



Leading the IT Governance Community

COBIT

4.1

**Versione
Italiana**

Framework
Control Objectives
Management Guidelines
Maturity Models

COBIT®

4.1

Traduzione italiana



Capitolo di Milano

Maggio 2007

Versione originale

pubblicata dall'IT Governance Institute™

Maggio 2009

Traduzione italiana a cura di

Associazione Italiana Information Systems Auditors – AIEA

Capitolo di Milano di ISACA

INGLESE

COBIT®: Control Objectives for Information and related Technology 4.1 (COBIT 4.1) is translated into Italian from the English language version of COBIT 4.1 by the Milan Chapter of the Information Systems Audit and Control Association (ISACA) with the permission of the IT Governance Institute. The Milan Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

©1996, 1998, 2000, 2005, 2007 IT Governance Institute (ITGI).

All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system, or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), without the prior written authorization of ITGI.

ITGI created COBIT 4.1 (“Work”) primarily as an educational resource for controls professionals. ITGI makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, the controls professional should apply his or her own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

ITALIANO

Autorizzazione

COBIT®: Control Objectives for Information and related Technology 4.1 (COBIT 4.1) è tradotto in lingua italiana dalla versione inglese di COBIT 4.1 a cura del Capitolo di Milano di Information Systems Audit and Control Association (ISACA) con l’autorizzazione dell’IT Governance Institute. Il Capitolo di Milano si assume la sola responsabilità della accuratezza della traduzione e della aderenza alla versione originale.

Copyright

© 1996, 1998, 2000, 2005, 2007 IT Governance Institute (ITGI). Tutti i diritti sono riservati. Nessuna parte di questa pubblicazione può essere usata, copiata, riprodotta, modificata, distribuita, pubblicata con sistemi video, memorizzata su sistemi di pubblicazione, o trasmessa in qualsiasi forma e con qualsiasi mezzo (elettronico, meccanico, di fotocopiatura, di memorizzazione o di altro tipo), senza la preventiva autorizzazione scritta dell’ITGI.

Disclaimer

ITGI ha prodotto COBIT 4.1 (Prodotto) innanzitutto come una risorsa formativa per gli esperti del controllo. ITGI non assicura alcun risultato dovuto all’utilizzo del Prodotto. Il Prodotto non deve essere considerato come comprensivo di tutte le informazioni, procedure e test relativi ai controlli, o alternativo ad altre informazioni, procedure e test che ragionevolmente possono permettere di ottenere lo stesso risultato. Nel determinare l’applicabilità di ciascuna specifica informazione, procedura o test, l’esperto dei controlli deve valutare sotto la propria responsabilità la particolare circostanza influenzata dallo specifico sistema o dallo specifico ambito tecnologico.

Avvertenze

Pubblicazione edita in Italia con autorizzazione di ITGI. La traduzione italiana è curata da AIEA – Associazione Italiana Information Systems Auditors - ISACA - Capitolo di Milano. Per usi commerciali si suggerisce di abbinare il testo italiano con quello inglese.

AIEA – Associazione Italiana Information Systems Auditors
20141 Milano— Via Valla, 16
Tel 0039 02 84742.365- Fax 0039 02 84742.366
E-mail: aiea@aiea.it; Sito: www.aiea.it
P.IVA 10899720154 C.F. 97109000154

AIEA – Associazione Italiana Information Systems Auditors (Capitolo di Milano di ISACA) – ringrazia tutte le aziende di appartenenza dei componenti il Gruppo di Ricerca per la disponibilità e per il valore del contributo apportato dai rispettivi rappresentanti. A questi ultimi un particolare ringraziamento per l’impegno, la professionalità dimostrate e per aver contribuito al successo dell’iniziativa.

