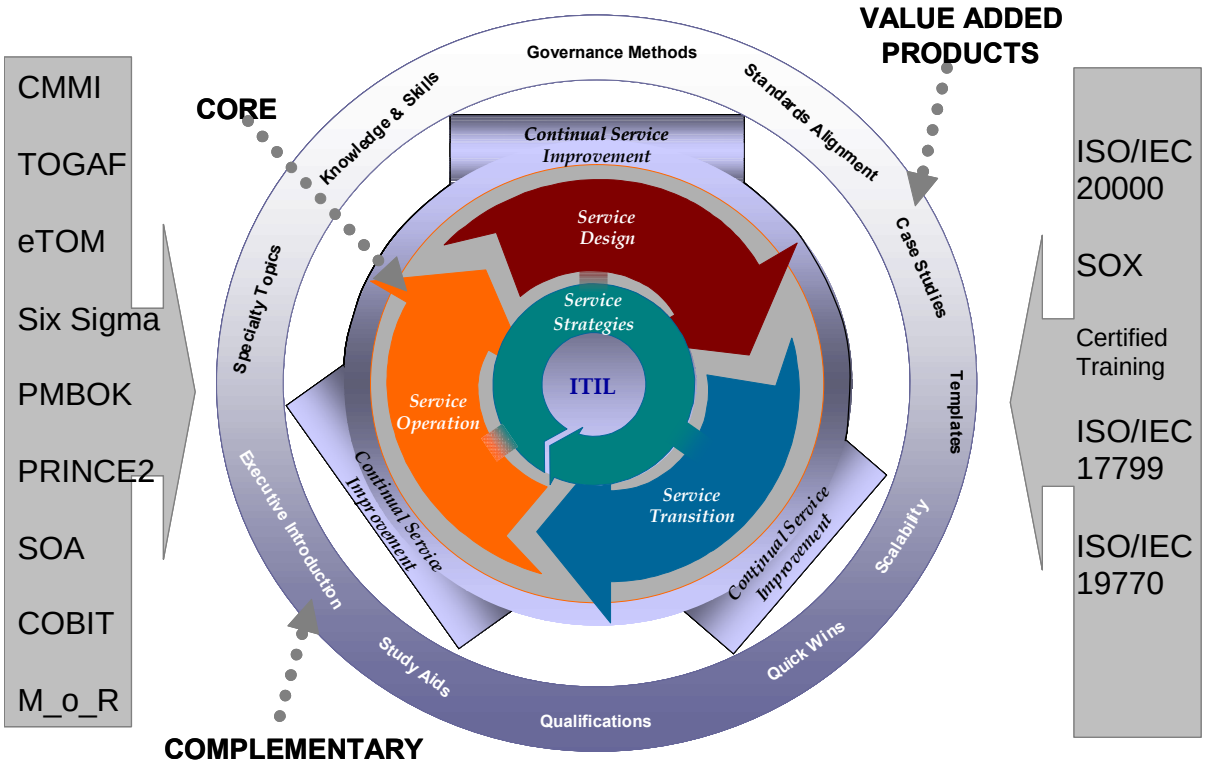

Figura 3 – Schema di insieme di ITIL v3

8.8 Ricadute sulle considerazioni espresse (utilizzo congiunto di Cobit e ITIL)

Dall'esame delle evoluzioni previste per COBIT® ed ITIL® emerge che i contenuti dei due standard appaiono per alcuni aspetti convergere, in particolare in relazione ai criteri ed alle logiche di riferimento e nello specifico, ad esempio, in relazione ai temi dell'IT Governance.

Proprio sotto il profilo della convergenza dei riferimenti, appare significativo notare che COBIT® ed ITIL® si citano vicendevolmente fra le fonti a cui ciascuno dei due standard si richiama.

Il convergere nei principi dei due principali standard di riferimento nel mondo per la definizione dell'organizzazione e dei processi dell'IT conferma che il corpo di conoscenza concernente il governo e la gestione dell'IT sta raggiungendo un importante livello di maturità e consolidamento.

E' possibile infatti oggi riconoscere un certo insieme di buone pratiche di governo per l'IT, che richiedono la definizione di specifici aspetti, fra i quali, ad esempio:

⇒ Organizzazione dell'IT;

⇒ Processi dell'IT, inclusi ad esempio:

- processi per la produzione dei servizi (Service Delivery);
- processi per il supporto degli utenti (Service Support);
- processi specifici per la gestione del software (software development and maintenance lifecycle);

⇒ Sistemi nell'ambito delle organizzazioni IT, inclusi ad esempio:

- sistema per la gestione dei progetti;
- sistema per la gestione della qualità;
- sistema per la gestione della sicurezza;
- sistema di controllo interno.

E' generalmente riconosciuta l'opportunità, in organizzazioni moderne, di definire tali elementi e sistemi[12] sulla base di buone pratiche definite dal mercato e descritte nella letteratura e negli standard dedicati[13].

