L’adozione di COBIT come strumento di IS Governance. Stato dell’arte, risultati e fattori critici di successo nelle esperienze analizzate.

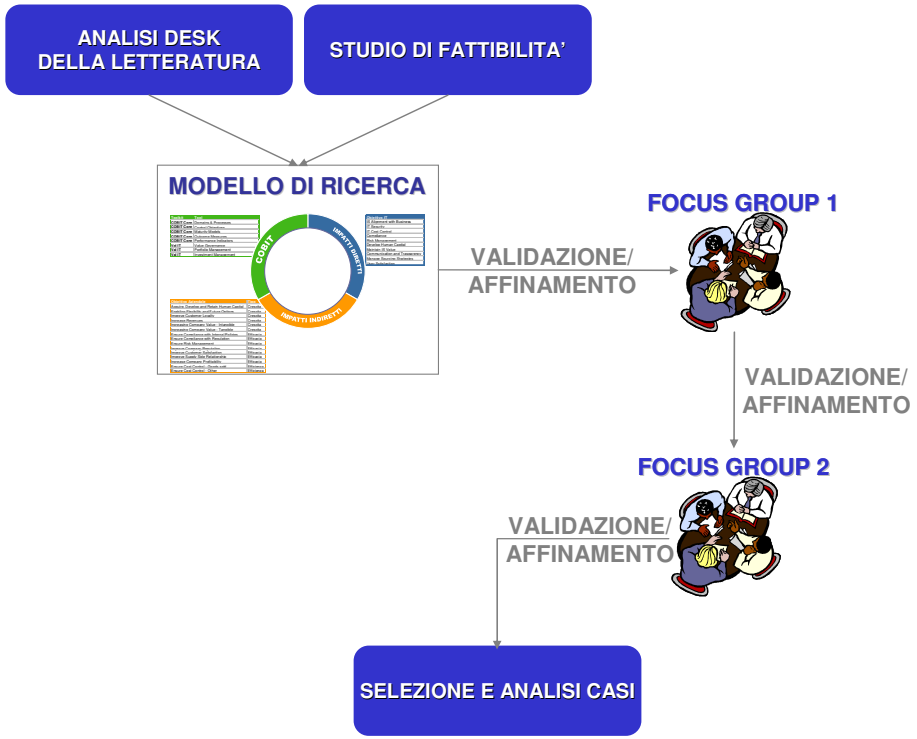
Elisa Pozzoli, Gianluca Salviotti

Agenda

- Premessa
- Il percorso di adozione di COBIT
- I benefici di adozione di COBIT
- Punti di forza, punti di debolezza e aree di criticità
- Conclusioni

Premessa

- I risultati di seguito presentati emergono dai Focus Group e dall'analisi dei casi aziendali
- Le evidenze riportate hanno natura qualitativa e riguardano le esperienze di introduzione di COBIT



Il percorso di adozione di COBIT

Il percorso di adozione di COBIT

(*COBIT Waves* © SDA Bocconi School of Management)

Wave 1 – Compliance

- In questa fase l'adozione di COBIT supporta l'adeguamento normativo
  - In particolare a SOX e 262
- Le prime attività sono finalizzate a introdurre il sistema dei controlli (approccio progettuale)
  - implementazione dei control objectives
  - gestione della relazione con gli auditor
  - set-up di strutture interne deputate al controllo
- Seguono attività di ottimizzazione e affinamento del sistema dei controlli (approccio manageriale)
  - risorse dedicate alle attività di controllo
  - numero di controlli implementati
  - tempo dedicato alle attività di controllo

Wave 2 – Process/Performance improvement

- In questa fase si amplia il numero di attività sottoposte a controllo
- Aumenta la consapevolezza della validità del sistema di controlli proposto da COBIT come strumento di assessment a supporto delle iniziative di miglioramento dell'IT
  - riduzione dei costi operativi,
  - incremento della produttività delle risorse,
  - aumento della soddisfazione degli utenti,
  - miglioramento della sicurezza IT,
  - …
- In questa fase COBIT viene utilizzato in affiancamento ad altri framework che forniscono delle best practices di processo a copertura di aree specifiche

