Nel contesto attuale, in cui tutte le aziende sono concentrate sull'efficienza, sul controllo dei costi e sulla redditività delle iniziative, l'It governance ha il compito di garantire livelli di servizio certi e di massimizzare il valore aziendale degli investimenti It.

Per non naufragare nel caos dell'informatica

di Giancarlo Magnaghi

All'inizio degli anni '90 le organizzazioni di tutto il mondo hanno investito in maniera sempre più estesa e consistente in Information & Communication Technology (Ict) al fine di armonizzare le attività dei sistemi informativi con gli obiettivi di business, recuperare competitività e sperimentare nuovi applicazioni e tecnologie.

Negli ultimi anni '90, l'accavallarsi dei grandi progetti relativi agli adeguamenti dei programmi all'anno 2000 e all'euro e all'introduzione dei sistemi Erp e delle tecnologie Internet hanno dato un notevole impulso alla spesa It. Poi, in seguito allo "sboom" della new economy alla fine del 2001, è iniziato un periodo di "austerity", in cui l'imperativo è diventato "fare di più con meno", con maggiori controlli e adempimenti richiesti da nuove leggi come il Codice sulla Privacy, la regolamentazione "Basilea 2" sulla gestione del credito bancario e la legge Usa Sarbanes-Oxley sulla trasparenza amministrativa.

Il responsabile dei sistemi informativi non è più un semplice esperto di informatica (Edp manager), ma diventa un manager di prima linea (Cio - Chief Information Officer), spesso parte del consiglio di direzione, che deve essere in grado di gestire una complessa *business unit* di importanza strategica: un insieme di componenti organizzative e di strumenti tecnologici capaci di governare le tecnologie, mantenendole allineate e coerenti con le esigenze aziendali. Al Cio si richiede di migliorare il Roi e incrementare i livelli di servizio e di sicurezza, mantenendo costante il budget e il numero di collaboratori. Però non deve avere come obiettivo solo il contenimento dei costi, ma soprattutto la capacità dell'azienda di concentrarsi sul core business e aumentare l'agilità nel rispondere al mercato. Deve fungere da cerniera fra le esigenze delle funzioni aziendali e i fornitori di prodotti e servizi, e deve avere la capacità di definire e di governare costi e livelli di servizio (Sla) sulla base di parametri (Kpi) che non si limitano agli aspetti tecnologici ma includono anche indicatori legati agli obiettivi di business. Per far fronte a tutte queste richieste, soprattutto nelle organizzazioni medio-grandi si è affermata la necessità di una gestione più strutturata dell'Information Technology, ed è nata così una nuova specializzazione della scienza del management: l'It Governance.

It Governance

L' It governance è l'insieme di regole, processi, procedure, strutture organizzative e misure di controllo che supportano tutte le attività della funzione It, come gestione di fornitori in outsourcing, skill management, change management, gestione dei problemi, gestione dei progetti, gestione dei livelli di servizio, gestione della sicurezza e della qualità.

Nel contesto attuale, in cui tutte le aziende sono concentrate sull'efficienza, sul controllo dei costi e sulla redditività delle iniziative, l'It governance ha il compito di garantire livelli di servizio

certi e di massimizzare il valore aziendale degli investimenti It. La maggior parte delle organizzazioni It incontra tuttavia difficoltà a mettere in atto questo mandato, poiché non dispone dei processi e dei sistemi necessari per valutare accuratamente valore, costi, rischi e prestazioni dei servizi che fornisce. Si stanno quindi diffondendo strumenti e metodi per supportare questa nuova forma di management.

Standard e Framework

A partire dagli anni 70, si sono sviluppate molte metodologie a supporto dell'It, in particolare nel campo dello sviluppo delle applicazioni e del project management, ma solo a partire dagli anni 90 sono nati modelli (*framework*) orientati al management, con vari orientamenti e obiettivi: dai metodi per misurare la maturità dei processi aziendali, come Cmm (Capability Maturity Model), alle dettagliate guide alla gestione dei servizi, come Itil, ai modelli di It governance ad alto livello, come Cobit.

Il primo modello per l'It governance a livello mondiale, Cobit (*Control Objectives for Information and Related Technology*), nacque all'inizio degli anni 90 per allineare le risorse e i processi It con gli obiettivi di business, gli standard qualitativi, i controlli delle spese e la sicurezza ed è stato affiancato nel corso degli anni da altri framework, come Itil e Iso17799. A questi si aggiungono i framework per la qualità come Iso 9000 per i processi delle imprese, Six Sigma per la produzione e il Capability Maturity Model (Cmm) per lo sviluppo software.