Coordinamento

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

Gruppo di Ricerca

Stefano Niccolini, CISA, CISM	Federazione Lombarda BCC
Leonardo Nobile, CISA	Deloitte
Alberto Piamonte	Ing. Alberto Piamonte
Marco Salvato, CGEIT, CISM,CISA	KPMG
Giulio Spreafico, CGEIT,CISA,CISM	Studio Spreafico

AVVISO

Il Gruppo di Ricerca sollecita i lettori a segnalare correzioni e miglioramenti scrivendo alla Segreteria AIEA all’indirizzo: aiea@aiea.it; sottolinea inoltre l’opportunità di utilizzare nella pratica le due versioni, italiana ed inglese, con il testo a fronte.



Capitolo di Milano

Pagina intenzionalmente bianca

EXECUTIVE OVERVIEW

SINTESI PER LA DIREZIONE

Per molte imprese, l'informazione e la tecnologia che la supporta rappresentano il bene più prezioso, ma spesso il meno compreso. Le imprese di successo invece riconoscono il contributo positivo dell'Information Technology e lo utilizzano per accrescere il valore per gli stakeholder. Queste imprese, inoltre, comprendono e gestiscono i rischi associati, come la crescente esigenza di conformità alle normative e la dipendenza critica di molti processi aziendali dall'Information Technology (IT).

Il bisogno di garanzie sul valore generato dall'IT, la gestione dei rischi correlati all'IT ed i sempre maggiori requisiti relativi al controllo sulle informazioni sono finalmente compresi come elementi chiave per la gestione dell'impresa. Valore, rischio e controllo costituiscono la parte centrale dell'*IT Governance*.

Il governo dell'IT è responsabilità dei dirigenti e del Consiglio di Amministrazione ed è costituita da una direzione (leadership), da una struttura organizzativa e da processi che assicurano che l'IT di un'impresa sostenga e sviluppi le strategie e gli obiettivi aziendali.

Inoltre, l'IT Governance integra e istituzionalizza le best practice che assicurano che l'IT supporti gli obiettivi aziendali. Il governo dell'IT aiuta l'impresa a trarre il massimo beneficio dal proprio sistema informativo, massimizzando i benefici, cogliendo le opportunità ed acquisendo vantaggi competitivi. Tali risultati richiedono un *framework* per il controllo dell'IT che sia coerente e supporti sia l'*Internal Control – Integrated Framework* predisposto dal Committee of Sponsoring Organization of the Treadway Commission's (COSO's), cioè il quadro di riferimento per il controllo ampiamente accettato per il governo dell'impresa e la gestione del rischio, sia analoghi modelli conformi ad esso.

Le aziende devono assicurare che il proprio patrimonio informativo soddisfi i requisiti di qualità, affidabilità e sicurezza, così come avviene per tutti i loro beni. Il management, inoltre, deve ottimizzare l'uso delle risorse IT disponibili che comprendono i sistemi applicativi, le informazioni, le infrastrutture ed il personale. Per far fronte a tali responsabilità, come pure per perseguire i propri obiettivi, il management deve conoscere lo stato dell'architettura informatica della propria impresa e decidere quale livello di governo e di controllo intenda assicurare.

Il *Control Objectives for Information and related Technology* (COBIT®) fornisce le cosiddette *good practice* in un quadro di riferimento fatto di domini e di processi e presenta le attività in una struttura gestibile e logica. Le *good practice* contenute in COBIT sono condivise dagli esperti e riguardano principalmente il controllo piuttosto che gli aspetti operativi. Tali prassi possono aiutare ad ottimizzare gli investimenti nell'IT, ad assicurare l'erogazione dei servizi ed a fornire un metro di valutazione per capire quando le cose non vanno per il verso giusto.

Perché l'IT sia in grado di erogare i propri servizi con successo rispetto ai requisiti aziendali, il management deve adottare un modello per il sistema di controllo interno. Il framework di controllo proposto in COBIT risponde a tali necessità attraverso:

- l'individuazione di un collegamento con i requisiti aziendali;
- la strutturazione delle attività IT secondo un modello di processo generalmente accettato;
- l'identificazione delle principali risorse IT su cui fare leva;
- l'individuazione del livello di controllo atteso.