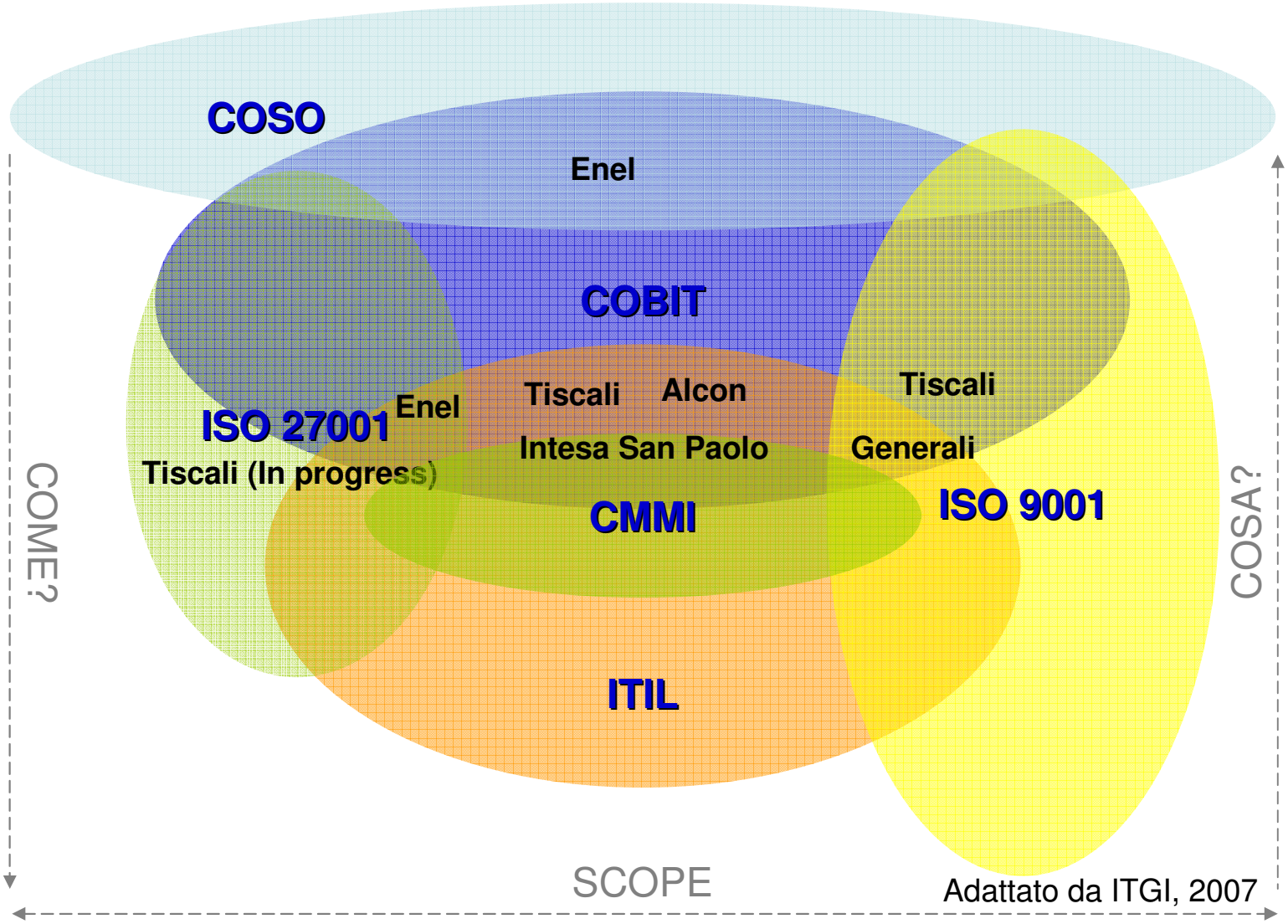
Wave 2 – Process/Performance improvement
Il ruolo di COBIT come meta-framework (1)

- Non sembra esistere un framework di processo che consenta di indirizzare adeguatamente le esigenze delle aziende in termini di IS Governance

- La ricerca conferma la propensione delle aziende all'utilizzo congiunto dei diversi framework di processo disponibili, in funzione dei punti di forza e delle specificità di ciascuno di essi

- COBIT si è rivelato nelle esperienze analizzate un **meta-framework** che ha consentito il dialogo e l'integrazione degli altri IT framework già presenti o successivamente introdotti in azienda
  - COBIT + ITIL nella strutturazione dei processi operativi (dominio DS)
  - Complementarietà di COBIT e ITIL rispetto ad altri framework maggiormente focalizzati sulla qualità aziendale (ISO9001) e sulla sicurezza del sistema informativo (ISO27000)