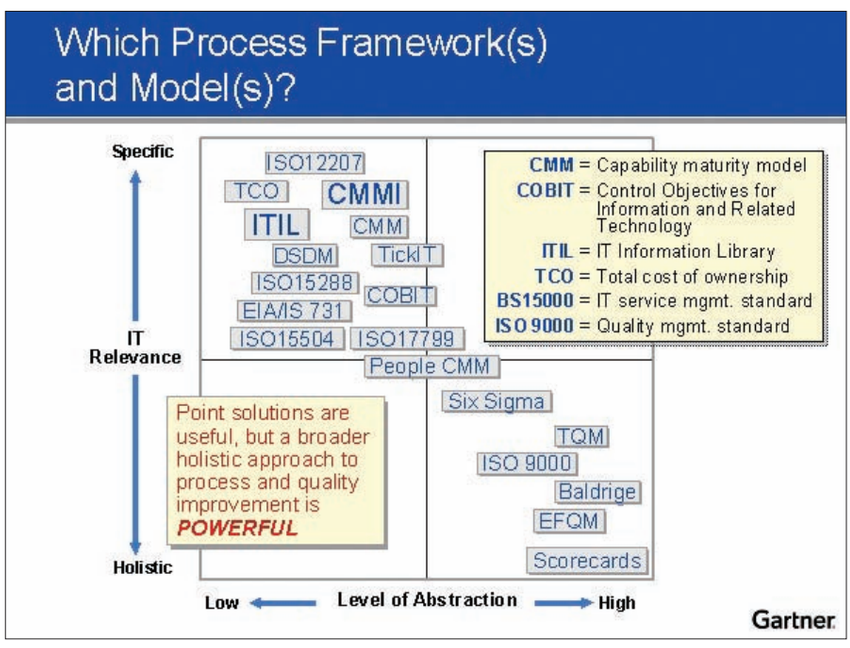
Poiché non esiste un'unica metodologia in grado di supportare tutti gli aspetti dell'It Governance, ognuno di questi framework può offrire qualche beneficio alle organizzazioni poiché copre alcuni aspetti della governance. Per esempio, Iso17799 è principalmente focalizzato sulla sicurezza, mentre Itil offre un supporto alle decisioni relative all'esercizio dei sistemi e alle gestione dei servizi. Cobit è stato progettato come un "ombrello" a più alto livello e può lavorare bene insieme agli altri framework più settoriali. Sono poi in corso vari progetti di armonizzazione, come quello sponsorizzato da governo britannico e It Governance Institute per integrare Cobit e Itil.

Tipicamente le grandi organizzazioni utilizzano più di un framework contemporaneamente. Per esempio le principali corporation dell'informatica, come Hewlett Packard, Sun Microsystems, Microsoft, Computer Associates utilizzano Itil e altri framework, Ibm utilizza Iso 9000, Cmm, Itil e Six Sigma insieme a programmi di qualità proprietari.

Le aziende non dovrebbero adottare questi framework "a scatola chiusa", ma utilizzare solo le parti di ognuno che si adattano meglio al proprio modo di lavorare. Bisogna comunque evitare di spendere risorse sproporzionate per i programmi di certificazione, e di causare appesantimenti dei processi e diminuzione dell'efficienza, come suggeriscono gli esperti di alcune tra le maggiori società di consulenza che abbiamo intervistato.

Cmmi (Capability Maturity Model Integration)

Il primo Capability Maturitity Model (Cmm) fu definito nel 1991 dal Software Engineering Institute (Sei) dell'università Carnegie Mellon di Pittsburg per conto del Dod (Dipartimento della Difesa Usa) come modello di valutazione e miglioramento della maturità (maturity) del processo di sviluppo del software. In seguito nacquero diverse varianti per altre discipline come l'ingegneria dei sistemi, la gestione del personale e lo sviluppo di prodotti integrati, arrivando a una situazione eterogenea e confusa. Nel 2000, fu creato il **Capability Maturity Model Integration** (Cmmi) per riprendere il controllo della situazione, rivisitare i vari modelli di valutazione dell'efficacia del processo (maturity model) nati come funghi, e, facendo tesoro dell'esperienza accumulata in un decennio di utilizzo, creare un framework predisposto per integrare futuri modelli e costruire un primo nucleo di Cmm integrati.



Il Cmmi descrive un modello evolutivo da un processo immaturo a uno disciplinato e maturo, attraverso il miglioramento di qualità e di efficienza. Consiste di un insieme di best practice, focalizzate a migliorare i processi aziendali per l'acquisizione, lo sviluppo, l'integrazione e la manutenzione di prodotti e servizi.

