CMMI, ITIL, TOGAF…OGNI UFFICIO IT ADOTTA LA SUA BEST PRACTICE! Ma… se i giocatori seguono schemi diversi, difficilmente si va a canestro!

A cura di Francesco Csciati, Manager di HSPI

Introduzione

«*Da quando in azienda abbiamo adottato COBIT è aumentato il lavoro e sono peggiorate le performance!*» «*Adesso, oltre a tutto il lavoro che normalmente svolgo, devo anche compilare tutti questi documenti*» «*Perdo più tempo a compilare il ticket, che a risolvere il problema*» etc.

Sostituite **COBIT** con **ITIL**, **PMBoK**, **TOGAF** o qualsiasi altra best practice e le frasi che vi capiterà di ascoltare saranno sempre, o quasi, le stesse.
Quindi verrebbe da chiedersi – *ma è veramente vantaggioso definire un modello di processi e strutturare il lavoro di conseguenza?* – In un contesto come quello in cui le aziende si muovono, dove chi si occupa di ICT deve da un lato allinearsi con rapidità ai mutevoli fabbisogni aziendali, e dall'altro garantire stabilità e performance soddisfacenti, è assolutamente necessario dotarsi di un modello di funzionamento atto a presidiare con metodi e strumenti strutturati l'intero assetto tecnico-organizzativo dei Sistemi Informativi.
L'errore da evitare, semmai, è quello di avere un approccio troppo rigido all'implementazione che si traduca in una eccessiva "**burocratizzazione**" delle modalità operative.
Utilizzo una best practice per definire il mio modello di funzionamento o sviluppo un mio modello?
È sicuramente consigliabile adottare una best practice come vedremo nel corso dell'articolo.
Ma tra i diversi framework presenti sul mercato, quale scelgo? Dipende dagli obiettivi che si vogliono raggiungere.

Questo articolo, dopo un breve excursus sulle principali best practice per il governo e la gestione dei Sistemi Informativi, evidenzia come sia determinante, per il successo di iniziative di definizione di un framework integrato di IT Governance e IT Management, scegliere (**ADOPT**) la/le best practice che meglio soddisfa/soddisfano gli obiettivi che si vogliono raggiungere e compiere uno sforzo per "adattarla/le" (**ADAPT**) alle proprie esigenze. In particolare analizza come una Funzione ICT possa costruire il proprio modello di funzionamento, adottando il COBIT 5 come framework di riferimento, per affrontare in modo olistico le diverse tematiche e garantire il governo dei Sistemi Informativi (**IT Governance**), integrandolo poi con le diverse prassi di Demand Management, Project Management, Enterprise Risk Management, Service Management, etc., per specializzare i processi da implementare e garantire la corretta gestione delle attività da realizzare (**IT Management**).

Le principali Best Practice ed i principali Standard per il governo e la gestione dei SI

Negli ultimi anni abbiamo assistito alla proliferazione di numerose best practice per il governo e la gestione dei sistemi informativi e sempre più spesso le aziende ne prevedono l'adozione. Esistono diverse Best Practice che possiamo raggruppare per aree di focalizzazione:

- **Governance and Quality Assurance**: racchiude tutti quei framework orientati alla Governance complessiva, al controllo e all'audit dei Sistemi informativi, che forniscono linee guida per garantire la qualità e l'efficienza dei processi IT e il rispetto di standard, politiche di qualità e requisiti di legge stabiliti, come il **COBIT** ed il **CGEIT** di **ISACA®**, lo standard **ISO/IEC 38500**, l'**IC-IF del CoSO**, il **Six Sigma** di Motorola.
- **Demand**, **Planning & Control**: racchiude tutti quei framework orientati alla gestione della domanda e al controllo dei costi IT, che forniscono linee guida per sviluppare la relazione con i clienti, per

la raccolta dei fabbisogni e la promozione della domanda verso nuovi servizi, e per definire il piano strategico e il budget dell'IT e monitorarne gli scostamenti. Alcuni esempi sono il **BABoK** dell'IIBA per la Business Analysis, l'**IREB** per la raccolta dei requisiti, il **Portfolio Management Standard** sviluppato dal PMI per la gestione della domanda e del Portfolio progetti e investimenti.

- **Enterprise Architecture**: racchiude quei framework che forniscono metodi e strumenti per favorire l'accettazione, la produzione, l'uso e il mantenimento di una "Enterprise Architecture", come il **TOGAF** dell'Open Group, lo **Zachman Framework** e il **DoDAF** del Dipartimento della Difesa USA.
- **Information Security Management**: racchiude quei framework orientati alla gestione della sicurezza dei sistemi informativi mediante la definizione di un insieme di misure di carattere organizzativo, procedurale e tecnologico necessarie a preservare la sicurezza logica delle informazioni e la continuità operativa dei sistemi IT di produzione, come **ERM del CoSO**, la **serie 800** delle pubblicazioni del **NIST**, le **ISO/IEC 27001**, **27005** e **27031**.
- **Project Management e Development**: racchiude quei framework orientati alla progettazione e sviluppo dei servizi, che forniscono linee guida sulla gestione dei progetti, sullo sviluppo e sulla gestione dei test e dei passaggi in produzione, come il **PMBoK** del PMI e il **Prince2** dell'OGC[1] per la gestione dei progetti, il **CMMI-DEV** della Carnegie Mellon University, **Unified Process** (UP), lo **SCRUM** e il **DevOps** per lo sviluppo software, e l'**ISTQB** per la gestione dei test.
- **Service Management**: racchiude quei framework incentrati sulla gestione dei servizi, che forniscono linee guida per la definizione, realizzazione, passaggio in produzione ed erogazione dei servizi IT, come **ITIL v3** dell'OCG e lo standard **ISO/IEC 20000**.
- **IT Outsourcing**: racchiude quei framework incentrati sul controllo e il governo dei fornitori, che forniscono linee guida per gestirli lungo tutto il ciclo di vita del contratto, dall'analisi di fattibilità, alla progettazione e implementazione dei servizi, per monitorare le prestazioni dei fornitori rispetto alle condizioni previste nei contratti e per identificare, analizzare e mitigare i rischi di fornitura applicando le necessarie azioni correttive. Per citarne alcuni: **eSCM** della Carnegie Mellon University, o l'**OPBoK** della IAOP.
- **Skill & Competence Management**: racchiude quei framework incentrati sulle competenze necessarie in ambito IT, che forniscono indicazioni per censire e valorizzare le competenze delle risorse e definiscono in modo chiaro, coerente e univoco le competenze necessarie all'interno di una Funzione ICT, come **SFIA v5.0** e e-**CF v3.0**.