L'orientamento al business di COBIT si estrinseca nel collegare gli obiettivi tipici aziendali con quelli IT, nel fornire metriche e modelli di strutturazione per misurare il perseguimento di questi obiettivi, nell'identificare le responsabilità attribuite alle persone di riferimento dei processi aziendali e dei processi IT.

L'approccio per processi di COBIT è illustrato da un modello che suddivide l'IT in 4 domini e 34 processi coerente con le aree di responsabilità relative a pianificazione, realizzazione, erogazione e monitoraggio, fornendo una visione completa dell'IT. Il concetto di architettura aziendale aiuta ad identificare le risorse essenziali per il successo dei processi, cioè le applicazioni, le informazioni, l'infrastruttura ed il personale.

Riassumendo, al fine di fornire le informazioni di cui l'azienda ha bisogno per raggiungere i propri obiettivi, le risorse IT devono essere gestite da un insieme di processi naturalmente raggruppati.

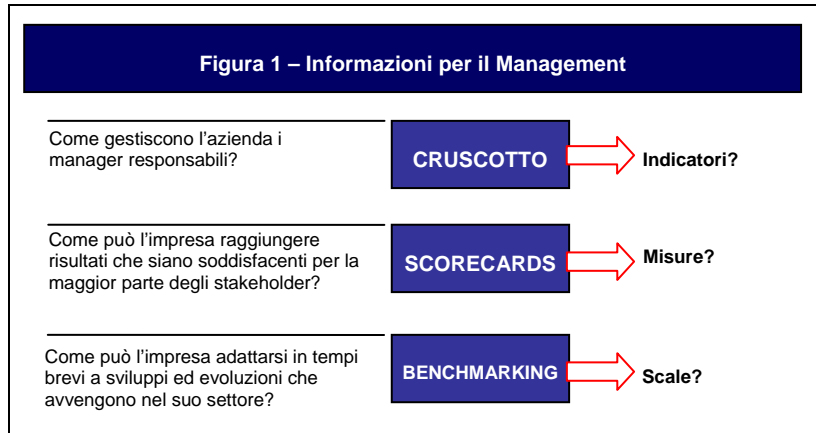
Ma l'impresa, come tiene l'IT sotto controllo in modo che esso fornisca le informazioni di cui l'impresa stessa necessita? Come gestisce il rischio e mantiene sicure le risorse IT da cui è così dipendente? Come fa l'impresa ad assicurare che l'IT raggiunga i propri obiettivi nel mentre supporta il business?

Innanzitutto, il management ha bisogno di obiettivi di controllo che individuino gli obiettivi finali che derivano dall'implementare politiche, piani e procedure, strutture organizzative tali da garantire con ragionevole certezza che:

- gli obiettivi aziendali siano raggiunti,
- gli eventi indesiderati siano evitati o rilevati e corretti/superati.

In secondo luogo, vista la complessità delle situazioni, il management è costantemente alla ricerca di informazioni sintetiche e tempestive che gli permettano prendere velocemente ed efficacemente le difficili decisioni in materia di valore aggiunto, rischi e controlli. Ma cosa deve essere misurato, e come? Le imprese necessitano di una misura oggettiva della situazione attuale e delle aree di miglioramento, e hanno bisogno di strumenti direzionali per monitorare tale miglioramento.

La **Figura 1** mostra alcune domande frequenti e gli strumenti informativi utilizzati dal management per avere le risposte, ma questi cruscotti hanno bisogno di indicatori, le *scorecard* hanno bisogno di misure, ed il *benchmarking* ha bisogno di una scala di confronto.



Una risposta a queste richieste di determinare e monitorare l'appropriato livello di controllo e di performance per l'IT si trova nelle definizioni che COBIT fornisce per:

- **il Benchmarking** delle capacità e delle performance dei processi IT, espresso in termini di modelli di strutturazione, derivati dal Software Engineering Institute's Capability Maturity Model (CMM);
- **gli obiettivi e le metriche** dei processi IT per stabilire e misurare i loro risultati e le loro performance, basati sui principi della *balanced business scorecard* di Robert Kaplan e David Norton;
- **gli obiettivi delle attività** per tenere sotto controllo questi processi, basati sugli obiettivi di controllo di COBIT.