Il **Maturity Level** misura l'efficacia del processo organizzativo e l'estensione e precisione con cui le fasi e le attività sono definite, gestite, misurate e controllate.

Rappresenta una valutazione del livello di padronanza e controllo del processo da parte dell'organizzazione, inclusa la capacità di migliorarlo, ottimizzarlo o modificarlo. Sono definiti 5 livelli di maturità.

Livello 1 (Iniziale) - rappresenta un processo con risultati non prevedibili. Il processo di produzione è instabile e disorganizzato e definito implicitamente da chi lo realizza.

Livello 2 (Ripetibile) - il processo è caratterizzato da performance di progetto ripetibili; è pianificato, realizzato, monitorato e controllato rispetto a obiettivi di business predefiniti;

Livello 3 (Definito) - rappresenta un processo fondato su metodologie e tecnologie ben definite, sia per gli aspetti gestionali che per gli aspetti operativi;

Livello 4 (Gestito) - il processo viene controllato usando tecniche quantitative e statistiche. Gli obiettivi di business dell'organizzazione sono controllati in termini statistici;

Livello 5 (Ottimizzato) - Esiste una politica di gestione della qualità con l'uso di metodi quantitativi, per il miglioramento del processo stesso, anche attraverso l'introduzione controllata di nuove metodologie e tecnologie.

Itil

Mentre il Cmmi è lo standard di qualità di fatto per i processi di sviluppo software, It Infrastructure Library (Itil) è lo strumento più usato per l'esercizio e la gestione dell'infrastruttura It, e in particolare per i servizi It come help desk, supporto alle applicazioni e software distribution. Si sovrappone a Cmmi in alcune aree come il configuration management.

Itil nasce da un'iniziativa del governo inglese per creare uno standard per l'implementazione, la gestione e il controllo dei processi It; è gestito e mantenuto dall'Office of Government Commerce (OGC) che appartiene alla pubblica amministrazione inglese e viene sponsorizzato dall'It Service Management Forum (itSMF), un'organizzazione composta a sua volta da varie organizzazioni nazionali, tra cui una di recente costituzione in Italia, che ha l'obiettivo di sponsorizzare e implementare Itil a livello internazionale.

Itil definisce la struttura organizzativa e gli skill necessari per l'area It e documenta una serie di procedure operative (best practice) che forniscono chiare linee guida su come gestire un'organizzazione It e la relativa infrastruttura, come fornire, gestire i servizi It e come controllarne la qualità.

Il framework Itil è composto da sette volumi: Service Support; Service Delivery; Planning to Implement Service Management, Applications Management, ICT Infrastructure Management; Security Management, The Business Perspective. Le parti utilizzate più comunemente sono le prime due: Service Support e Service Delivery.

Itil è attualmente utilizzato per la gestione di organizzazioni It medio grandi, che erogano servizi alla pubblica amministrazione e a diversi settori industriali, dove chi usufruisce dei servizi può essere il cliente finale o l'utente interno.

Itil è molto diffuso in Europa ma sta guadagnando popolarità anche in Nord America.

I principali sistemi di Help Desk, come Remedy, Vantive e Siebel (ora Oracle), supportano le best practice Itil.

Iso/IEC 20000

È il nuovo standard internazionale per la gestione dei servizi It (It Service management), più specifico rispetto a UNI EN Iso 9001:2000. Descrive un set integrato di processi per rendere maggiormente efficace ed efficiente l'erogazione dei servizi che l'It mette a disposizione dei clienti esterni e degli utenti interni. È allineato con l'approccio descritto nell'It Infrastructure Library (Itil).

Iso 20000 è basato sullo standard inglese BS15000, il primo standard che indirizza specificamente le tematiche di It Service Management, pubblicato da BSI (British Standard Institute) nel 2000.

Lo standard BS 15000 è formato da due parti:

- **BS 15000-1** definisce i requisiti a cui si deve conformare un'organizzazione per fornire livelli di servizio di qualità accettabile ai propri clienti
- **BS 15000-2** descrive le *best practice* per i processi di *Service Management*.

La procedura per la trasformazione dello standard BS 15000 in Standard Iso è iniziata nel novembre 2004 ed è stato accettato come standard internazionale Iso 20000 nell'aprile 2005.

