L'utilizzo di COBIT© in Italia

Quanto è consolidato l'utilizzo di COBIT e per quali scopi è stato adottato? Oltre agli auditor lo utilizza anche il settore ICT? Da quando COBIT è divenuto un riferimento aziendale stabile? Vi sono dei processi aziendali IT che sono analizzati con maggiore frequenza ed altri che non sono considerati? Quali sono le componenti del framework che risultano più utilizzate?

Per rispondere a queste domande è stato predisposto un questionario[1], strutturato distintamente per le società di consulenza, che lo utilizzano per la clientela, e per tutti gli altri tipi di società, che invece lo utilizzano internamente. Inoltre, il questionario è stato suddiviso in due parti: utilizzo di COBIT nell'ambito dell'audit e utilizzo di COBIT nell'ambito della funzione ICT.

Presentiamo nella "Parte I. Aziende non di consulenza" i risultati relativi all'utilizzo di COBIT da parte degli Internal Auditors e da parte del settore ICT. Nella "Parte II. Aziende di consulenza" riportiamo i risultati relativi all'utilizzo di COBIT da parte delle maggiori società di consulenza italiane presso i loro clienti, a supporto di attività di assurance o a supporto degli ICT Manager.

Per facilitare la lettura dei risultati per coloro che conoscono meno il modello, completiamo la presentazione con il riepilogo delle componenti di COBIT 4.1.

Bottom line.

La diffusione di COBIT è stata in continua crescita negli ultimi 10 anni: in tutti i settori economici, fra gli auditor come pure nell'ambito della funzione ICT, con ampia soddisfazione degli utenti.

L'utilizzo delle varie componenti del framework è sempre più esteso: già completo per le società di consulenza, più selettivo per gli internal auditor. L'utilizzo di COBIT per finalità di IT Governance, in senso lato, sta crescendo e gli IT Manager ricorrono a COBIT in particolare per supportare il self assessment, il benchmark, la misura delle performance.

La generalità degli utenti fa riferimento al modello nel suo complesso ed ai "Control Objectives", utilizzando un linguaggio comune compreso dalla community professionale (auditor interni ed esterni, funzione ICT, aziende). Gli strumenti più avanzati sono utilizzati in modo selettivo.

[1] Nel 2008 il Consiglio Direttivo AIEA ha deliberato di effettuare una indagine sull'utilizzo e la diffusione di COBIT in Italia. Il questionario è stato proposto in novembre e dicembre 2008 con il titolo "Quick survey su COBIT". L'adesione ci consente alcune considerazioni di carattere qualitativo. Ringraziamo tutti coloro che hanno contribuito all'iniziativa.

Parte I.
Aziende non di consulenza.

I.1. COBIT e gli IS Auditor.

Sono pervenute una trentina di risposte da società di diversi settori economici. La rappresentatività dei risultati è qualitativa anche se complessivamente stiamo parlando di aziende che occupano quasi 400.000 addetti, 16.000 dei quali sono collocati nella funzione ICT (pari a poco più del 4%). Gli IS Auditor sono più di un centinaio con la presenza di quasi un IS auditor ogni 100 dipendenti della funzione ICT (0,78%).

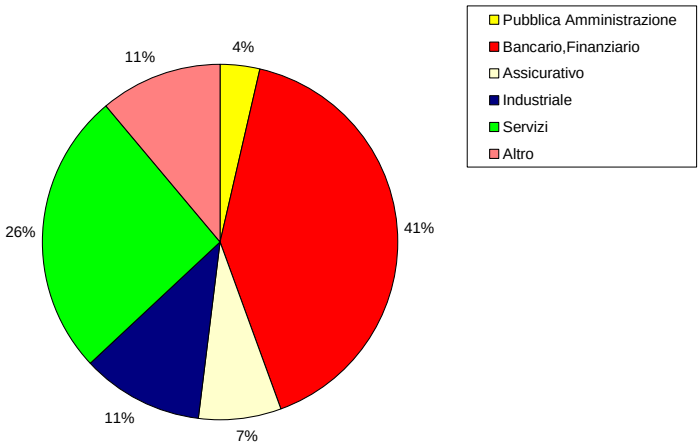

Fig. 1 – Distribuzione delle risposte: per settore economico

Le risposte al questionario indicano in circa 300 gli utilizzatori di COBIT (100 Internal Auditor e circa 200 professionisti di società di consulenza, cfr. Parte II). Ai corsi COBIT AIEA hanno partecipato più di 350 persone. E' nostra opinione che i professionisti che utilizzano COBIT in Italia possano pertanto essere stimati in più di un migliaio, pur con diversi gradi di coinvolgimento ed operatività.

