N° 1 2009

di Lorenzo Caselli

Un'altra economia è possibile

saggi

Roberto **Cafferata**

Il cantiere aperto della responsabilità sociale dell'impresa

Marco **Frey**

Il bilancio sociale delle Università

Emanuele **Invernizzi**

Comunicazione, processi decisionali strategici e marketing (di Emanuele **Invernizzi**, Rossella **Gambetti** e Stefania **Romenti)**

Gianni **Cozzi**

Note in margine al saggio di Dario Velo sulla continuità e sulla discontinuità negli studi di marketing

Silvia **Bruzzi**

Innovazione scientifica e innovazione imprenditoriale nel settore farmaceutico

Paolo **Parini**

I confidi locali nella transizione ad intermediari finanziari: miti da sfatare e modelli alternativi di sviluppo

Silvana **Gallinaro**

La modularità nello sviluppo e nella produzione dei servizi

working paper

Sara **Cepolina**

La politica per la ricerca e l'innovazione in Piemonte: coordinare e coinvolgere. Un confronto con la Liguria

Renata Paola **Dameri**

Le determinanti dell'IT governante e la creazione di valore

Riccardo **Amidei**

Governance ICT e competenze professionali

Stefano **Privitera**

Governance ed accountability aziendale in Finmeccanica

< indietro

Reg. Tribunale di Genova, n. 11/2004 del 31 maggio 2004 ISSN 1824-3576 Cod. CINECA E187020 p.iva 00754150100

IMPRESAPROGETTO
RIVISTA ON LINE DEL DITEA
n. 1 - 2009

Governance ed accountability aziendale in Finmeccanica

Stefano Privitera

Sommario: 1. L'IT governance: compliance view e governance view - 2. L'implementazione dell'IT governante - 3. L'IT compliance e il change culturale - 4. Preparazione ai test ITGC: approccio top-down e bottom-up

Abstract

Information Systems (IS) compliance is one of the main challenges for the IT governance. Not only because IS compliance is difficult to implement and maintain, but also because the investment for IS compliance is very heavy. Companies could pursue two different behaviours: the *compliance view* considers IS compliance as a duty and the cost to implement it as necessary; the *governance view* considers IS compliance like an opportunity for improving the quality of administrative processes and accounting information systems, and its cost as an investment able to produce important returns for the company.

1. L'IT governance: compliance view e governance view

- In un mondo che cambia velocemente, anche sotto effetto di eventi estremi, generando incertezza…
- …aumentando la pressione sulle aziende sia in termini di rapidità di intervento che di decisioni da prendere con dati confusi…
- …e con la necessità di mantenere qualità e trasparenza nei sistemi informativi a supporto del business, per evitare la penalizzazione sui mercati finanziari…
- ...è necessario un cambiamento di mentalità nel management, che deve abituarsi a convivere ed operare nell'incertezza…..
- …utilizzando tutte le leve disponibili ed in particolare quella della Corporate Governance e nello specifico della IT Governance.

La principale spinta alla Governance IT viene dall'introduzione delle leggi emanate a protezione degli azionisti delle società quotate in Borsa, dopo il caso

Enron negli USA e Parmalat in Italia. La prima di queste leggi è stata la Sarbanes Oxley (SOx) e di conseguenza le leggi Europee derivate si sono chiamate gergalmente Euro SOx. In Italia le norme relative alla compliance contabile sono contenute nella legge 262/2005, cosiddetta "Legge sulla tutela del risparmio".

La legge prevede una serie di regole di governance dell'azienda e dà delle direttive, molto generiche, anche in merito alla governance IT. Queste direttive vengono generalmente interpretate come una versione ridotta delle regole dettate dalla SOx, in particolare per quanto riguarda l'applicazione del framework chiamato CObIT for SOx, che detta regole di implementazione della compliance molto dettagliate. In Italia si preferisce applicare una selezione dei controlli previsti dal CObIT for SOx, data la mancanza di un regolamento attuativo, per cui l'attuazione dell'IT governance per la compliance può essere diversa nelle varie società. Al di là delle singole scelte, è però importante vedere l'implementazione di queste normative, che presenta costi molti elevati per l'impresa, come una parte di Governance e non solo come un obbligo di compliance, per poterne sfruttare al meglio le possibilità offerte.

Possiamo quindi delineare due diversi comportamenti aziendali: la Compliance view e la Governance view.

La Compliance view mira al governo dell'IT semplicemente al fine di rispondere alle norme della legge in merito alla sicurezza dei sistemi informativi relativamente all'informativa finanziaria. La Governance view, invece, mira a realizzare un sistema di governo dell'IT che interessi l'intero sistema informativo aziendale e consenta di trarre dalla compliance benefici che vanno oltre il mero rispetto delle norme di legge.

La condotta tenuta dalle imprese nelle due visioni può essere sintetizzata come segue.