La valutazione della capacità dei processi basata sui modelli di strutturazione di COBIT è una parte cruciale dell'implementazione dell'IT Governance. Dopo aver identificato i processi ed i controlli IT critici, l'utilizzo dei modelli di strutturazione consente di identificare e riportare al management le opportunità di miglioramento della capacità di questi processi. Per portare questi processi al grado di capacità desiderato si possono poi sviluppare specifici piani di azione.

COBIT è pertanto funzionale alla definizione di un sistema di IT Governance (Figura 2) perché fornisce un modello per assicurare che:

- l'IT sia allineato con le strategie dell'azienda;
- l'IT consenta la gestione delle funzioni aziendali e ne massimizzi i benefici;
- le risorse IT siano usate responsabilmente;
- i rischi IT siano gestiti opportunamente.



La misurazione delle performance è essenziale per il governo dell'IT. Tale attività è supportata da COBIT ed include la definizione ed il monitoraggio di obiettivi misurabili relativi ai servizi (risultati attesi) dei processi IT e alle modalità di erogazione (capacità e performance del processo). Diverse indagini hanno identificato che la carenza di trasparenza nei costi, nel valore e nei rischi dell'IT è uno dei fattori più importanti che porta all'introduzione dell'IT Governance. Infatti, la trasparenza si raggiunge principalmente attraverso la misurazione delle performance, mentre le altre aree forniscono solo un contributo.

Le aree in cui è suddivisa l'IT Governance descrivono gli ambiti che l'alta direzione deve considerare per gestire l'IT all'interno dell'azienda. La gestione operativa utilizza dei processi per organizzare e gestire le attività IT di tutti i giorni. COBIT fornisce un modello generalizzato che rappresenta tutti i processi normalmente presenti nelle strutture IT, fornendo un modello di riferimento comune che possa essere compreso sia dai manager dell'IT sia dai manager degli altri settori aziendali. Il modello dei processi di COBIT è stato mappato sulle aree dell'IT Governance (vedi appendice II) creando un collegamento fra le informazioni per la gestione, che servono ai manager più operativi, e quelle che sono attese dall'alta direzione per il governo.

Per conseguire una governance efficace, la direzione si aspetta che i controlli vengano definiti dai manager operativi all'interno di uno schema di riferimento predefinito e valido per tutti i processi IT. Gli obiettivi di controllo dell'IT previsti da COBIT sono organizzati per processi. Pertanto il modello fornisce un chiaro legame tra i requisiti di governance, i processi ed i controlli dell'IT.

COBIT mira a definire gli aspetti necessari per conseguire un adeguato livello gestionale e di controllo dell'IT ed ha un approccio di alto profilo. COBIT è stato allineato ed armonizzato con altri più dettagliati standard e best-practice di riferimento per l'IT (vedi appendice IV) e funge da integratore di queste differenti linee guida, sintetizzando i principali obiettivi sotto un unico cappello che funge da modello e che è collegato anche con i requisiti aziendali e di governance.

COSO (e analoghi schemi di riferimento per la conformità) è generalmente accettato come il modello per il controllo interno delle imprese. COBIT è il modello per il controllo interno dell'IT generalmente accettato.