Cobit ("Control Objectives for Information and related Technology")

Giunto alla terza edizione dopo oltre dieci anni di utilizzo sul campo, Cobit è un framework sviluppato dalla Informa-

I PRINCIPALI FRAMEWORK PER L'IT GOVERNANCE

Acronimo	Cmmi	Itil	Cobit
Nome completo	Capability Maturity Model Integration	It Infrastructure Library	Control Objectives for Information and related Technology
Sponsor	Software Engineering Institute - Carnegie Mellon University (SEI - www.sei.cmu.edu)	U.K. Office of Government Commerce (OGC - www.ogc.gov.uk), It Service Management Forum (itSMF – www.itsmf.com, www.itsmf.it)	Information Systems Audit and Control Association (ISACA – www.isaca.org) e It Governance Institute (ITGI - www.itgi.org).
Descrizione	Collezione di best practice per lo sviluppo e la manutenzione del software. Classiffica la maturità dei processi in cinque livelli: initial, managed, defined, predictable e optimizing.	*Best practice* per la gestione e le operation del service It, divise in sette volumi (Book): service-desk, incident, change, capacity, service-level e security management. Grande diffusione soprattutto in Europa.	Insieme di linee guida pratiche e controlli orientata all'audit dei processi It con particolare riguardo a riduzione dei rischi, integrità, e sicurezza. Copre quattro *domini*: planning & organization, acquisition & implementation, delivery & support, monitoring. Prevede sei *maturity level*, simili a quelli del Cmm.
Punti di forza	Molto dettagliato e concepito per le organizzazioni che sviluppano software. È focalizzato sul continuo miglioramento. Può essere utilizzato per un'autovalutazione.	Framework molto stabile, maturo, dettagliato e focalizzato sulla gestione e l'operatività degli ambienti It. In combinazione con Cmmi può coprire tutto il ciclo di vita dei prodotti It.	Buone checklist per l'It. Permette di analizzare rischi non considerati esplicitamente dagli altri framework. Può funzionare bene con altri framework come Itil.
Limitazioni	Non copre aspetti operativi dell'It come sicurezza, change management, capacity planning, troubleshooting e help desk. Stabilisce gli obiettivi, ma non dice come raggiungerli.	Non definisce il sistema di controllo di qualità, pur essendo compatibile con i principi di Iso 9001. Non copre il processo di sviluppo del software.	Dice cosa bisogna fare ma non come farlo. Non entra nel merito dello sviluppo software e dei servizi software o It. Non fornisce una road map per migliorare i processi.

tion Systems Audit and Control Association (Isaca) e dall'It Governance Institute (Itgi) per aiutare le organizzazioni a gestire i rischi It e ad assicurare che i processi It siano coerenti con le necessità di business.

La missione di Cobit è ricercare, sviluppare e rendere pubblico un set internazionale di obiettivi di controllo generalmente accettati e che possano essere utilizzati non solo dai tecnici ma anche dai manager e dagli auditor.

Cobit è particolarmente interessante per i manager poiché affronta la gestione del completo ciclo di vita dell'It visto dalla prospettiva del Cio: pianificazione e organizzazione, acquisizione e implementazione, delivery e supporto e definisce i processi necessari per eseguire con successo ogni funzione.

Il framework Cobit identifica 34 processi principali di Information Technology, raggruppati in quattro domini e supportati da 318 obiettivi di controllo dettagliati. Ciascuno dei 34 processi individua le risorse It coinvolte e i requisiti di qualità, fiducia e di sicurezza richiesti.

Le linee guida di Cobit sono generiche e orientate ai processi e hanno lo scopo di indirizzare le seguenti necessità del management che si occupa di controlli: misurazione delle performance (quali sono i migliori indicatori di performance?), definizione dei controlli (cosa è veramente importante controllare?), consapevolezza (quali sono i rischi che potrebbero impedirci di raggiungere i nostri obiettivi?), benchmarking (cosa fanno gli altri?).

Per ciascuno dei 34 processi Cobit, è previsto di adottare una scala di misura con un punteggio che varia fra 0 e 5, associata con un modello di maturità ispirato al Cmmi.

Cobit non è direttamente una metodologia poiché dice cosa bisogna fare ma non come farlo; non entra nel merito dello sviluppo software e dei servizi software o It e non fornisce una road map per migliorare i processi. È quindi un framework ad alto livello che deve essere complementato da modelli operativi specifici.

Fine Prima parte, La seconda parte del servizio sull'It Governance verrà pubblicata sul numero di gennaio e conterrà interviste a Simon Gay Vice president Gartner, a Roberto Rizzardo, Senior Manager Strategy & Operations-Deloitte e a Marco Ometto, Senior Executive di Accenture