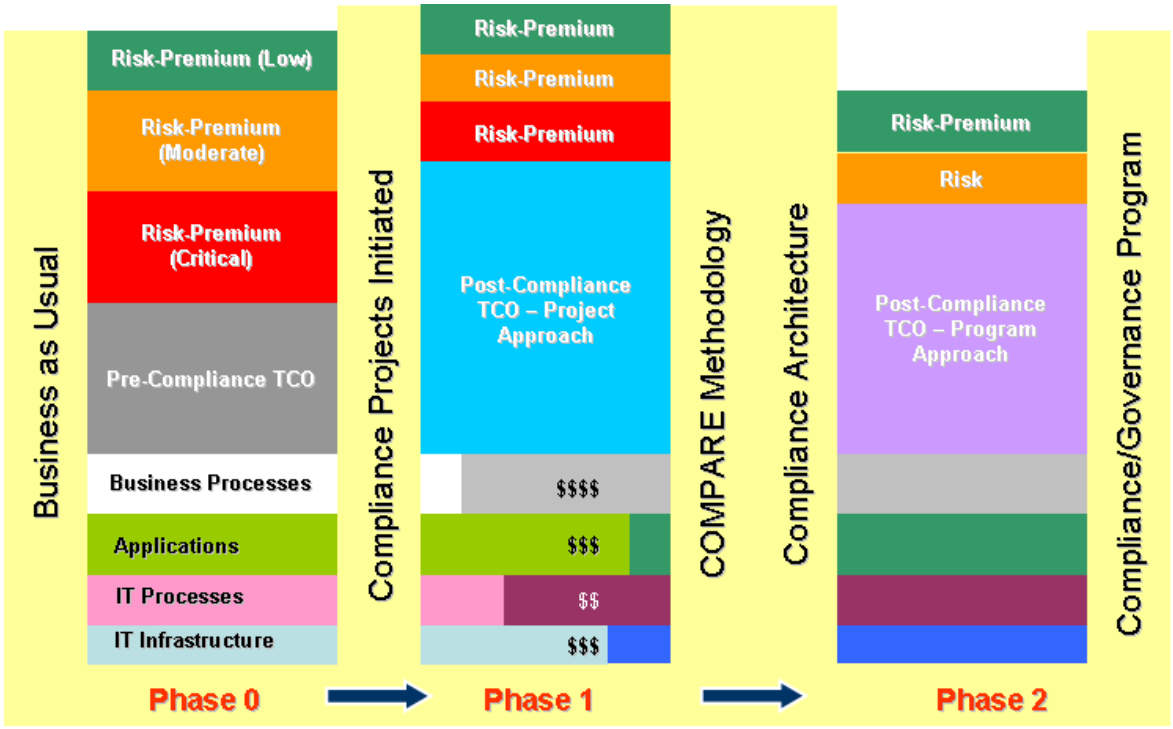
Compliance view
- ✓ attenzione alla sola compliance;
- ✓ evitare cambiamenti nelle infrastrutture.

Governance view
- ✓ vedere la compliance come un'opportunità di miglioramento;
- ✓ aumentare la trasparenza, affidabilità, tempestività ed accuratezza del flusso informativo finanziario e di bilancio;
- ✓ affrontare la compliance per incrementare l'efficacia della gestione;
- ✓ implementare miglioramenti organizzativi.

E' evidente che per le società quotate il calcolo del ritorno dell'investimento nell'implementare un progetto 262 per l'IT è estremamente complesso e gli studi attualmente disponibili riguardano solo la SOx e non sono del tutto applicabili in Italia; pur tuttavia è possibile seguire un quadro di riferimento di origine Gartner (vedi di seguito) che nella sostanza dice che un sistema di Governance e Compliance ben progettato porterà ad un momentaneo aumento dei costi, ma deve ridurli a vita intera, ovvero deve ridurre il TCO (Total Cost of Ownership). Ovviamente nei costi sono considerati anche quelli mediamente derivanti dal

rischio che l'impresa si assume ed in particolare si tiene conto dell'azzeramento di rischi critici che normalmente l'azienda non affronta e quindi non elimina.

Figura 1 - Livello dei costi IT prima dell'applicazione dell'IT governance, dopo la prima implementazione e a regime



- Dipendenza dei TCO dal rischio che si intende assumere
- Gestire la compliance come un processo e non come un progetto consente la riduzione dei TCO
- Riduzione del Risk-Premium

Fonte Gartner

Come si vede in Fig. 1, l'implementazione del sistema di IT governance e compliance può essere analizzata dal punto di vista di costi secondo tre momenti: prima dell'applicazione (Fase 0), dopo l'implementazione (Fase 1) e a regime (Fase 2). Le caselle colorate indicano i diversi tipi di costi sostenuti per i sistemi informativi: infrastruttura, processi, applicazioni, ma anche costi derivanti dal rischio di failure o malfunzionamenti del sistema. È importante osservare che il rischio incide sul TCO in due modi:

- se il rischio viene affrontato e mitigato, genererà costi certi e tangibili;

- se il rischio non viene affrontato, genererà costi incerti e intangibili.

Pertanto, il livello di TCO visibile prima dell'implementazione del sistema di IT governance e compliance dipende dal rischio assunto e mitigato, ma c'è una parte non compresa nel TCO che riguarda il risk-premium non affrontato.

Nella prima fase di implementazione dell'IT governance, il TCO aumenta a causa delle attività di governo e controllo che devono essere progettate ed eseguite; tuttavia, quando il sistema di governo dell'IT va a regime, a fronte di un TCO tangibile più elevato l'impresa può contare su un ridotto livello di rischio e quindi su un minore TCO complessivo, che tiene conto anche dei costi incerti derivanti dal rischio in essere.

Questo schema è difficilmente monetizzabile, ma dà l'idea dei vantaggi derivanti in termini di costo e rischio dal governo dell'IT. Vi sono inoltre due vantaggi esplicitamente misurabili, che riguardano l'accesso al mercato dei capitali e il costo assicurativo.

L'adeguamento alla Legge 262/05 consente un più semplice accesso al Mercato dei Capitali:

- maggiore trasparenza del governo societario = maggiore fiducia da parte degli investitori; Moody's, Standard & Poor's e Fitch Ratings hanno pubblicato documenti su come valutare nel rating l'implementazione di SOX/EURO SOX;
- conformità ai requisiti per il governo societario richiesti per la qualifica di STAR (Segmento Titoli con Alti Requisiti).

L'adeguamento alla Legge 262/05 consente inoltre risparmi in ambito assicurativo:

- riduzione dei rischi e dei premi assicurativi in ambito globale (Risk Premium), vedi la 8th EU Directive ('EURO-SOX');
- assicurazione sui rischi informatici; infatti non è facile ottenere coperture contro la perdita di dati a causa di virus, contro la frode informatica, contro le perdite derivanti da disaster recovery, contro le perdite di profitto o le penali derivanti da interruzioni di trasmissioni o da responsabilità patrimoniali imputabili alla società ed ai suoi amministratori che derivino dalle attività informatiche (es. sicurezza dei dati ecc.).