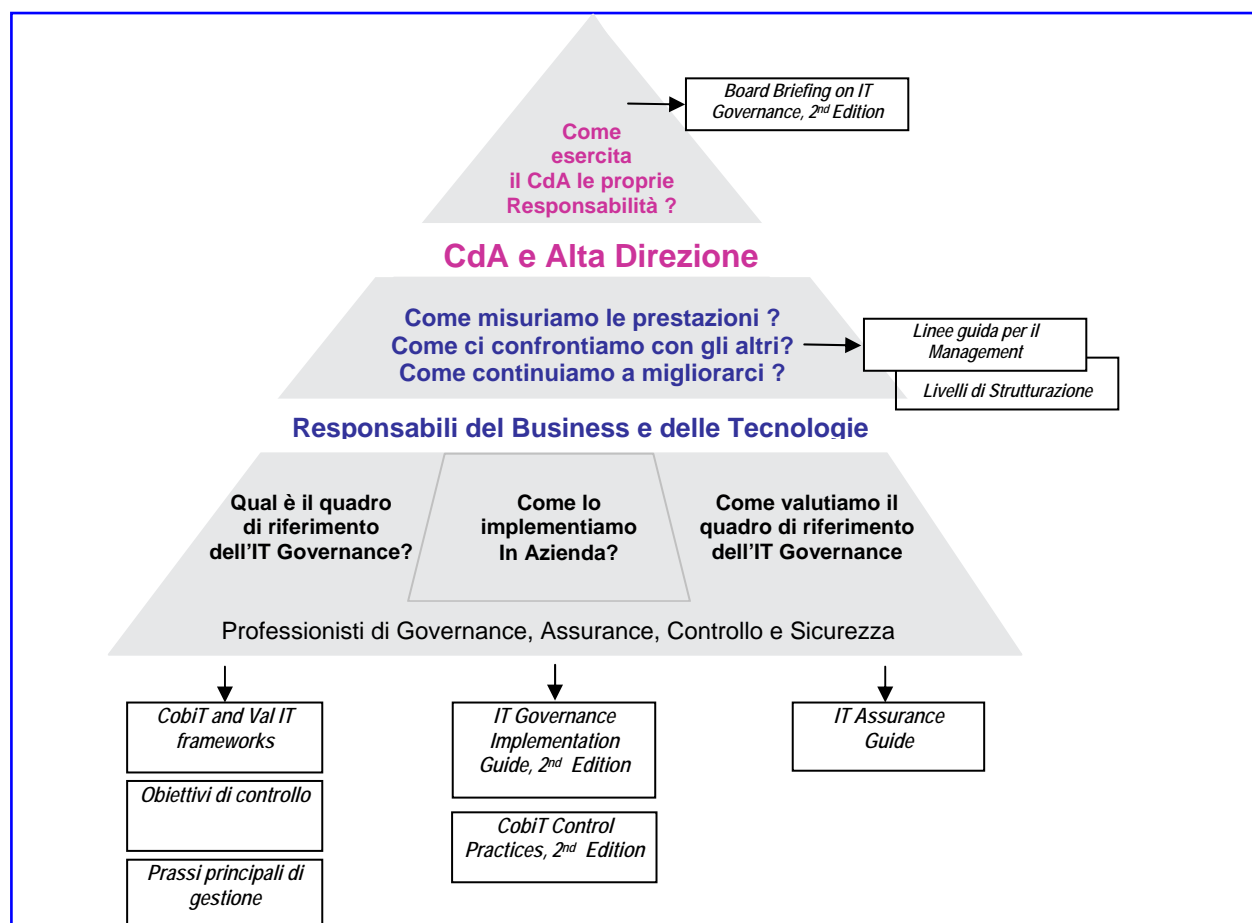


Figura 3 – Schema dei contenuti di COBIT ⁽¹⁾

COBIT 4.1

Le componenti di COBIT sono strutturate su tre livelli (vedi figura 3) progettati per aiutare:

- l'alta direzione e il consiglio di amministrazione,
- i manager dell'IT e degli altri settori aziendali,
- i *professional* che si occupano di governance, assurance, controllo e sicurezza.