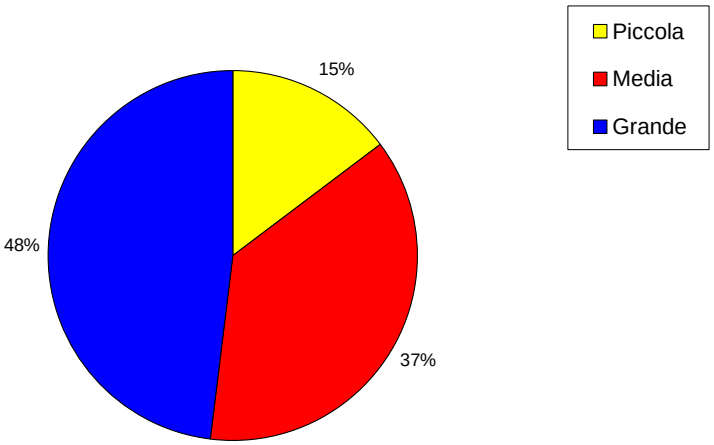

Fig. 2 – Distribuzione delle risposte: per dimensione aziendale

COBIT è ampiamente diffuso fra tutti gli IS Auditor italiani che lo usano ufficialmente nella loro attività. A livello aziendale, circa il 65% delle imprese o gruppi industriali ha un referente COBIT; indicazione di una adozione aziendalmente riconosciuta del modello e di un supporto professionale che si è evoluto passando dalla sperimentazione/progettualità ad una prassi consolidata di controllo.

Il riferimento a COBIT, in Italia e negli ultimi 10 anni, è avvenuto secondo un trend lineare ma interessando settori diversi nei due lustri. Nel periodo 1998-2002 lo utilizzano le aziende di servizi e le banche. Negli anni a seguire lo adottano le aziende industriali o le utility, in particolare quelle soggette alla SOX.

Gli strumenti di supporto sono principalmente "Word ed Excel" (43% delle aziende), ma sono presenti anche COBITONLINE fornito da ISACA (25%), ACCESS (14%) e alcuni tools acquistati o prodotti internamente (18%).

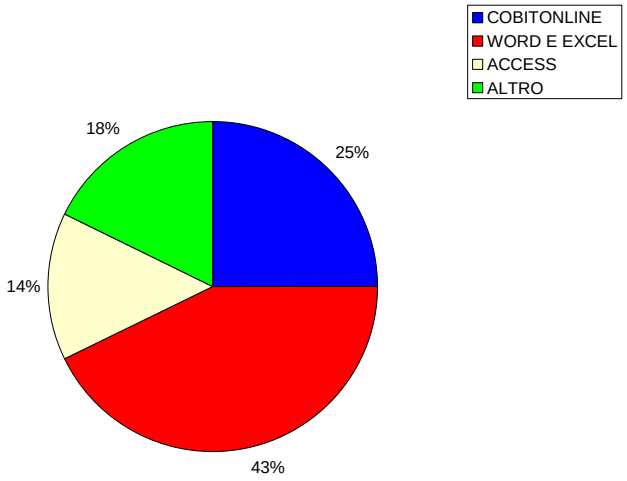

Fig. 3 – Supporti utilizzati

I lavori di internal audit si concentrano sui processi più tradizionali (Sicurezza ed Operation), ma non mancano gli esempi di utilizzo completo relativo a tutti i processi. Il 30% delle aziende (principalmente aziende di medie dimensioni) ha infatti effettuato valutazioni su tutti e 34 processi, e comunque il 51% ha approfondito non meno di 10 processi. Il dominio meno considerato (63% circa delle aziende) è quello relativo al Monitoraggio e Valutazione.

I.2. Gli strumenti proposti da COBIT come sono utilizzati dagli auditor?

Il più conosciuto, utilizzato dalla quasi totalità degli utenti, è costituito dagli "Obiettivi di Controllo". Due terzi delle aziende utilizzano anche le "Assurance Guide" e le "Control Practice". Il 40% circa utilizza le "Metriche" ed i "Maturity Model", mentre solo il 30% sfrutta i "Documenti di Input e Output" e le "Tavole di Responsabilità (RACI)".