Esistono, inoltre, degli **standard verticali per industry**, ovvero pubblicazioni che contengono informazioni sulle "buone prassi" relative a specifici settori di business, tipologie di organizzazioni, modelli operativi e/o architetture tecnologiche, come ad esempio **eTOM**, sviluppato dal TM Forum, che descrive i processi di business per il settore delle Telecomunicazioni.
Ecco le ragioni per cui gli standard e le best practice elencate offrono **numerosi benefici**:

- sono da tempo adottate in realtà fra loro eterogenee che ne validano l'efficacia e le sottopongono ad un continuo aggiornamento;
- prevedono percorsi formativi e di certificazione;
- possono essere adottate sia dalle aziende clienti che dai fornitori di servizi, consentendo, quindi, l'utilizzo di un linguaggio comune e favorendo l'integrazione.

Di contro, non affrontano:

- gli aspetti legati alla progettazione organizzativa, all'allineamento organizzativo e alla gestione del cambiamento;
- gli aspetti economici (es: controllo di gestione, analisi delle performance, pianificazione economica).

Il loro ambito, per giunta, è spesso limitato ad alcune fasi del ciclo di vita dei servizi (es: Project Management) o ad un aspetto particolare della gestione del sistema informativo (es: ISO27001).

1. Dal 1° Gennaio 2014 la proprietà intellettuale del portafoglio prodotti denominato "Best Management Practice", di cui fanno parte tra le altre best practice come ITIL v3 e Prince2, è passata ad AXELOS società joint venture costituita da Capita e dal Cabinet Office.

Ciascuna best practice è settoriale, incentrata su tematiche peculiari per rispondere ad esigenze specifiche ed è, quindi, insufficiente da sola a spiegare e coordinare l'insieme delle attività svolte da una Funzione ICT, che invece, deve fornire un sistema efficace ed efficiente in grado di dare le giuste risposte al business e offrire soluzioni funzionali agli obiettivi.

Per questo motivo è necessario dotarsi di un framework in grado di guardare in maniera integrata e complessiva alle tematiche relative alla gestione della relazione con il cliente, al governo dell'evoluzione delle architetture e dei processi di business, alla gestione dei progetti di sviluppo, al governo e controllo dei fornitori, all'erogazione dei servizi.

COBIT 5: La necessità di un framework integrato di IT Governance e IT Management

Vista la frammentazione e la settorialità dei diversi framework, **ISACA®**[2], Organizzazione internazionale no profit e indipendente - impegnata nello sviluppo di best practice per divulgare la conoscenza in ambito IT Governance and IT Management, ha sviluppato nel 2012 la versione 5 del **COBIT** (COBIT 5.0). Chiaro l'intento di integrare tutti i principali framework di sua proprietà e di allinearsi con gli altri presenti sul mercato (ad es. ITIL, PMBoK). COBIT 5 merita quindi un approfondimento.
Il modello COBIT, **Control Objectives for Information and related Technology**, è nato per supportare le attività di revisione dell'IT. Arrivato alla quinta versione, ha ampliato sostanzialmente la sua mission originaria, unendo al tradizionale approccio di controllo e audit dei sistemi informativi gli attuali strumenti di Governance per l'IT. "*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 azienda e della necessità di porre in primo piano le problematiche del top management anche nell'ambito del governo dell'IT*"[3] .

L'obiettivo del COBIT 5 è quello di fornire delle linee guida per costruire il sistema di IT Governance di un'azienda, tramite cui il vertice aziendale può finalmente ottenere visibilità sull'andamento dell'IT, sul suo allineamento con gli obiettivi strategici e sul valore che porta al business aziendale.

Il framework COBIT5 è composto da 37 processi che suddivide in 5 famiglie:

- **Processi di Valutazione**, **indirizzo e monitoraggio** (*Evaluate, Direct and Monitor*), noti come processi EDM, volti ad assicurare che la Direzione IT sia in grado di comprendere il suo ruolo nella realizzazione della strategia dell'organizzazione e di erogare valore al business, mantenere sotto controllo i rischi e utilizzare in modo efficiente le risorse;
- **Processi di Allineamento col business**, **pianificazione e organizzazione** (*Align, Plan and Organize*), conosciuti come processi APO, volti a permettere la definizione di una strategia IT allineata e di supporto alla strategia del Board, all'interazione con le Business Unit e all'organizzazione del lavoro nella Direzione IT;
- **Processi di Realizzazione, Acquisizione e Rilascio in Esercizio** (*Build, Acquire and Implement*), noti come processi BAI, volti alla realizzazione di progetti e servizi, a partire dalla raccolta dei requisiti, per giungere alle attività di test e rilascio delle applicazioni nell'ambiente di produzione;
- **Processi di Erogazione dei servizi e di Supporto** (*Deliver, Service and Support*), chiamati processi DSS, volti a permettere il corretto funzionamento delle attività di monitoraggio dei servizi, della loro gestione e mirati all'esecuzione delle attività di supporto e assistenza agli utenti;
- **Processi di Monitoraggio**, **Valutazione e Assessment** (*Monitor, Evaluate and Assess*), indicati come processi MEA, volti a controllare le performance di progetti e servizi, il rispetto dei livelli di performance stabiliti e ad assicurare la compliance normativa.

Nell'immagine seguente sono riportati in dettaglio tutti i 37 processi COBIT, suddivisi per processi di Governo dell'IT (EDM) e processi di IT Management (APO, BAI, DSS, MEA).

2. www.isaca.org
3. ISACA, AIEA - White paper "COBIT e ITIL due framework complementari – Maggio 2007".