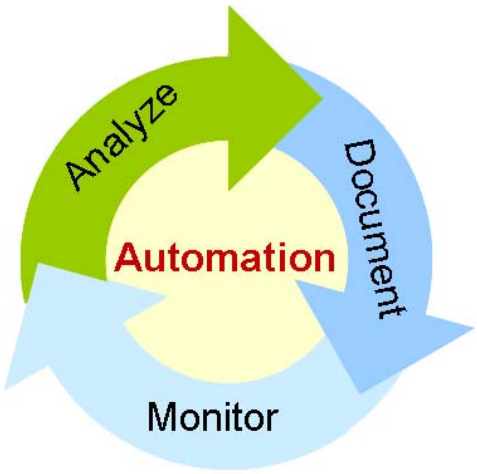
Ma tutto questo pone ulteriori sfide per la compliance all'IT, perché l'analisi dei processi, l'individuazione delle criticità e dei rischi incombenti sui processi di business deve portare a:

- ridurre la complessità del sistema;
- costi più bassi di gestione ed evoluzione;
- migliorare l'affidabilità;
- incrementare la velocità di cambiamento per seguire il business.

Conviene inoltre sempre pensare a muoversi da processi di controllo manuali a controlli di sistema automatizzati focalizzandosi su tre aree chiave (Fig. 2)**:**

- documentazione;
- monitoraggio;
- analisi.

Figura 2 - L'automazione dei controlli per la compliance



Fonte: nostra elaborazione

2. L'implementazione dell'IT governance

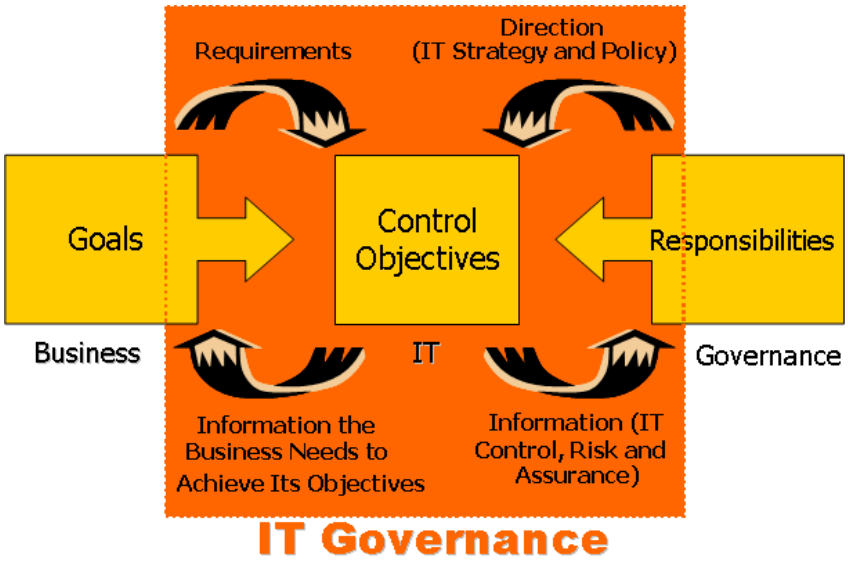
Per facilitare l'implementazione della compliance, sono stati creati degli standard applicativi, che riguardano sia la compliance contabile che quella informatica.

Mentre il riferimento per l'area amministrativa è lo standard COSO II, che riguarda l'internal auditing, l'area IT ha avuto necessità di un riferimento e per questo è universalmente in uso il CObIT, per cui possiamo dire che:

- l'ICT Governance è "l'insieme dei processi messi in atto per garantire che l'ICT partecipi con successo alla creazione del valore ed attui le strategie e gli obiettivi che l'organizzazione si è data";
- nel caso Finmeccanica, la Governance ICT è implementata attraverso l'applicazione di un sottoinsieme dei requisiti definiti dal framework CObIT (release 4.1), standard riconosciuto a livello di mercato per la Governance ICT in correlazione con lo standard COSO II dei sistemi di auditing finanziario;
- la Governance, in tal modo implementata, garantisce la compliance rispetto alla Legge 262/05.

Il concetto di IT governance va quindi molto oltre la semplice compliance amministrativa. Si tratta piuttosto di una attività di governo che si interpone tra requirement formali e sostanziali, tra le norme di legge e il business (Fig. 3). Essa agisce da un lato garantendo informazioni affidabili e sistemi informativi sicuri, dall'altro erogando al business le opportune informazioni atte a supportare le decisioni. Per questa ragione, deve essere guidata sia dalle politiche di controllo, che assicurano la qualità dei dati, sia dalle esigenze strategiche, che garantiscono l'adeguatezza dei dati. Il conseguimento dei risultati ottenuti deve essere perseguito sia grazie all'applicazione delle norme, che alla responsabilizzazione dei soggetti, in funzione dei loro comportamenti.

Figura 3 - Strumenti e azioni dell'IT governance

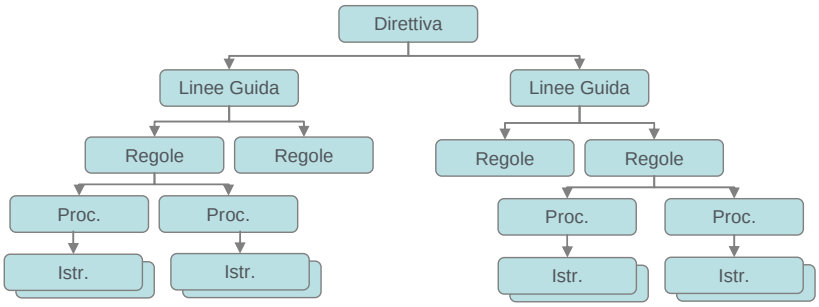


Fonte: nostra elaborazione

Il framework CObIT propone un insieme di processi applicabili all'IT che le imprese devono implementare e formalizzare in maniera adeguata. Questo porta alla predisposizione di un quadro documentale che descriva per ogni processo le attività di controllo necessarie alla sua gestione e presidio. Dal framework di riferimento scelto da Finmeccanica per la gestione dei sistemi informativi di Gruppo, ovvero lo standard CObIT, sono stati selezionati 77 punti di controllo, rispetto ai quali è attivato il processo di analisi che ha generato una serie di direttive, linee guida, regole attuative, procedure ed istruzioni operative, che man

mano sempre più in maniera tecnica e dettagliata, descrivono i processi coinvolti nei 77 punti di controllo e ne designano i controlli operativi (Fig. 4).