I.3. COBIT e la funzione ICT.

L'ICT utilizza COBIT, autonomamente rispetto all'audit, nel 70% delle aziende che hanno risposto al questionario. Fra queste troviamo aziende che appartengono principalmente al settore bancario e dei servizi, uniformemente distribuite per grandezza e con una adozione concentrata negli ultimi 4 anni.

Se gli IS Auditor che usano COBIT sono più di un centinaio, i professionisti della funzione ICT sono quasi una cinquantina. In questo tipo di aziende, dove vi è un referente COBIT nel 50% dei casi, il numero di utenti nel settore ICT appare in crescita e destinato a raggiungere quello degli auditor. COBIT, da strumento di supporto all'attività di assurance, si sta sempre più affermando anche come strumento di supporto all'attività di Compliance svolta dalla funzione ICT e come strumento di supporto all'attività di IT Governance della Direzione ICT. In particolare si rileva come COBIT si sia diffuso presso i CIO e le strutture ICT come strumento che aiuta ad impostare e gestire i processi ICT.

Anche la funzione ICT utilizza come tools principalmente "Word ed Excel", ma è significativa la presenza di prodotti acquistati o realizzati internamente, a dimostrazione dell'utilizzo strutturato e sistematico. Quasi tutte queste le aziende effettuano reporting o analisi che riguardano tutti e 4 i domini di COBIT.

I.4. Quali fra gli strumenti proposti da COBIT sono utilizzati dalla funzione ICT?

Anche presso la Direzione ICT gli "Obiettivi di Controllo" di COBIT sono la parte più conosciuta ed utilizzata. Il settore ICT usa, molto più degli auditor, le "Metriche" (oltre il 50% delle aziende). Medio è l'utilizzo degli altri strumenti, che sono tutti considerati ad esclusione dell'"Assurance Guide".

Il quadro che si delinea è di un comparto informatico che è arrivato ad utilizzare COBIT dopo degli auditor, ma che sfrutta una più ampia gamma di supporti del modello (in particolare quelli dedicati al management) ed appare possedere una buona conoscenza complessiva del modello. Il miglioramento continuo viene indotto da attività di self assessment che permettono di acquisire una buona consapevolezza dei punti di forza e di debolezza, delle opportunità e dei rischi del settore. La maggior diffusione delle metriche, in particolare, indica che il framework non è vissuto come un male necessario, ma come una fonte di strutturazione e miglior governo.

Parte II.

II.1 COBIT e le Aziende di Consulenza.

Sono pervenute dieci risposte, suddivise – da un punto di vista dimensionale – fra 4 società piccole, 1 media e 5 grandi. Le società della prima classe hanno pochi IS Auditor mentre le società "grandi" hanno più di 20 IS Auditor per ciascuna. Il numero di risposte è contenuto, ma riscontriamo sia le maggiori società di revisione al completo sia alcune società minori attive in questo settore. L'adozione risale ai primi anni di disponibilità di COBIT e si satura nel 2004-5, quando il riferimento a questo modello diventa imprescindibile per i progetti di conformità alle norme previste dalla SOX e più in generale dalla Compliance. Tutte queste società hanno un centro di competenza su COBIT ed un referente di coordinamento.

L'utilizzo, sia per assistenza ai clienti per fini di assurance sia su progetti di supporto all'ICT (per questi ultimi i riferimenti sono più recenti), è ampio e copre generalmente tutti e 4 i domini e tutti i processi di COBIT. I progetti sono supportati da vari tools scelti in base alle esigenze della clientela, e viene sfruttata tutta la gamma delle componenti disponibili.

L'approccio è generalmente più ampio ed approfondito rispetto agli auditor interni. Riportiamo solo alcuni risultati interessanti del questionario. Diversamente dagli auditor interni le società di consulenza fanno sempre riferimento, sia per l'assurance sia per la consulenza ICT, ai processi del dominio Monitor and Evaluate. Nell'assurance fanno ricorso in misura maggiore, rispetto agli auditor interni, agli strumenti di più recente introduzione (RACI, Documenti Input/Output) o di misura (Maturity Model e Metriche). Nei progetti ICT lo sfruttamento delle Metriche e dei Maturity Model è sempre presente.