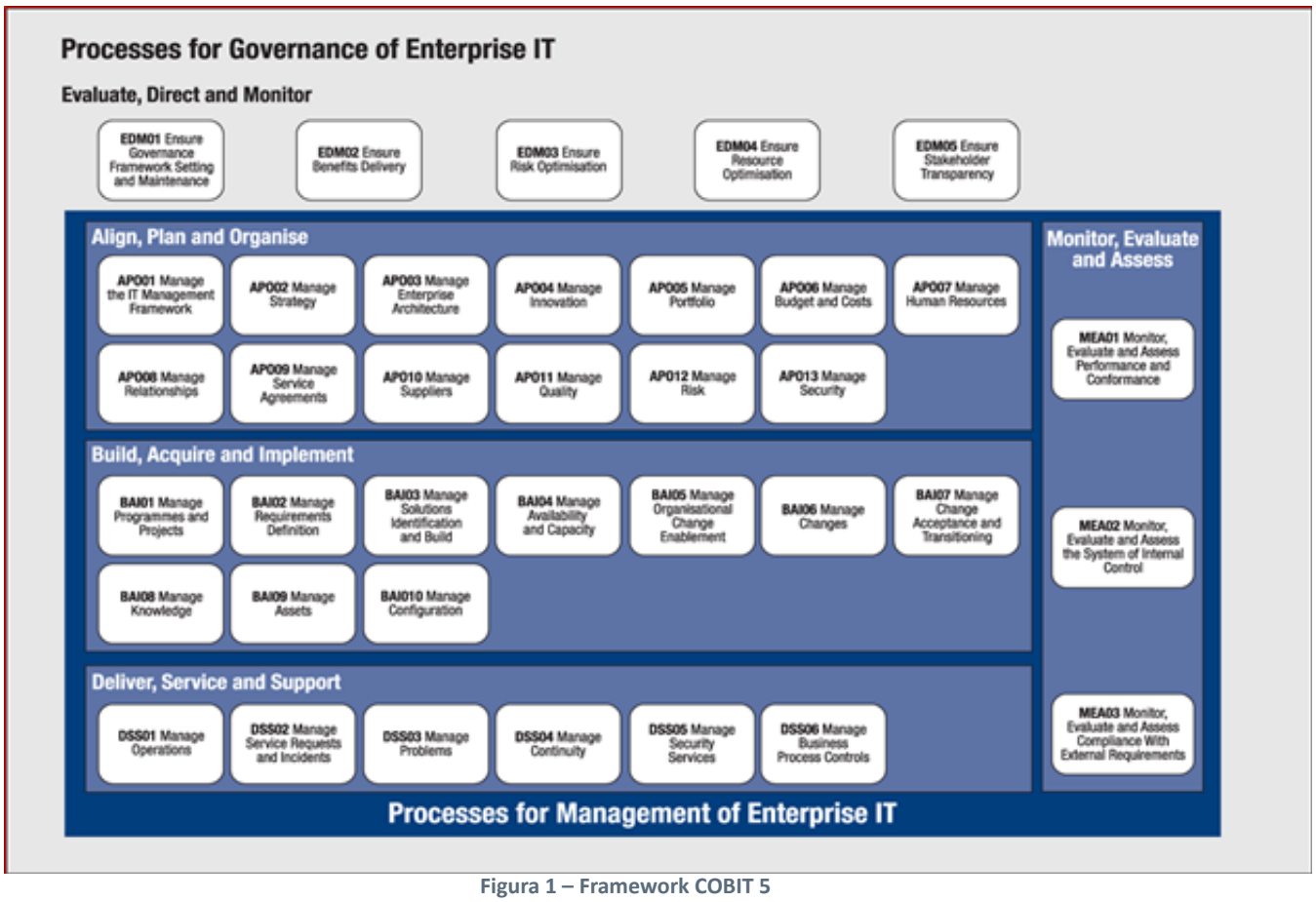


Figura 1 – Framework COBIT 5

Il framework **COBIT** ha l'obiettivo di supportare le Funzioni ICT nella **creazione del valore per il business**, mantenendo un equilibrio ottimale tra l'utilizzo delle risorse, l'esecuzione delle prestazioni e i livelli di rischio. Il suo utilizzo favorisce una **gestione olistica** dei Sistemi Informativi, tenendo conto degli **interessi** e delle **responsabilità di tutti gli stakeholder** interni ed esterni all'IT.
In particolare, il framework COBIT 5 rafforza l'accento **sul governo dell'IT** (IT Governance) **e la sua gestione** (IT Management) in funzione del Business.
L'**IT Governance** assicura che gli obiettivi aziendali siano raggiunti attraverso:

- la valutazione delle necessità di tutti gli stakeholders;
- la direzione delle attività dell'IT attraverso la definizione delle priorità e degli obiettivi interni;
- il monitoraggio delle prestazioni dell'IT, verificando l'on-going e la compliance rispetto alle strategie IT definite in funzione degli obiettivi aziendali.

L'**IT Management** garantisce la pianificazione, lo sviluppo, l'esercizio e il monitoraggio delle attività in linea con gli obiettivi definiti dall'IT Governance.

Livello di copertura del COBIT 5 rispetto ai principali framework di mercato

Nella figura seguente[4] si riportano sinteticamente le principali aree di sovrapposizione tra il COBIT 5 e i principali framework di mercato.

4. COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT – Appendix E - Mapping of COBIT 5 With the Most Relevant Related Standards and Frameworks - ISACA

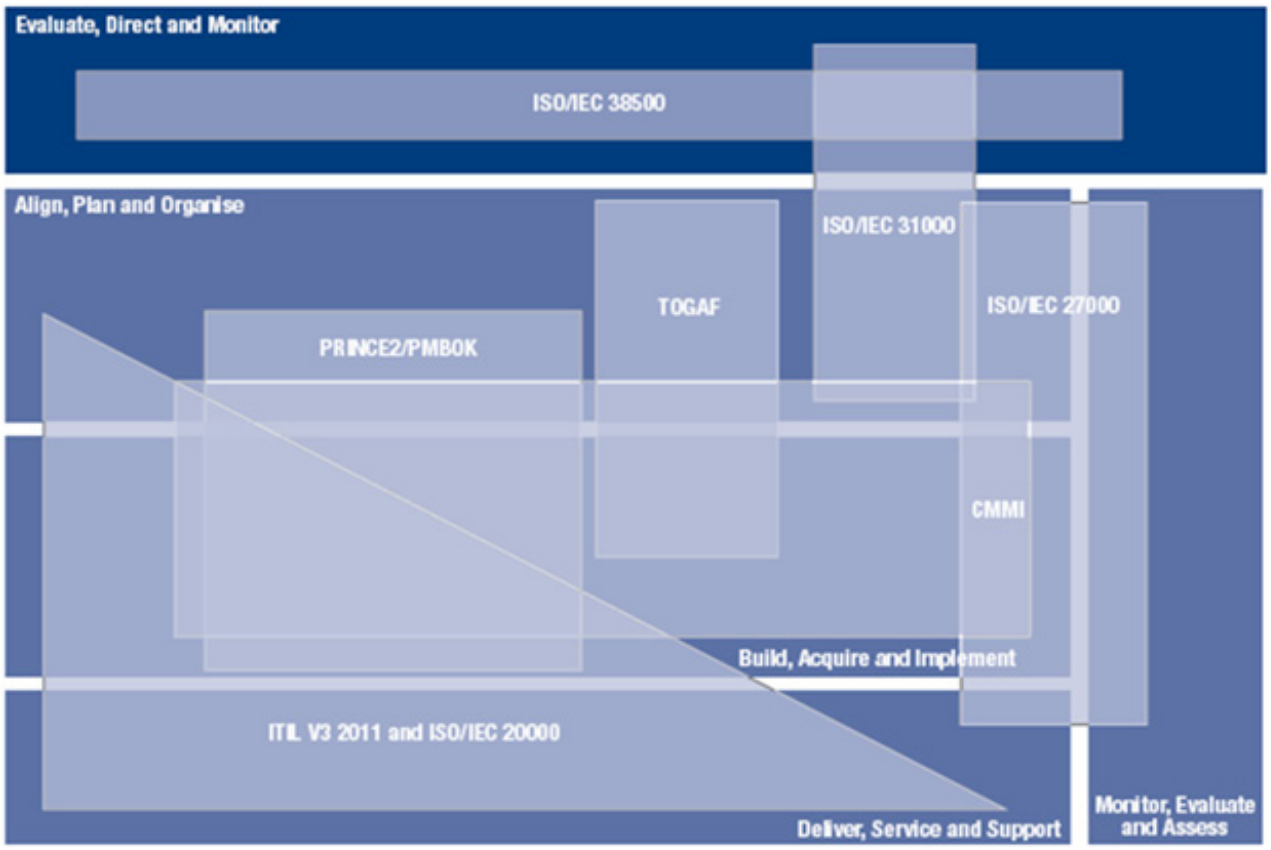


Figura 2 – Aree di sovrapposizione tra il COBIT 5 e i principali framework

Il COBIT 5.0 deriva dal COBIT 4.1 ed è stato costruito espandendo e integrando quest'ultimo con altri framework, tra cui ITIL v3, PMBoK, TOGAF e gli standard dell'International Organization for Standardization (ISO).
Come si evince dalla figura, il COBIT 5 copre tutte le aree definite in precedenza (ad eccezione dell'area relativa alla gestione delle competenze - **Skill & Competence Management**). Tuttavia mentre il COBIT è principalmente uno strumento di Governance che fornisce supporto per stabilire che "***cosa fare***" in termini di obiettivi e processi da attivare e **come controllare il raggiungimento di tali obiettivi**, i "framework verticali" forniscono le indicazioni e gli strumenti per definire "***come fare***" risultando pertanto complementari rispetto al COBIT 5.0, che ha alcuni limiti:

- **non fornisce linee guida** su come implementare i processi, mira essenzialmente a identificarne i confini, le relazioni, gli obiettivi di controllo e le metriche;
- **rimanda a best practice e standard** specializzati per indicazioni di dettaglio sulla progettazione di processo, la definizione di procedure operative e l'implementazione.

Nel prossimo paragrafo analizzeremo alcune aree particolari per mettere in evidenza come utilizzare i framework verticali per arricchire ed integrare COBIT.

Come costruire il proprio framework integrato attraverso il tailoring del COBIT

In questo paragrafo si analizza come costruire il proprio modello di funzionamento attraverso il tailoring del COBIT 5.0. Come detto nell'introduzione, le aziende devono evitare un approccio troppo rigido che si basi sull'adozione pedissequa di uno standard o di un singolo framework, perché ciò non porta reale valore e al di là di superficiali effetti "make-up".

Il risultato che si ottiene, infatti, è quello di ingabbiare la struttura organizzativa, rendendola meno efficiente

ed a volte anche meno efficace.
Nella scelta delle best practice da "adottare" è necessario, quindi, considerare il giusto livello di "tailoring" valutando quanto di buono, efficiente, efficace ogni framework porta con sé, e contestualizzarlo alle reali esigenze dell'organizzazione e alla sua capacità di assorbimento.
Sulla base della propria esperienza nella revisione dei modelli di funzionamento delle organizzazioni IT, abbiamo fatto nostro l'utile suggerimento proposto da tutti gli organismi che si occupano dello sviluppo degli standard, che prevede due precisi passi nell'adozione di una best practice da parte di una organizzazione:

- **Step 1** "**Adopt**", ovvero "**Adottare**" le best practice e gli standard, beneficiando del lavoro di sistematizzazione effettuato dalle organizzazioni internazionali;
- **Step 2** "**Adapt**", ovvero "**Adattare**" le best practice selezionate allo specifico contesto aziendale, selezionando e integrando le porzioni di standard che meglio rispondono alle esigenze della propria Funzione Sistemi Informativi.

Come si evince, l'approccio non prevede di adottare necessariamente una best practice nella sua interezza.