Figura 4 - La struttura gerarchica delle linee guida per l'implementazione dell'IT governance in Finmeccanica



Fonte: nostra elaborazione

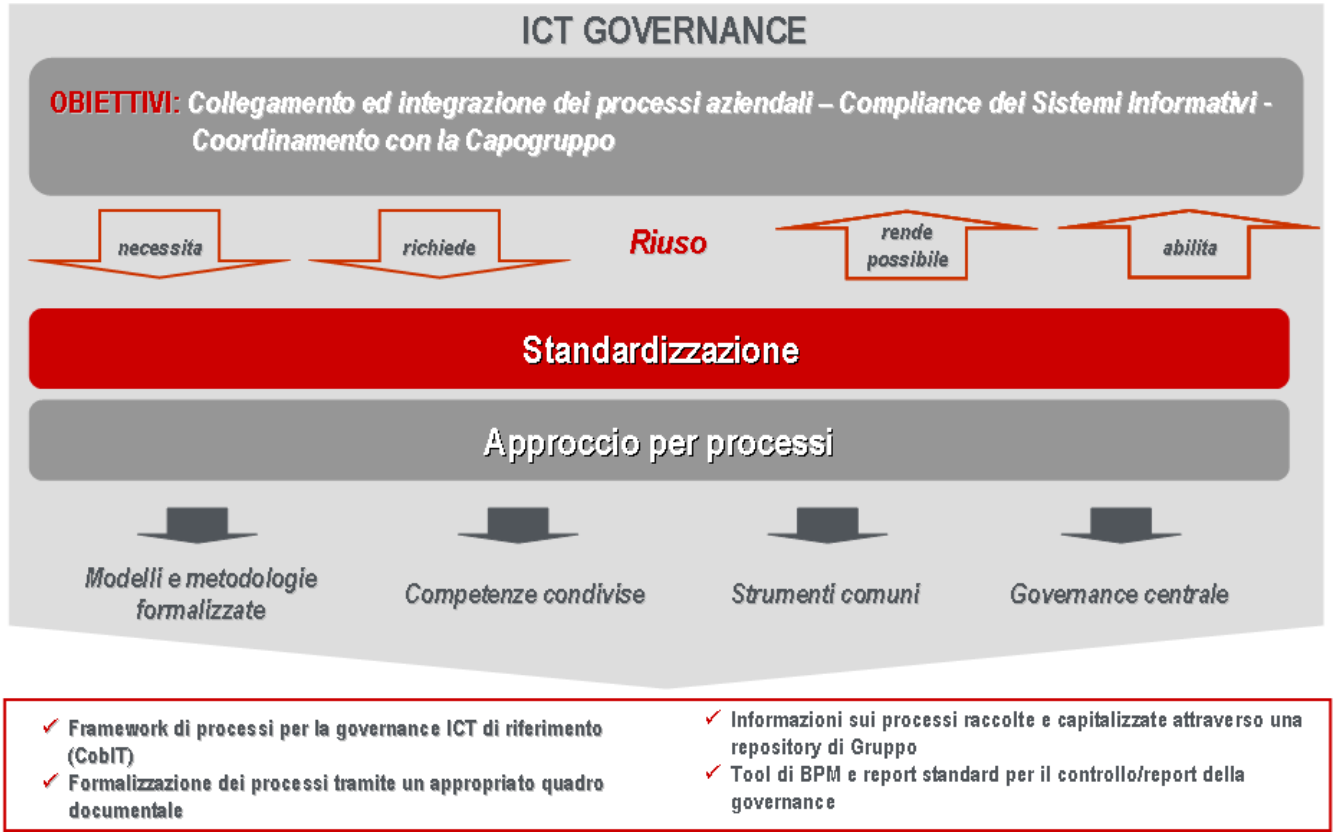
Utilizzando la terminologia CObIT in Finmeccanica questi documenti sono stati divisi tra livello Entity, che governano l'insieme del sistema, livello Application, specificatamente indirizzati allo sviluppo, manutenzione e gestione delle applicazione, e livello Infrastructure per lo sviluppo, manutenzione e gestione delle infrastrutture. I contenuti delle attività rispetto ai tre ambiti sono elencate nella Fig. 5.

Figura 5 - Le attività di IT governance classificate rispetto agli ambiti applicativi

Fonte: nostra elaborazione

In linea con quanto detto all'inizio, in Finmeccanica è stato deciso di utilizzare in maniera integrata alla Governance IT questo set di documenti e non limitarli alla sola compliance delle legge 262, per trarre dall'attività di governo dell'IT benefici più ampi; per cui, ad esempio, i documenti delle politiche di governo dell'IT valgono non solo per i processi che rientrano nel perimetro di applicazione della Legge 262 (generalmente amministrativi), ma per tutte le operazioni IT del Gruppo, sono inoltre utilizzate per altre certificazioni come la ISO9000. L'approccio integrato al governo dell'IT abbraccia quindi tutta l'area IT e conferisce ai sistemi informativi di Finmeccanica un livello qualitativo omogeneo ed elevato. Tale approccio è descritto in Fig. 6.

Figura 6 - L'approccio integrato all'IT governance in Finmeccanica



Fonte: nostra elaborazione

Il modello parte dagli obiettivi dell'IT governance, che non si limitano alla compliance, ma comprendono anche benefici strategici quali l'integrazione dei processi aziendali e il coordinamento di tutte le società del vasto gruppo Finmeccanica. Il pilastro di tale approccio è la standardizzazione dei processi attraverso tutta l'organizzazione del gruppo aziendale, il che permette sistemi informativi omogenei e più facilmente controllabili, nonché il riuso delle procedure e, di conseguenza, notevoli risparmi nelle attività di presidio, integrazione, manutenzione, aggiornamento. Grazie ai modelli formalizzati, alle competenze IT condivise, all'utilizzo di strumenti comuni e ad una forte centralizzazione del governo dei sistemi informativi, è stato possibile realizzare un ambiente IT fortemente integrato e ben documentato, quindi più facilmente presidiabile a minori costi e con maggiori benefici in merito di qualità dei processi aziendali e delle informazioni erogate.

Proprio allo scopo di utilizzare la partenza del programma 262 come opportunità di governance è stato anche deciso di fare un importante attività di "preparazione ai test 262" in modo da permettere alle aziende del gruppo di

allinearsi alle strategie di IT governance e contemporaneamente di rendere più semplice e veloce l'esecuzione di quelli che in gergo degli auditor si chiamano Test IT General Control, che nella sostanza sono i test sui punti di controllo individuati nel frame di processi selezionati dal CObIT.