Coordinamento
Orillo Narduzzo, CGEIT, CISA, CISM, Vicepresidente AIEA, Banca Popolare di Vicenza

Analisi e commenti:
Orillo Narduzzo, CGEIT, CISA, CISM, Vicepresidente AIEA, Banca Popolare di Vicenza
Elisa Pozzoli, SDA BOCCONI
Gianluca Salviotti, SDA BOCCONI
Enzo Toffanin, CISA, CISM, Vicepresidente AIEA, DELOITTE

Commenti:
Daniela Bolli, CISA, POSTE Spa, Faculty COBIT di AIEA
Stefano Niccolini, CISA, Federazione Lombarda BCC, Faculty COBIT di AIEA
Leonardo Nobile, CISA, CISM, DELOITTE, Faculty COBIT di AIEA
Alberto Piamonte. ADFOR, Faculty COBIT di AIEA

Milano, agosto 2009.

APPENDICE

COBIT® : *Control Objectives for Information and related Technology*

Il modello di riferimento internazionale per il controllo ed il governo dell'IT.

Cosa è COBIT 4.1?
COBIT 4.1 è:

- un modello internazionale che unifica e integra i principali standard per l'IT, compresi ITIL, CMMI, e ISO17799,
- il risultato di 15 anni di ricerche e cooperazione tra esperti manager e professionisti dell'IT,
- uno strumento per la compliance.

Quali benefici si possono ottenere utilizzando COBIT?
Eccone alcuni:

- un linguaggio comune fra il personale IT e quello non IT
- la possibilità di capire cosa fa l'IT per i manager aziendali
- una miglior comprensione di come l'IT e l'azienda possono lavorare assieme per completare con successo le iniziative IT
- un miglior allineamento dell'IT basato su una chiara comprensione delle esigenze aziendali
- un servizio IT migliore
- un servizio IT più efficiente
- rischi e costi operativi ridotti
- una gestione dell'IT più efficace

COBIT è strutturato in 4 Domini e 34 Processi.

PIANIFICAZIONE E ORGANIZZAZIONE (PO)

- 10 processi che riguardano la formulazione delle strategie e delle tattiche; l'individuazione di come l'IT può meglio contribuire al raggiungimento degli obiettivi aziendali; la pianificazione, comunicazione e realizzazione della visione strategica; la costruzione di una appropriata organizzazione e di una efficace infrastruttura tecnologica.

ACQUISIZIONE E REALIZZAZIONE (AI)

- 7 processi che concernono l'identificazione, lo sviluppo o l'acquisizione, la realizzazione e l'integrazione nei processi aziendali delle soluzioni IT e comprendono anche la manutenzione delle applicazioni per assicurare che le soluzioni continuino a soddisfare gli obiettivi aziendali

EROGAZIONE ED ASSISTENZA (DS)

- 13 processi sull'erogazione dei servizi IT, inclusa la sicurezza e la continuità dei dati e delle infrastrutture operative

MONITORAGGIO E VALUTAZIONE (ME)

- 4 processi che inquadrano il monitoraggio del sistema: la gestione delle prestazioni, il monitoraggio del sistema di controllo interno, la conformità ai regolamenti, il soddisfacimento dei requisiti di governo.

Componenti di COBIT

Le componenti sono integrate nel modello e sono specifiche per ciascuno dei 34 processi.

ASSURANCE GUIDE

- Descrive per ciascun Obiettivo di Controllo le modalità con le quali effettuare la verifica del disegno e dell'efficacia del sistema di controllo interno

CONTROL PRACTICE

- Indica quali sono le pratiche di controllo generalmente adottate per gestire opportunamente le attività individuate da ciascun obiettivo di controllo

DOCUMENTI DI INPUT E OUTPUT

- Per ogni processo sono individuati i documenti che provengono da altri processi, quelli prodotti o aggiornati nello specifico processo, quelli forniti ad altri processi

MATURITY MODEL

- Descrive i cinque livelli del grado di strutturazione di ciascun processo ed è la base per il benchmark con le altre aziende

METRICHE

- Relativamente agli obiettivi aziendali ed a quelli IT, ai processi ed alle attività principali viene indicato quali metriche sono generalmente utilizzate per misurare efficacemente le performance

OBIETTIVO DI CONTROLLO

- Specifica quale è la prassi di controllo opportuna per ciascun contesto selezionato nell'ambito di ogni processo

TAVOLA DI RESPONSABILITA' (RACI)

- Individua le attività principali e mappa le responsabilità sulle figure professionali tipiche di una struttura aziendale ICT