Step 1. Adopt. Individuare le best practice adatte al contesto

Per l'adozione di una o più best practice suggeriamo un **approccio sistemico**, che miri a definire il modello di funzionamento complessivo della Funzione ICT e stabilisca **quali unità organizzative** devono eseguire **quali attività** e con **quali strumenti**, seguito poi da **interventi attuativi** "**verticali**" finalizzati alla risoluzione di specifiche criticità. Seguendo questo metodo va da sé che il framework più adatto per definire l'impianto dei processi della Funzione ICT sia **COBIT 5.0**, da integrare poi con le best practice e gli standard specializzati (ITIL, PMBoK, etc.) in funzione degli obiettivi e delle esigenze che si vogliono indirizzare.

Step 2. Adapt. Adattare le best practice al contesto

Nell'effettuare il tailoring del COBIT 5.0 è necessario:

- selezionare i processi che meglio si addicono al contesto e alle esigenze dell'azienda;
- integrare il COBIT con le diverse best practice "vertical".

Identificazione del set di processi da inserire nel modello dei processi

Una volta scelta la best practice di riferimento (COBIT 5), il primo passo è individuare quanti e quali processi inserire nel proprio framework in funzione di obiettivi, esigenze, vincoli, punti di forza dell'azienda, ma anche delle criticità e delle aree di miglioramento che si vogliono indirizzare e delle indicazioni delle best practice (COBIT 5, ITIL v3, PMBOK, ISO/IEC 27001, OPBOK, etc.).
Per identificare i processi "necessari", è fondamentale condurre un'analisi iniziale in cui:

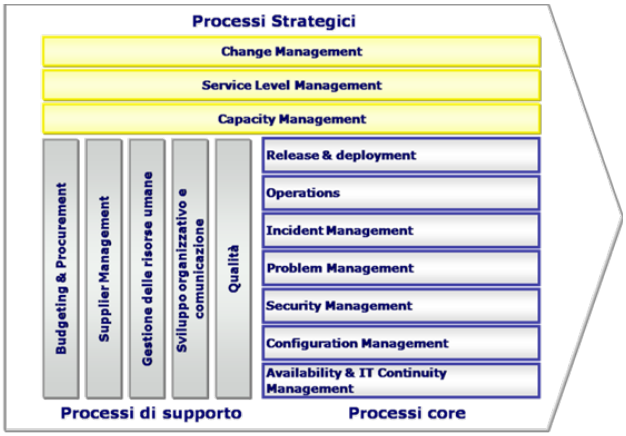
- Contestualizzare l'impresa cliente nel mercato di riferimento (Public Utility, Energy, ecc.);
- Definire il grado di complessità dell'impresa cliente;
- Definire l'attuale ampiezza della Funzione ICT (limitata/media/ampia), i suoi compiti, il grado di considerazione dell'IT nell'organizzazione, il grado di supporto alla realizzazione della strategia aziendale, la capacità di attrarre investimenti, il suo grado di strategicità, etc;
- Capirne l'organizzazione (Organigramma, Ruoli e responsabilità);
- Valutare i volumi gestiti, in termini di progetti, servizi erogati, ampiezza delle Operations, capacità di soluzione delle criticità, ecc.;
- Analizzare i modelli di outsourcing utilizzati: la Funzione ICT utilizza l'outsourcing? Quanti fornitori esterni sono presenti? Come sono gestiti i contratti? Si fa utilizzo del Time-material?;
- Analizzare quanti e quali sono i clienti; etc.

Per definire correttamente il modello di riferimento, tra tutti gli elementi elencati, va posta particolare attenzione alla scelta del modello di outsourcing e alla definizione dei processi di gestione e monitoraggio degli stessi, al fine di garantire sia la coerenza dei servizi erogati con quanto richiesto, sia l'interazione ottimale a livello operativo tra tutti gli attori, interni ed esterni alla Funzione ICT.
Effettuata l'analisi, per creare un modello coerente e di semplice adozione bisogna selezionare i processi che

meglio garantiscono una risposta e un indirizzo alle criticità/problematiche riscontrate e che consentono di raggiungere gli obiettivi definiti, codificando una procedura compatibile con la capacità di gestione dell'IT con le risorse disponibili.
Un utile strumento per definire questi step è rappresentato dalla **Goal – Cascade** proposta da COBIT 5, che consente di individuare i processi da implementare e di legarli agli obiettivi strategici dell'azienda.

Figura 3 - Goal Cascade

La Goal Cascade serve ad individuare i bisogni degli stakeholder (**Stakeholder Needs**), a trasformare quest'ultimi in obiettivi strategici (**Enterprise Goals**), e a declinarli in obiettivi per l'ICT (**IT Goals**). Individuati gli obiettivi IT è possibile selezionare, all'interno del framework, i processi che abilitano il loro raggiungimento e, quindi, definire gli interventi prioritari basandosi sugli obiettivi strategici dell'impresa.
Attraverso la Goal – Cascade è possibile, inoltre, monitorare e controllare l'andamento dell'IT e verificarne l'allineamento agli obiettivi di business.
Individuati i processi si può procedere a una categorizzazione in funzione della loro strategicità per l'azienda:



- **Processi Strategici**, che definiscono la strategia e indirizzano la gestione del Sistema Informativo. Questi processi sono incentrati su acquisizione e conoscenza delle esigenze del cliente interno ed esterno e sul coordinamento delle modifiche e delle evoluzioni del Sistema Informativo e dei servizi.
- **Processi Core**, che costituiscono i processi maggiormente legati alla missione dell'IT ovvero a garantire la realizzazione e il funzionamento dei servizi.
- **Processi di Supporto**, che descrivono le attività che non sono strategiche né peculiari dell'IT.

Integrare le diverse best practice

Definito il modello complessivo, il passo successivo è il passaggio dal punto di vista olistico a uno più verticale, integrando il COBIT con le best practice "specialistiche" dedicate a processi o domini di processi affini. Quindi, ad esempio, per ottimizzare l'erogazione dei servizi (Service Management), è possibile progettare i relativi processi di gestione (*Incident Management, Problem Management, Configuration Management, Service Level Management*, etc.) utilizzando quanto previsto dal framework ITIL. Al contrario, per migliorare il governo e la gestione dei programmi e dei progetti aziendali è opportuno fare ricorso alle metodologie proposte dal PMI (PMBoK) o da PRINCE2.
In altre parole è necessario approfondire le singole aree di processo facendo riferimento alla best practice o allo standard più maturo su quell'aspetto. A seguire analizzeremo come integrare il COBIT con i framework vertical su alcune delle aree sopra menzionate.