Nella sostanza è stata data una grande enfasi alla accountability nella sua più completa estensione. Se infatti andiamo a cercare su WIKIPEDIA cosa si intende per accountability troviamo:

"Accountability** is a concept in ethics with several meanings. It is often used synonymously with such concepts as responsibility, answerability, enforcement, blameworthiness, liability and other terms associated with the expectation of account-giving. **As an aspect of governance, it has been central to discussions related to problems in both the public and private (corporation) worlds."

Il sistema costruito ha una forte enfasi sia sulla accountability interna, in termini di definizione di responsabilità e di obblighi, ma anche di capacità e di auto responsabilizzazione nel dare le giuste risposte alle necessità dell'IT aziendale, sia sulla accountability esterna nel senso di capacità di dare trasparenza e risposte responsabili agli stakeholder dell'Azienda.

3. L'IT compliance e il change culturale

Un'attività fondamentale per ottenere un più elevato grado di accountability e responsabilizzazione dei soggetti coinvolti dall'IT governance è stata la gestione della Compliance alla 262 come un programma complesso, in cui la Direzione ICT di Finmeccanica (funzione realizzata dalla società Finmeccanica Group Services - FGS) svolgeva una serie di azioni a favore delle Aziende del Gruppo su indicazione del Dirigente Preposto. Sostanzialmente si tratta di un programma di cambiamento organizzativo più che tecnico, dato che le IT delle Aziende del Gruppo erano già sostanzialmente in linea con i dettami tecnici richiesti dalla Norma.

Essendo un programma di Organizzational Change esso è stato focalizzato su tre iniziative, da ognuna delle quali derivano diverse aree progettuali,:

- la prima essenzialmente tecnologica, che andava o ad aggiornare aspetti di workflow delle applicazioni ricadenti nel perimetro di azione della legge 262 o ad automatizzare alcuni aspetti che richiedevano un forte impegno manuale nel mantenimento della compliance; ad esempio la "Segregation of Duties" richiede uno sforzo continuativo di allineamento con le politiche di responsabilità dei profili SAP, per cui è stata attivata una applicazione SAP GRC che automatizzava questa attività abbassando anche il total cost of ownership;

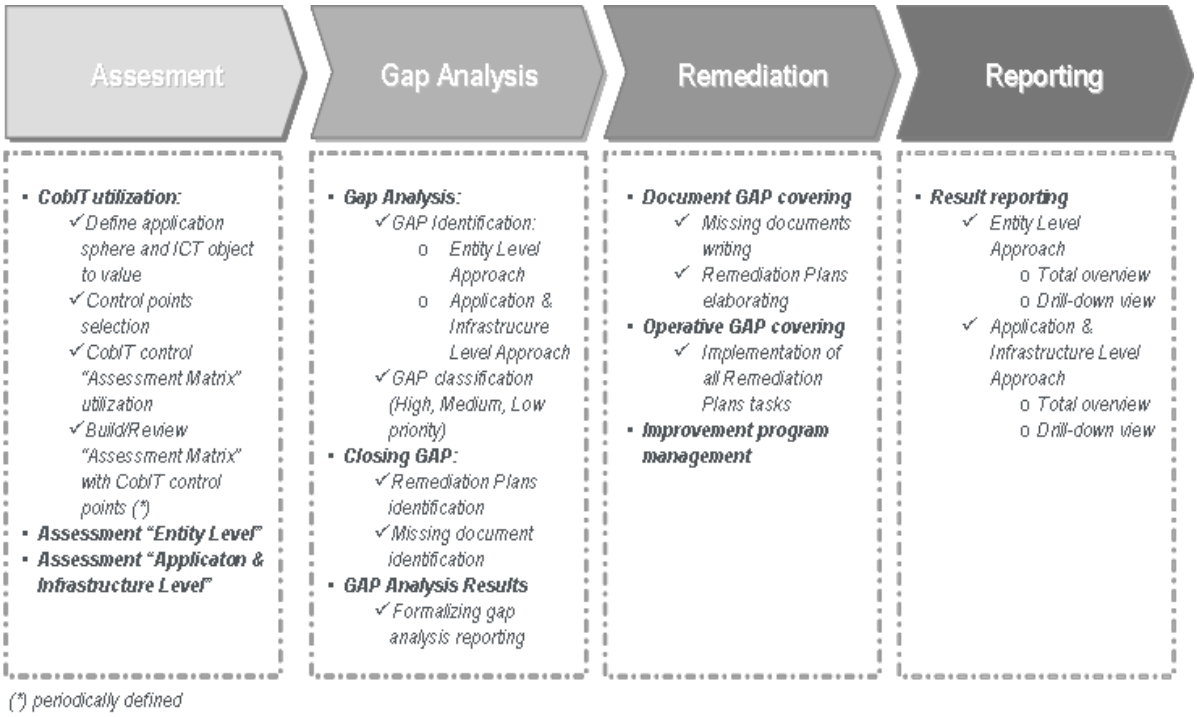
- la seconda essenzialmente normativa, in cui tutte le prassi non completamente formalizzate venivano esplicitate in una forma coerente con i processi ed i punti di controllo CObIT selezionati. Questa attività oltre a razionalizzare le linee Guida di Gruppo per l'IT Governance e Management, implicava l'estensione e la normalizzazione delle procedure operative, almeno sui punti di controllo specificatamente selezionati, su tutte le società del Gruppo;
- la terza area è stata chiamata "Preparazione ai Test ITGC" ed è un classico progetto di change culturale travestito da attività di supporto e di preparazione ai test; infatti mentre operativamente si analizzava lo stato dei processi IT delle varie aziende e si evidenziava la maturità del processo (tramite il Maturità Model) in corrispondenza dei punti CObIT selezionati, monitorando anche le attività di remediation o di miglioramento che spontaneamente l'Azienda si assegnava, nella realtà si implementava un progetto di cambiamento di mentalità sulle responsabilità che l'IT aveva su una serie di processi critici per i suoi stakeholder e sulla capacità di dare risposte certe e chiare avendo definito le giuste responsabilità di azione.