Wave 2 – Process/Performance improvement
Il ruolo di COBIT come meta-framework (2)



Adattato da ITGI, 2007

Wave 3 – Risk Management

- In questa fase si sperimenta un ulteriore step nell'utilizzo di COBIT

- I controlli COBIT sono utilizzati nella fase di risk assessment per
  - individuare i rischi relativi ai processi IT
  - impostare le azioni di mitigazione del rischio IT
  - ridurre il livello di esposizione al rischio delle attività IT

Wave 4 – Governance Risk & Compliance

- In questa fase la dimensione di processo rappresenta il punto di riferimento fondamentale per valutare
  - la governabilità dell'IT
  - la compliance alle normative
  - il grado di esposizione al rischio dell'IT

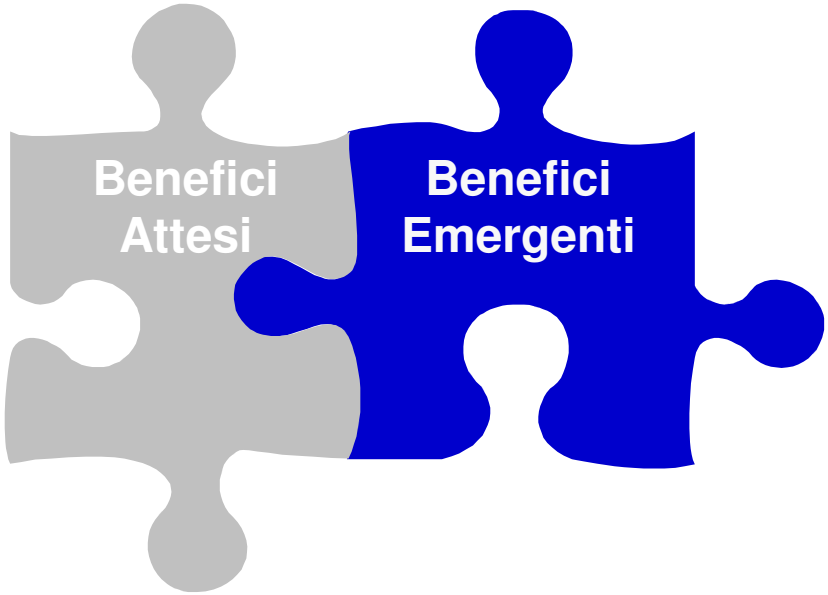
- Approccio riscontrato solo in realtà aziendali in cui l'IT ha un impatto significativo sull'azienda e in cui COBIT è stato utilizzato come uno strumento non solo di audit, ma di IS Governance gestito internamente

Il benefici di adozione di COBIT

I benefici di adozione di COBIT

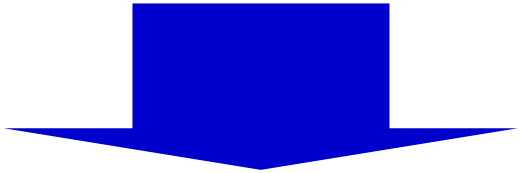
- Nella fase di compliance l'adozione di COBIT (imposta o spontanea) ha l'obiettivo **esplicito** di supportare la risposta dell'IT a specifiche normative (**benefici attesi**)

- Nelle fasi successive emergono opportunità di miglioramento stimolate dalla prima esperienza di introduzione (**benefici emergenti**)



Benefici attesi (1)

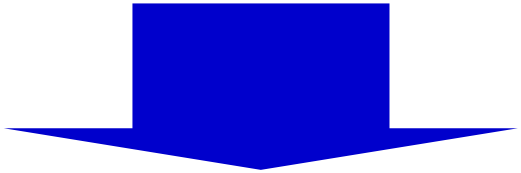
COMPLIANCE



L'adozione di COBIT si conferma un passaggio cruciale nel percorso di implementazione di un modello aziendale di IS Governance in grado di allineare il sistema informativo ai vincoli posti dal contesto esterno

Benefici attesi (2)

"…e se venissero meno i vincoli di compliance?"



L'orientamento è stato quello di mantenere l'utilizzo di COBIT, in quanto il suo contributo è stato ritenuto fondamentale per il governo dei sistemi informativi e, soprattutto, per anticipare alcune nuove necessità di compliance.