Service Management

Nello sviluppare il COBIT 5 gli autori hanno integrato e allineato il modello alla versione ITIL v3 del 2011: ad oggi non ci sono lacune rispetto all'impianto di processi previsti dall'ITIL.
La differenza sta dunque nell'approccio: mentre il COBIT ha l'obiettivo di offrire una metodologia per definire quali processi implementare e garantire il governo dei Sistemi Informativi, ITIL fornisce indicazioni operative per erogare servizi di qualità, allineati alle esigenze di business.
All'interno dell'area di Service Management, quindi, i due modelli sono complementari e, se utilizzati insieme, riescono a fornire tutti gli elementi necessari a creare un efficace modello di IT Governance ed IT Management. Il COBIT può essere utile per ottenere indicazioni sulle aree di intervento e sugli obiettivi da porre - verificando che siano raggiunti - mentre ITIL può essere preso a riferimento per descrivere in maniera dettagliata i processi, le attività da realizzare, quali strumenti utilizzare.
La sinergia tra i due framework è evidenziata anche dal fatto che si citano vicendevolmente. Vediamo come integrare COBIT 5.0 e ITIL v3, ad esempio, per il disegno del processo di Gestione degli Incidenti (**Incident Management**).
Nel COBIT la gestione degli incidenti viene gestita insieme alle Service Request all'interno del processo **DSS02 Manage Service Request and Incident** viene descritta così: "*Fornire una risposta tempestiva ed efficace alle richieste degli utenti e per la risoluzione di tutti i tipi di incidenti, ripristinare la "normale operatività", registrare e soddisfare le richieste degli utenti, e registrare, analizzare, diagnosticare, inoltrare e risolvere gli incidenti*". Il processo, secondo COBIT, ha l' obiettivo di "*raggiungere una maggiore produttività e ridurre al minimo le interruzioni attraverso la rapida risoluzione delle richieste degli utenti e degli incidenti*".
In ITIL v3 i processi di Gestione degli incidenti e Gestione di Service Request sono separati. Il processo di I**ncident Management** gestisce quindi esclusivamente i malfunzionamenti, come emerge dalla pubblicazione Service Operation: "*Incident Management è il processo responsabile della gestione del ciclo di vita di tutti gli incidenti. Gli incidenti possono essere riconosciuti dal personale tecnico, rilevati e segnalati da strumenti di monitoraggio, comunicati dagli utenti, o riportati da terzi (es. fornitori e partner)*". L'obiettivo, secondo ITIL, è di "*ristabilire le normali condizioni di servizio il più rapidamente possibile minimizzando l'impatto negativo sul business di incidenti e malfunzionamenti*". Le due descrizioni, così come gli obiettivi, sono molto simili e si possono utilizzare in maniera indifferente selezionando quella che meglio si addice al contesto aziendale o facendo un mix delle due.

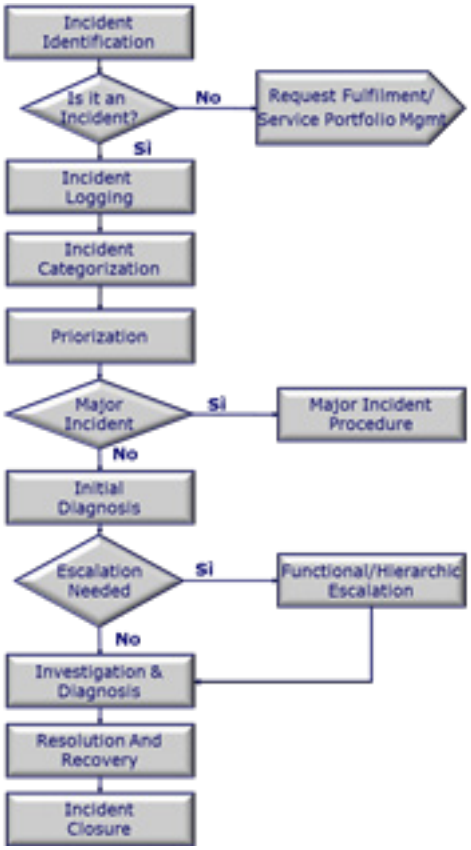


Figura5 - Processo di Incident Management

Per la definizione delle attività e per il supporto all'implementazione del processo ITIL può darci maggiori indicazioni con interessanti suggerimenti, ad esempio:

- Definisce cosa si intende per Incident "*Interruzione non pianificata, riduzione della qualità o malfunzionamento a un componente IT di un servizio IT che tuttavia ancora non ha causato impatti al servizio stesso*";
- fornisce indicazioni su come approcciare al processo;
- indica i benefici ed il valore del processo per il business;
- descrive i principali problemi, rischi e fattori

critici di successo che si possono incontrare nell'implementare il processo;
- definisce le relazioni con gli altri processi;
- descrive nel dettaglio le attività ed il flusso di attività;
- descrive come registrare, categorizzare e elencare le priorità degli incidenti;
- descrive i campi minimi che deve contenere il record dell'incident;
- descrive come costruire degli "Incident Model" per gestire correttamente gli incidenti;
- descrive come analizzare i ticket e che strumenti utilizzare;
- fornisce indicazioni sugli strumenti e sulla loro configurazione;
- elenca suggerimenti sulla reportistica e sulle metriche operative da utilizzare.