Di seguito ci soffermeremo su questo terzo punto, sicuramente più innovativo in cui si sono utilizzate tecniche di compliance per avere un change organizzativo o in altre parole ottenendo un adeguamento alla compliance avendo usato tecniche di change organizzativo.

4. Preparazione ai test ITGC: approccio top-down e bottom-up

L'iniziativa sviluppata da Finmeccanica nel suo complesso prevedeva 4 fasi, in cui: si partiva da una valutazione/auto valutazione dei sistemi in essere, se ne evidenziavano i gap, si individuavano i rimedi per coprire i gap, si arrivava ad un report finale che servisse primariamente alle stesse aziende come elemento di miglioramento continuativo, alla Direzione ICT di Gruppo come strumento di Governance, alla Corporate (Dirigente Preposto e Internal Audit) come elemento di valutazione della consistenza dell'intera IT di gruppo e come input per la definizione della strategia dei test ITGC (Fig. 7).

Figura 7 - Le fasi di implementazione dei test ITGC in Finmeccanica



Fonte: nostra elaborazione

Le attività di preparazione ai test ITGC in Finmeccanica ormai dal 2007, riguardano tutte le attività di controllo (alta, media e bassa priorità secondo uno schema inizialmente preparato a seconda della criticità dei processi); in effetti sono state definite delle regole ed emessi dei documenti a livello di Gruppo, perché tutto avvenisse nel modo più esplicito possibile (dici prima quello che farai….); per esempio è stata emessa la regola FGS REG-07 "ICT Governance Monitoring Process – Compliance Toolkit", che descrive il processo di assessment della Governance ICT e del sistema di compliance alla 262.

Il processo di valutazione dell'ICT Governance realizzato da FGS è stato utilizzato anche come strumento di supporto per preparare le Aziende del Gruppo ai test ITGC previsti dall'adeguamento alla L.262, ed in particolare, il processo di preparazione è implementato seguendo un duplice approccio Top Down e Bottom Up (Fig. 8).

L'approccio Top Down considera le attività di controllo Entity Level, viene svolta operativamente dalle strutture della Direzione ICT di Gruppo ed è orientato a comprendere il livello di:

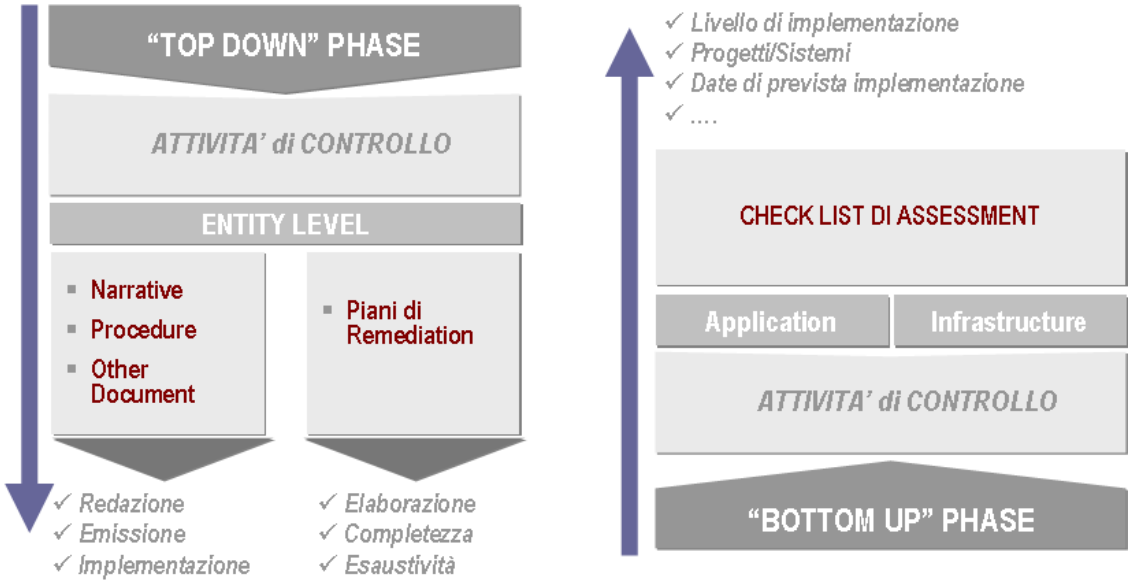
- adeguamento alle linee guida emesse da FGS, attraverso la presenza di tutta la documentazione (Narrative/Procedure, Remediation Plan, Altri Documenti) e lo stato di redazione delle Narrative/Procedure presentate per la copertura dei controlli Entity Level;

- completezza, esaustività e avanzamento dei Remediation Plan e dell'implementazione dei suggerimenti per il miglioramento relativi ai controlli Entity Level.

Nell'approccio Top-Down si utilizzano:

- strumenti per la raccolta delle informazioni;
- algoritmi per la valutazione analitica del disegno del controllo:
- template standard per la restituzione dei risultati ottenuti alle Aziende.