Anche dopo il perfezionamento delle operazioni di deregistration, abbiamo optato per mantenere il sistema dei controlli interni, in quanto coerente con le richieste espresse dalla legge n. 262/05

Benefici emergenti (1)

Benefici derivanti dall'adozione di COBIT	Esempi aziendali
Miglioramento dei processi IT	- Esplicitazione di carenze operative e formali nell'IT e individuazione delle aree di miglioramento (Intesa San Paolo) - Preparazione della funzione IT ad erogare servizi IT di qualità al mercato esterno (Tiscali) - Evidenza delle opportunità di ridisegno dei processi IT (Alcon Group) - Miglioramento dei processi IT pre-esistenti (Enel)

Benefici emergenti (2)

Benefici derivanti dall'adozione di COBIT	Esempi aziendali
Miglioramento delle performance operative dell'IT	- Riduzione degli incident e riduzione delle risorse dedicate alle attività di supporto (Intesa San Paolo) - Incremento di efficienza operativa (Tiscali) - Maggior certezza delle attività da svolgere e maggior possibilità di controllare quanto realizzato (Enel)

Benefici emergenti (3)

Benefici derivanti dall'adozione di COBIT	Esempi aziendali
Miglioramento della relazione tra funzione IT e funzioni di Business	- Miglior utilizzo del SW da parte degli utenti (intesa San Paolo) - Migliore allocazione delle risorse aziendali, con focus sulle priorità del cliente (Tiscali) - Responsabilizzazione delle divisioni di business (Tiscali) - Chiara definizione di ruoli e responsabilità reciproche del business e della struttura di Demand e Delivery (Enel)

Benefici emergenti (4)

Benefici derivanti dall'adozione di COBIT	Esempi aziendali
Estensione del perimetro di controllo IT	- Armonizzazione dei diversi processi IT seguiti in azienda (Generali) - Creazione di un glossario condiviso (Enel) - Strutturazione di processi omogenei su tutte le affiliate (Alcon Group)

Benefici emergenti (5)

Benefici derivanti dall'adozione di COBIT	Esempi aziendali
Miglioramento della capacità di reazione dell'IT	- Semplificazione delle attività di Risk Assessment (Enel) - Semplificazione delle operazioni di integrazione di nuove società (Enel)

Punti di forza, punti di debolezza e aree di criticità

Punti di forza e di debolezza di COBIT

Punti di forza	Punti di debolezza
• Ampiezza	• Profondità
• Versatilità di utilizzo	• Ridondanza di alcuni controlli
• Glossario standard	• Comprensibilità di alcuni controlli
• Omogeneità della struttura	
• Integrabilità con altri framework	

Criticità di introduzione vs Fattori Critici di Successo

Criticità di introduzione	Fattori critici di Successo
Resistenza al cambiamento	- Readiness dei Sistemi Informativi a processi di auditing e controllo - Creazione di ruoli ad hoc con responsabilità di applicazione dei controlli (control owner)
Committment aziendale	- Sponsorship dalle funzioni aziendali - Chiara suddivisione delle responsabilità tra business e IT - Legittimazione della funzione SI ad intraprendere azioni correttive su tutto lo scope dei processi IT
Eterogeneità dei processi IT	- Coesione dei team di IS Audit e di IS Governance - Pre-esistenza di un orientamento alla strutturazione dei processi IT

Conclusioni

In generale

- Il framework COBIT è progettato per agevolare l'applicazione di controlli ai principali processi IT e resta fedele alla sua missione, contribuendo, in ognuna delle esperienze di adozione esaminate nella ricerca, a raggiungere l'obiettivo di compliance dell'IT

- I benefici che si affiancano a quello di compliance, non sempre ricercati in modo esplicito dalle aziende, dimostrano come un'adozione matura di COBIT possa condurre a risultati di assoluto interesse per la funzione sistemi informativi e per l'intera azienda

- Occorre comprendere prima di tutto il ruolo di COBIT come framework dei processi IT

Per approfondire

- IS Governance: allineamento strategico e governo dei Sistemi Informativi, Milano, 10-12 marzo 2010

  http://www.sdabocconi.it/it/programmi_di_formazione/7565/
- IS Organization: strutture e processi dei Sistemi Informativi, Milano, 05-07 maggio 2010

  http://www.sdabocconi.it/it/programmi_di_formazione/7702