In particolare, per la **definizione delle metriche** ITIL e COBIT sono complementari. Infatti, COBIT afferma che ogni processo abilita alcuni obiettivi IT (IT Goal) che a loro volta abilitano gli obiettivi aziendali (Enterprise Goal). Per questo motivo le metriche indicate da COBIT (ad es. N° di major incident non identificati nel risk assessment, o N° di interruzioni del business dovuti a malfunzionamenti IT) sono principalmente orientate a valutare se il processo raggiunge gli IT Goal definiti. Le metriche proposte da ITIL, invece, sono legate ai Critical Success Factor individuati per il processo (ad es. risolvere gli incidenti nel minor tempo possibile, riducendo l'impatto per il business) e all'operatività del processo (ad es. tempo medio di risoluzione degli incident, backlog, etc.).
Quindi possiamo dire che, per l'implementazione del processo, ITIL fornisce numerosi spunti su come realizzarlo, sui problemi che si incontrano e su come superarli, mentre COBIT è di supporto all'individuazione di priorità sostenibili e al controllo del processo per verificarne la sua "maturità".
Infine i due framework risultano essere complementari nella definizione dei ruoli e dell'organizzazione a supporto.
Se da un lato ITIL si concentra sui ruoli di processo, identificando e descrivendo in dettaglio le attività e le responsabilità delle figure coinvolte (Service Desk, Incident Manager, Supporti di II livello, etc.), dall'altro COBIT mappa le responsabilità delle attività di processo sulle tipiche figure professionali di un'organizzazione IT, come mostrato nella figura a lato:

DSS02 RACI Chart

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
DSS02.01 Define incident and service request classification schemes.						C					I	I						A	C	R	R		R	C	C	C
DSS02.02 Record, classify and prioritise requests and incidents.						I					I	I									A		R			I
DSS02.03 Verify, approve and fulfil service requests.						R												I		R	R		A			
DSS02.04 Investigate, diagnose and allocate incidents.						R					I	I				I	I	I		C	R		A	C		
DSS02.05 Resolve and recover from incidents.						I					I	I				C	C	I		R	R		A	R		C
DSS02.06 Close service requests and incidents.						I					I	I				I	I	I		I	A		I	R		I
DSS02.07 Track status and produce reports.						I					I	I				I	I	I		I	A		R	I		

Figura 6 - COBIT RACI

Enterprise Risk Management

Anche in quest'area le prassi presenti ad oggi sul mercato sono fortemente complementari e per l'esperienza maturata in ambito sicurezza e gestione del rischio, suggeriamo di integrare il COBIT con diverse best practice e standard verticali sui temi di sicurezza, che lo stesso COBIT tra l'altro cita come "Related Guidance".
Vediamo come e dove è possibile integrare il COBIT:

- All'interno dei **processi EDM** che hanno come obiettivo la governance dei SI, troviamo il processo **EDM03 – Ensure Risk Optimization**, volto a mantenere sotto controllo i rischi aziendali. È possibile definire un **modello complessivo** per gestire in maniera olistica tutti i rischi aziendali, integrando quanto suggerito dal COBIT con i framework dedicati al governo della sicurezza e dei rischi, come la **ISO 31000** o l'**Enterprise Risk Management** (**ERM**) del CoSO, focalizzati sulla gestione del rischio aziendale.
- All'interno dei **processi APO** volti a definire e pianificare una strategia IT allineata alle esigenze del Business segnaliamo i processi **APO12 – Manage Risk** e **APO13 – Manage Security**, che hanno l'obiettivo rispettivamente di "*identificare gestire e ridurre i rischi*" e "*definire, gestire e controllare un sistema di gestione della sicurezza*". Su questi aspetti è opportuno integrare il COBIT con framework più verticali che affrontano in maniera

peculiare le diverse tematiche:

- ◊ Per la gestione del rischio (Information Risk Management) si possono utilizzare la ISO/IEC 27005, che ha un approccio più gestionale nel definire le linee guida di gestione dei rischi informatici, e la pubblicazione NIST 800-39 per scendere ad un livello più operativo e integrare le metriche definite dal COBIT, definire il processo e le procedure operative, attuare i controlli.
- ◊ Per la definizione di un sistema di sicurezza delle informazioni (Information Security Management System) si possono scegliere la ISO/IEC 27001, con focus più gestionale nel definire le linee guida di gestione del proprio Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS), e la pubblicazione NIST 800-53 per scendere ad un livello più operativo e integrare le metriche definite dal COBIT, definire il processo e le procedure operative, attuare i controlli.

- All'interno dei processi BAI volti alla realizzazione di progetti e servizi, a partire dalla raccolta dei requisiti fino alle attività di test e rilascio delle applicazioni nell'ambiente di produzione, non vi sono processi che esplicitamente richiamano aspetti di sicurezza. Tutti i framework citati finora possono dare delle indicazioni utili per gestire e ridurre i rischi presenti nel passaggio dallo sviluppo all'esercizio che è poi uno degli obiettivi principali di questa fase.
- All'interno dei processi DSS che garantiscono l'esercizio dei SI per assicurare servizi di qualità, ci sono molti aspetti legati alla sicurezza (gestione degli incidenti, gestione dei problemi, etc.). In particolare troviamo il processo DSS05 – Manage Security Services che ha l'obiettivo di gestire la sicurezza operativa e può essere integrato con i controlli previsti dalla ISO/IEC 27002 e quelli definiti nella pubblicazione NIST 800-53 rev1. Troviamo, anche, il processo DSS04 – Manage Continuity che ha l'obiettivo di garantire la continuità operativa e può essere integrato con i framework di Business Continuity Management, come la ISO 22301, la ISO/IEC 27031, la pubblicazione NIST 800-34, il DRI International (DRII) e il Business Continuity Institute (BCI). Questi ultimi forniscono un quadro di riferimento per la definizione di un processo olistico in grado di identificare potenziali minacce per l'organizzazione e anticipare gli impatti al business che quelle minacce, se realizzate, potrebbero causare.
- Per i processi MEA, infine, volti a controllare le performance di progetti e servizi e il rispetto dei livelli stabiliti di tali performance, nonché ad assicurare la compliance normativa, il COBIT rappresenta probabilmente il framework più ricco ed è autonomo nell'integrare quanto riportato all'interno degli altri standard in termini di controllo e audit.