Figura 8 - Il duplice approccio Top Down e Bottom Up

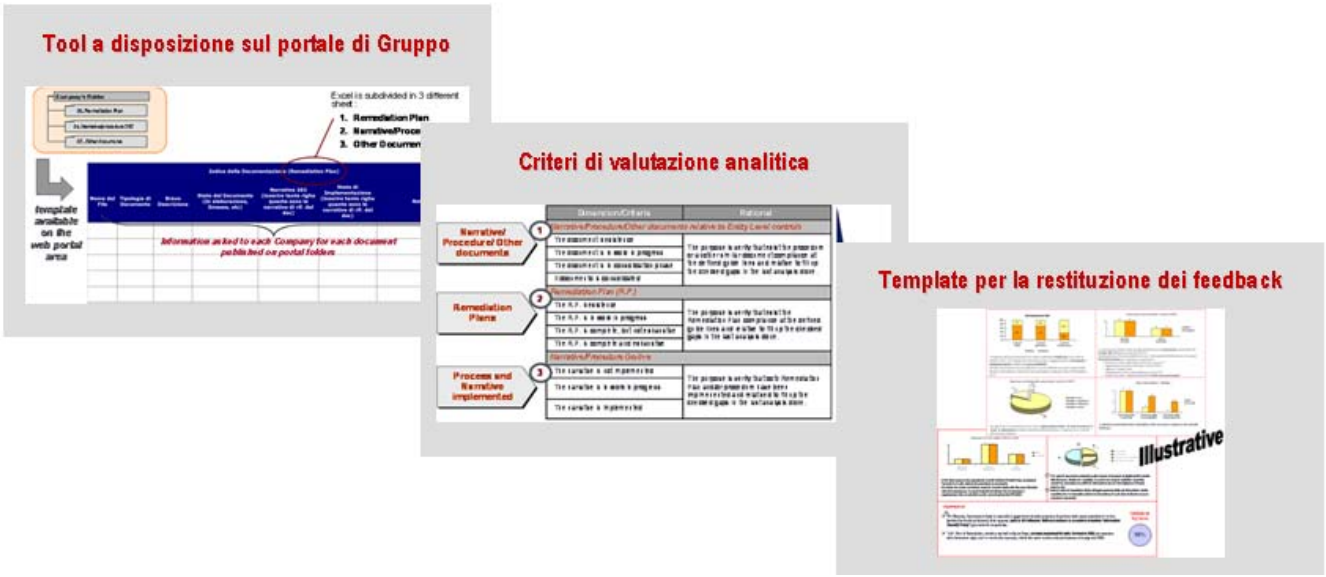


Fonte: nostra elaborazione

Di seguito alcuni deliverable tipici di questa fase (Fig. 9), quali:

- la videata relativa ai tool a disposizione sul portale del gruppo ed accessibili da tutte le società Finmeccanica;
- l'insieme dei criteri di valutazione analitica da applicare ai ITGC;
- la restituzione dei risultati relativi all'applicazione dei controlli.

Figura 9 - Videate relative all'attività di controllo top-down



Fonte: nostra elaborazione

L'approccio Bottom-Up è svolto in self assessment da parte delle ICT delle Aziende del gruppo e considera esclusivamente le attività di controllo Application e Infrastructure Level ed è orientato a comprendere il livello di implementazione dei controlli Application e Infrastructure Level attraverso la conduzione di una autovalutazione per ogni singola azienda del Gruppo Finmeccanica.

Nell'approccio Bottom-Up si utilizzano:

- check list per il self assessment, che saranno compilate dalle Aziende;
- algoritmi per la valutazione analitica dell'implementazione del controllo;
- template standard per la restituzione dei risultati ottenuti alle Aziende.

Tra gli aspetti comuni sia fase Top-Down che in quella Bottom-Up, è stata posta particolare attenzione:

- sulle attività di controllo risultate "Non Applicabili" nel corso di precedenti test ITGC;
- sulle eventuali attività di controllo risultate inefficaci nel corso di precedenti test ITGC;
- sull'implementazione dei suggerimenti per il miglioramento forniti nel corso di precedenti test ITGC.

Nella fase Top-Down, viene posta particolare attenzione:

- su tutti gli aggiornamenti della documentazione (Linee Guida, Regole e Narrative) effettuati in seguito ai test ITGC per la chiusura del bilancio, al fine di valutare eventuali scostamenti dagli obiettivi di controllo CobIT;

- sullo stato di avanzamento dei Piani di Remediation definiti per i test ITGC e sulle eventuali criticità di implementazione;
- sulla presenza delle Business Impact Analysis e sugli aspetti della sicurezza relativa ai Piani di Business Continuity e Disaster Recovery;
- sugli audit sugli outsoucer IT che le Aziende dovranno eseguire, come richiesto dal framework di riferimento CobIT.

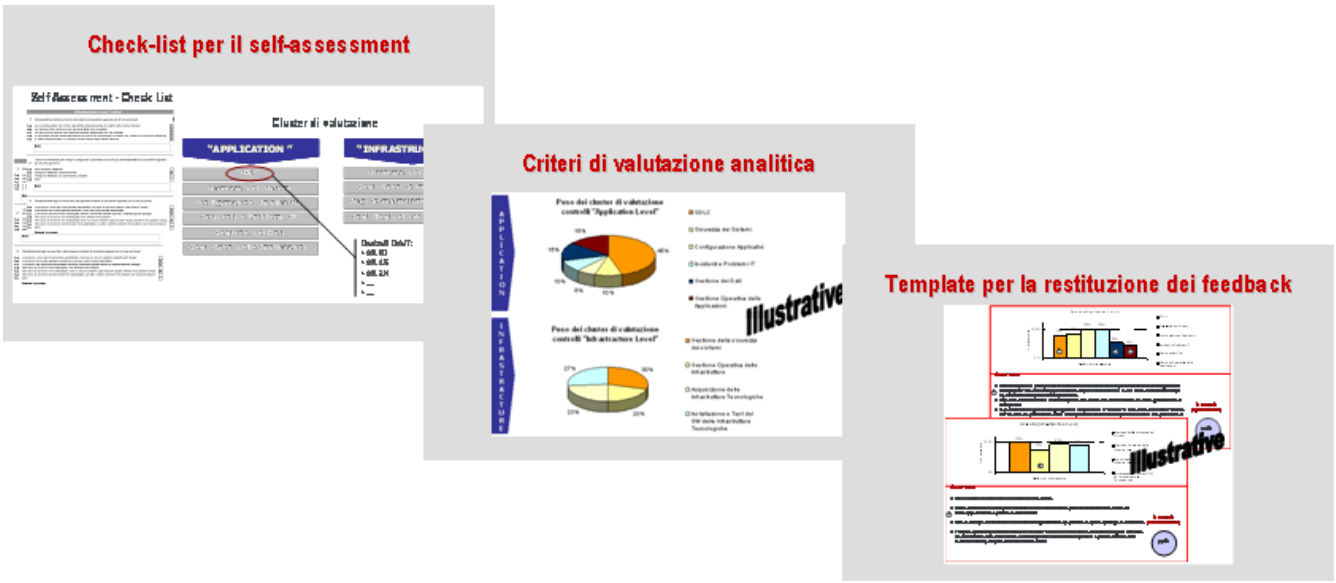
Nella fase Bottom-Up, viene posta particolare attenzione:

- sul monitoraggio, la raccolta e l'analisi dei log dei sistemi e delle applicazioni;
- sul censimento e la gestione del ciclo di vita dei sistemi sviluppati dagli utenti finali;
- sulla classificazione delle informazioni e relativo trattamento.