L'evoluzione vista per COBIT® e ITIL® consente di ritenere che essi continueranno nel prossimo futuro ad essere gli standard di riferimento per la definizione e la valutazione delle organizzazioni IT.

Con riferimento all'utilizzo congiunto dei due standard, a supporto delle attività di definizione di organizzazioni, processi e sistemi nell'ambito IT, da entrambi gli standard potranno essere acquisite indicazioni ed elementi di conoscenza che ciascuna organizzazione potrà adattare alle proprie esigenze.

Rispetto all'utilizzo di uno o dell'altro fra COBIT® ed ITIL®, è necessario rilevare che, in continuità con la propria tradizione, e anche nelle loro nuove versioni, i contenuti di COBIT® continuano ad apparire più direttamente utilizzabili per il disegno e la valutazione dei sistemi di governo e controllo interno sull'IT, mentre i contenuti di ITIL® continuano ad apparire più direttamente utilizzabili per il disegno dell'organizzazione e dei processi di gestione dell'IT.

In ragione pertanto del permanere di tale specializzazione dei contenuti – pur in presenza di una certa convergenza dei due standard come sopra ricordato – appare possibile concludere suggerendo l'opportunità che i soggetti responsabili della progettazione e gestione delle organizzazioni IT – manager, consulenti, analisti organizzativi e di processo per l'IT, responsabili della qualità e della sicurezza nelle stesse organizzazioni, etc. – conoscano e sappiano applicare opportunamente nei diversi contesti entrambi gli standard[14].

[12] E' importante notare che tali componenti organizzative non sono isolate o isolabili; vi sono infatti sovrapposizione e relazioni che rendono necessario intervenire su ciascuna componente considerando contestualmente gli impatti che la definizione o la modifica di ogni componente ha sulle altre.

[13] Unitamente ad altre componenti organizzative tradizionalmente riconoscibili in generiche organizzazioni – quale ad esempio il sistema dei poteri e delle deleghe.

[14] Vale la pena sottolinare, per completezza, che il bagaglio degli standard di riferimento per l'analista organizzativo e di processo per l'IT dovrebbe includere, oltre a CobiT ed ITIL, anche altri standard analogamente importanti e specializzati, quali ad esempio ISO17799 per i sistemi di gestione della sicurezza.

9 BIBLIOGRAFIA E FONTI

www.nist.gov

www.opengroup.org

www.opengroup.org/architecture/

www.opengroup.org/architecture/togaf8-doc/arch

www.zifa.com

www.isixsigma.com

www.coso.org

www.balancedscorecard.org

www.bscol.com

www.isaca.org

www.itgi.org

"A Framework for Information Systems Architecture."
John A. Zachman.
IBM Systems Journal, vol. 26, no. 3, 1987. IBM Publication G321-5298.

"Extending and Formalizing the Framework for Information Systems Architecture."
J.F. Sowa and J.
IBM Systems Journal, vol. 31, no. 3, 1992. IBM Publication.

"Enterprise Architecture: The Issue of the Century"
John A. Zachman
Database Programming and Design, Marzo 1997
Miller Freeman, Publisher.

“Six Sigma : SPC and TQM in Manufacturing and Services”
Geoff Tennant
Ashgate Publishing, Gennaio 2001

“Overview of International IT Guidance”
2ndEdition, IT Governance Institute.

“Verso un nuovo managment dell ICT: dalla gestione alla governance dei sistemi informativi”

Severino Meregalli

“Net Economy: tecnologie e nuovi paradigmi manageriali”

In Biffi, A. (a cura di)

Franco Angeli. 2001.

“Information System Governance” in “Management - Innovazione e Tecnologie Informatiche ”

Severino Meregalli, a cura di Ferdinando Pennarola

EGEA, 2006.

“Introduzione a ITIL”

Autori Vari

OGC

“Service Support”

OGC

“Service Delivery”

OGC

COBIT 4.0 - Control Objectives, Management Guidelines, Maturity Models

ITGI – IT Governance Institute - 2005

COBIT 4.0 - Control Objectives, Management Guidelines, Maturity Models

Traduzione italiana a cura della Associazione Italiana Information Systems Auditors

AIEA Capitolo di Milano di ISACA - 2006

“COBIT 4.0 in support of IT Governance, Management and Assurance” - Presentazione al “XX Convegno Nazionale di Information Systems Auditing” – Verona, maggio 2006 – (cfr. www.aiea.it)

Erik Guldentops

“Operations Management Capabilities Model”
Sun BluePrints On Line, Febbraio 2005

“ITIL Refresh: Scope and development Plan”

OGC, 26 Giugno 2006

Successivi documenti di aggiornamento apparsi sui siti web OGC e itSMF UK, tra cui

“ITIL Version 3 Answers straight from the source” del 24/8/2006

“ITIL v3 – The Final Countdown” - Presentazione nella Conferenza di itSMF UK a Birmingham il 13 Novembre 2006

Sharon Taylor

“ITIL v3 Refresh - ITIL Future” - Presentazione nella Conferenza annuale di itSMF Italia a Milano il 30 Novembre 2006.

Mr. David Wheeldon