Per maggiori dettagli su come integrare il COBIT con i framework di sicurezza e sui benefici che se ne possono trarre, rimandiamo ad un articolo già pubblicato in questa newsletter - ***IT Governance e Information Risk Management: un connubio perfetto*** *a cura di Corrado Pomodoro.*

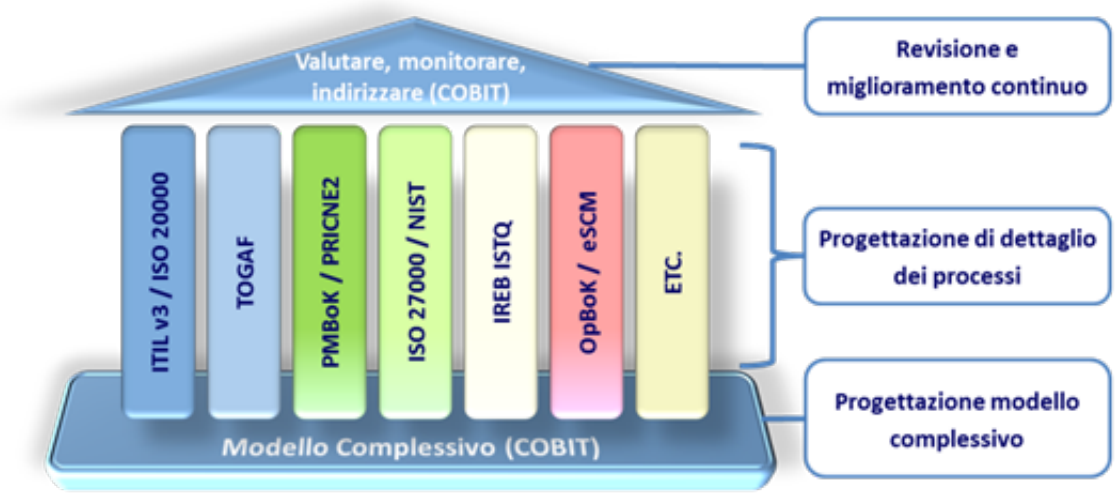
Gli esempi sopra esposti, e quanto detto finora, mettono in evidenza come sia fondamentale nell'implementazione del framework COBIT5 (come di qualsiasi altra best practice) adattarlo alle esigenze aziendali, eliminando i processi non significativi ed inserendone di nuovi (tailoring), se necessario.
Definito il modello complessivo e dettagliati i singoli processi, è possibile utilizzare il COBIT come linea guida per misurare l'efficacia, l'efficienza ed il livello di rischio del modello definito attraverso l'utilizzo degli obiettivi (IT Goal) stabiliti e delle metriche suggerite. Utilizzando a ritroso la Goal Cascade è possibile, infatti, risalire dalle performance di un processo agli obiettivi aziendali che si volevano raggiungere e verificarne, quindi, l'effettivo raggiungimento.

Conclusioni

Ricapitolando riteniamo fondamentale per una Funzione ICT dotarsi di un modello di funzionamento integrato di IT Governance e IT Management per presidiare in maniera completa e strutturata tutte le attività necessarie a garantire servizi efficaci ed efficienti e soprattutto allineati alle reali esigenze del business.
Abbiamo quindi esposto i passi che deve compiere una Funzione ICT per costruire il proprio modello di

funzionamento:

A. Adottare il COBIT 5.0 come “fondamenta” su cui modellare il proprio framework, attraverso cui identificare quali processi implementare, i loro confini, le loro relazioni e le responsabilità delle singole unità organizzative;
B. Adattare il COBIT alle esigenze aziendali e integrarlo con le best practice specializzate, per progettare i singoli processi e indirizzare le specifiche tematiche;
C. utilizzare il modello di valutazione del COBIT per definire le metriche di controllo, verificare l’efficacia di quanto implementato e indirizzare le opportune azioni di miglioramento.



Quindi possiamo concludere che, nel definire il proprio modello integrato di IT Governance e di IT Management, una Funzione ICT debba evitare l’approccio da “supermarket” - vedo, scelgo, implemento, utilizzo - in cui si seleziona una best practice o un framework e la si implementa così com’è, stand alone.
Infatti, come abbiamo visto, l’implementazione pedissequa di uno standard potrebbe essere onerosa oltreché inefficacie ed incompleta.
Al contrario, il successo di un’iniziativa di questo tipo è legata alla capacità delle risorse coinvolte nel progetto di “cucire” il framework (o i framework scelti) sulle esigenze dell’azienda, facendo in modo che “l’abito” vesta perfettamente il cliente.
Come un sarto (ecco perché si parla di "tailoring"), il team coinvolto nell’implementazione di un framework deve:

- consigliare il cliente sul capo adatto e sul tessuto più idoneo (scegliere lo/gli standard ed i processi che meglio si adattano al contesto);
- prendere le misure della persona (capire le reali esigenze dell’azienda);
- tagliare il tessuto su misura (adattare il framework, utilizzando se necessario le indicazioni delle best practice specialistiche per dettagliare i processi);
- confezionare il capo (costruire il macro-modello di funzionamento e progettare i singoli processi);
- perfezionare il capo, a seguito della prova del cliente, risolvendo criticità e difetti e aggiungendo le rifiniture (effettuare il tuning del modello, avviando un percorso di miglioramento continuo);
- consegnare il capo al cliente (fare formazione e gestire la comunicazione per curare le attività di Change Management verso le risorse umane coinvolte, necessarie a rendere possibile e facilitare il cambiamento e a permettere una più veloce ed efficace comprensione e interiorizzazione delle nuove modalità operative e dei motivi per cui abbracciarle).

È importante ricordare, infine, che nel costruire il proprio framework integrato di IT Governance ed IT Management è fondamentale trovare il **giusto equilibrio nell’introduzione delle nuove modalità operative**, e dare il tempo necessario affinché l’organizzazione sia “pronta” ad assorbire il cambiamento, attraverso un processo di approssimazioni successive.

HSPI SpA - Consulenti di Direzione
Viale Aldo Moro 16 - 40127 Bologna (Italy)
P.IVA 02355801206

Tel. +39 051 509861 | Fax. +39 051 509737
BOLOGNA | MILANO | ROMA
www.hspi.it | e-mail: info@hspi.it