In Fig. 10 sono rappresentati deliverable tipici della fase Bottom Up, composti da:

- una check-list per effettuare l'autovalutazione;
- l'insieme dei criteri di valutazione analitica;
- il template per la restituzione dei risultati derivanti dall'applicazione dei controlli.

Figura 10 - Videate relative all'attività di controllo bottom-up



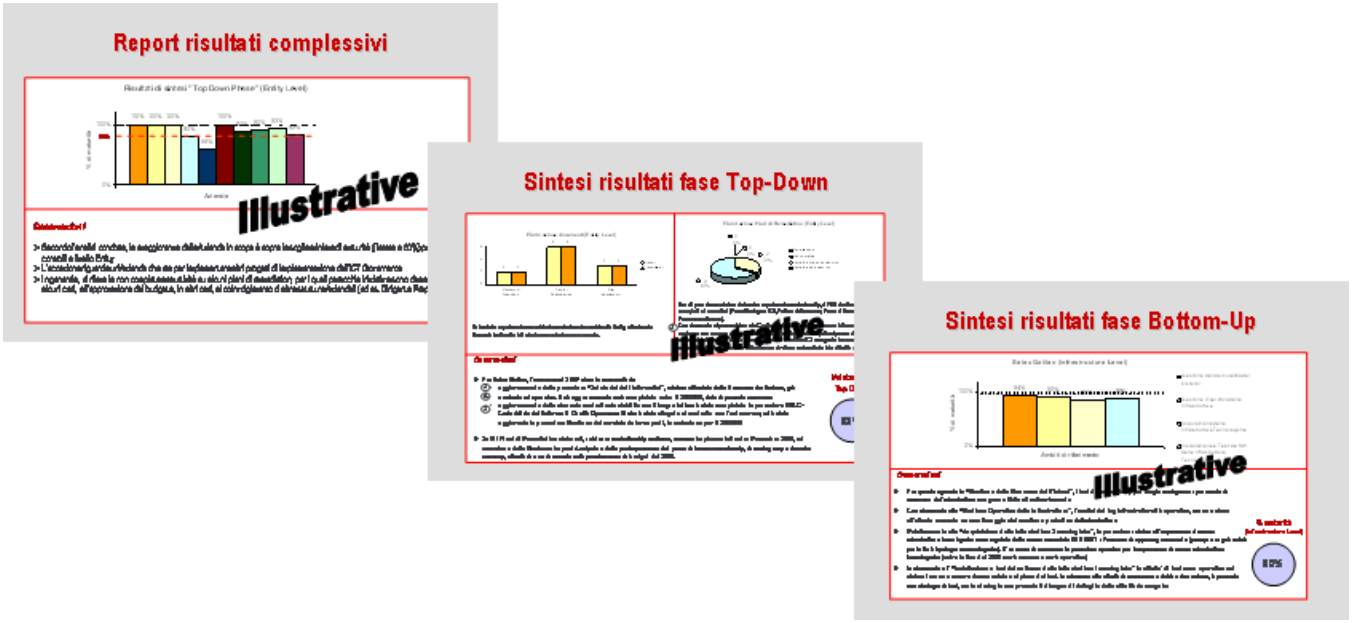
Fonte: nostra elaborazione

Nella fase finale vengono poi prodotti i report necessari ad Aziende, Direzione ICT di Gruppo, Internal Audit di Gruppo e Dirigente Preposto Finmeccanica, alla Governance dell'intero sistema. In particolare:

- report risultati complessivi delle fasi "Top-Down" e "Bottom-Up";
- report di sintesi dei risultati della fase "Top-Down" per azienda;
- report di sintesi dei risultati della fase "Bottom-Up" per azienda;
- analisi complessiva ed input per i successivi Piani Strategici dell'ICT.

Di seguito vengono riportati alcuni documenti esemplificativi del report finale (Fig. 11).

Figura 11 - Videate relative all'attività di controllo complessiva



Fonte: nostra elaborazione

I risultati che questo vero e proprio programma di change organizzativo ha ottenuto sono stati notevoli per Finmeccanica. Essi possono essere così sintetizzati:

- eliminazione di inefficienze nel sistema di controllo;
- eliminazione di duplicazioni di processi;
- migliore utilizzo di funzionalità IT non valorizzate;
- maggiori efficienze nei processi;
- miglioramento della governance e del controllo interno;
- più chiara definizione di ruoli e responsabilità interne;
- maggiore coinvolgimento dei vertici aziendali sulle tematiche del controllo.

Tutto questo è stato ottenuto passando da due momenti:

- una prima fase di disagio e preoccupazione, visto l'impegno e la novità del processo;
- una seconda fase di rivalutazione e riconoscimento di molti elementi positivi che vengono sfruttati come per il processo interno di miglioramento continuo.

In particolare indagini svolte nelle strutture IT delle aziende hanno portato ad evidenziare tutta una serie di vantaggi, quali:

- awareness su processi interni non eccellenti:
  - processi autorizzativi;
  - situazione profili dei workflow;
  - controllo di configurazione delle postazioni di lavoro;
  - verifica e ridefinizione degli obblighi dell'Outsourcer;
- scoperta del mondo delle applicazione End-user:
- ricadute sulla definizione dei Master Service Agreement con gli outsourcer:
  - definizione di uno specifico allegato relativo alla Compliance 262;
- ricadute sul tema della sicurezza:
  - attuazione, completamento messa a regime di progetti relativi alla Business Impact Analysis per il Gruppo e le singole Società;
- individuazione di nuovi servizi comuni e di nuove sinergie di Gruppo possibili.

La risposta data da Finmeccanica alla Compliance alla 262 in termini di "governance" invece che di pura "compliance" ha quindi consentito di creare un processo iterativo i cui benefici si mostreranno nel tempo su tutte le aree della gestione IT, confermando l'assunto per cui è possibile, ed anzi opportuno, sfruttare questo momento di riesame ed implementazione per creare un meccanismo virtuoso di miglioramento continuo.

Stefano Privitera
Responsabile del servizio Metodologie e processi ICT
Finemccanica Group Services
e-mail: stefano.privitera @ finmeccanica.com