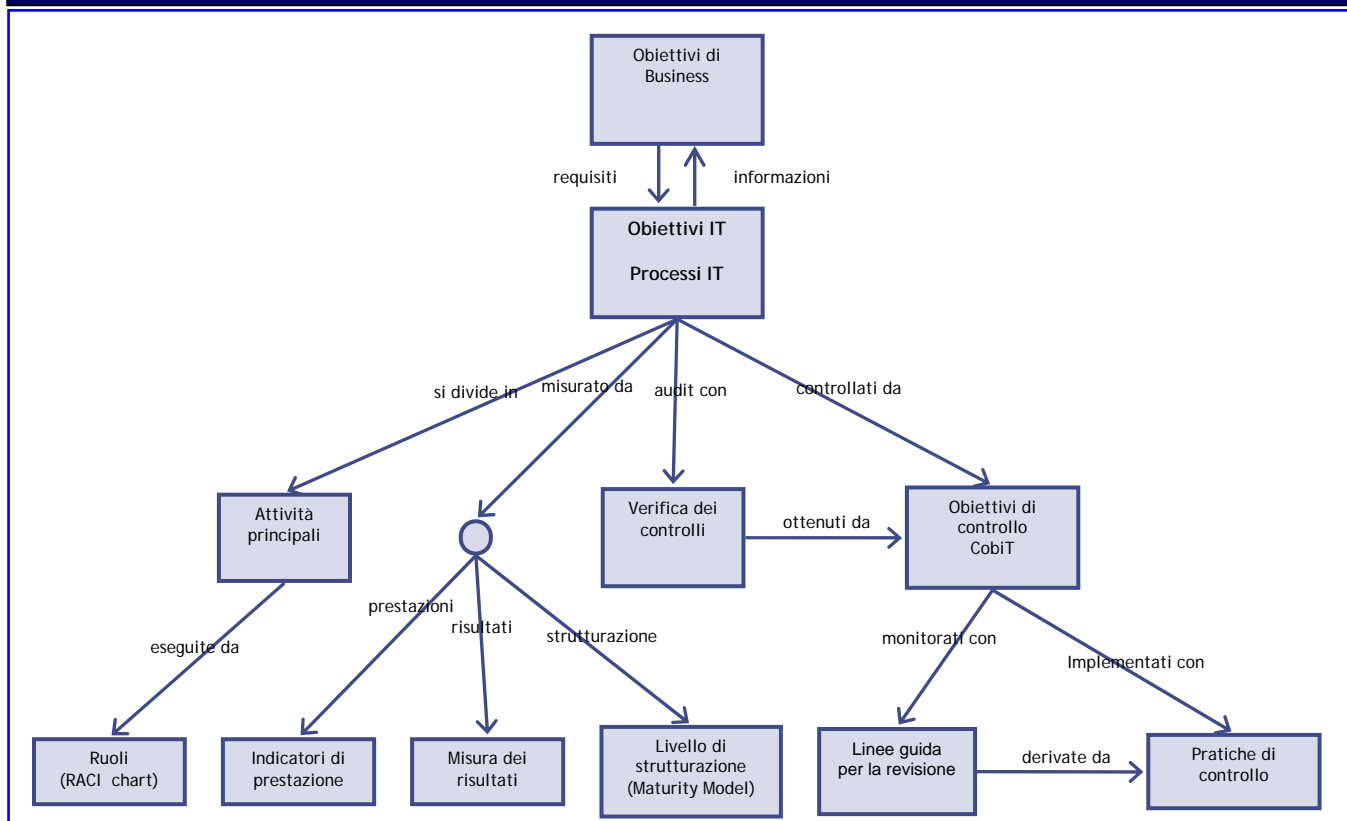
In sintesi, fra le componenti di COBIT vi sono:

- *Board Briefing on IT Governance, 2nd Edition* – Aiuta i dirigenti a comprendere perchè è importante il governo dell'IT, quali sono le sue problematiche e quale è la loro responsabilità nel gestirlo.
- *Management Guidelines, Maturity models* – Aiuta ad attribuire le responsabilità, misurare le performance, confrontarsi con gli altri e superare i punti di debolezza relativi alla capacità produttiva dei processi.
- *Framework* – Struttura gli obiettivi di governo dell'IT e le best-practice in domini e processi IT e li collega ai requisiti aziendali.
- *Control objectives* – Presenta un elenco completo di requisiti di alto livello che deve essere considerato dai responsabili per controllare efficacemente ciascun processo IT.
- *IT Governance Implementation Guide: Using COBIT® and VAL IT, 2nd Edition* – Fornisce un percorso generalizzato per implementare il governo dell'IT utilizzando le componenti di COBIT e di Val IT.
- *COBIT® Control practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition* – E' una guida per motivare l'introduzione dei controlli e per individuare le modalità più opportune per realizzarli
- *IT Assurance Guide: Using COBIT®* – Fornisce delle linee guida su come COBIT può essere usato per facilitare un'ampia gamma di attività di verifica, in particolare per gli opportuni test relativi a tutti i processi IT ed i loro obiettivi di controllo.

Le componenti di COBIT sono illustrate nella figura 3 che evidenzia i principali utenti, le loro problematiche riguardanti l'IT Governance e le componenti che sono generalmente utilizzabili per fornire una risposta. Nella figura vi sono ulteriori componenti specifiche per particolari ambiti quali la sicurezza o le PMI.

Tutte queste componenti di COBIT, con le loro interrelazioni ed il loro supporto alle diverse funzioni aziendali per esigenze di governance, gestione, controllo e verifica, sono illustrate nella **figura 4**.

Figura 4 – Le relazioni fra le componenti di COBIT



COBIT è costituito da un modello e da un insieme di strumenti di supporto che consentono al management di colmare il divario esistente tra requisiti di controllo, le problematiche tecniche e i rischi aziendali, e di comunicare tale livello di controllo agli stakeholder. COBIT rende possibile lo sviluppo di politiche chiare e di best-practice per il controllo dell'IT nelle aziende. COBIT è continuamente aggiornato ed armonizzato con gli altri standard e le altre linee guida. Per questa ragione, COBIT è divenuto sia l'integratore per le best-practice nell'IT sia il quadro generale di riferimento per la governance dell'IT, che aiuta a comprendere e gestire i rischi ed i benefici dell'IT. La struttura per processi di COBIT ed il suo approccio di alto livello orientato al business forniscono una visione completa dell'IT e delle decisioni che devono essere prese in merito.

I benefici derivanti dall'utilizzo di COBIT come schema di riferimento per il governo dell'IT comprendono:

- un migliore allineamento, grazie ad uno stretto collegamento con la realtà aziendale,
- una visione di cosa fa l'IT in termini comprensibili da parte del management,
- una chiara assegnazione delle proprietà e delle responsabilità, basata su un approccio orientato ai processi,
- una generale accettazione da parte di terzi e degli organi di vigilanza,
- una condivisione delle conoscenze fra tutti gli stakeholder, basata su un linguaggio comune,
- il soddisfacimento dei requisiti definiti nel modello COSO e relativi all'ambiente di controllo dell'IT.

Le pagine seguenti di questo documento forniscono una descrizione del modello di tutte le sue componenti principali organizzate nei 4 domini IT e nei 34 processi IT. Tutto questo costituisce un utile manuale di riferimento per tutte le linee guida di COBIT. Sono inoltre presenti anche diverse appendici per fornire utili riferimenti.

Informazioni aggiornate su COBIT e tutte le sue componenti, compresi gli strumenti on-line, le guide per l'implementazione, i case study, le newsletter ed il materiale didattico sono disponibili sul sito www.isaca.org/cobit.

(1) - La figura 3 mostra lo schema dei prodotti basati sul framework COBIT che illustra i prodotti generalmente applicabili e i ruoli principalmente coinvolti.

Oltre a questi prodotti, ve ne sono altri sviluppati per specifiche esigenze (*IT Control Objectives for Sarbanes-Oxley, 2nd Edition*), per particolari ambiti quali la sicurezza (*COBIT Security Baseline and Information Security Governance: Guidance for Boards of Directors and Executive Management*), o per specifiche tipologie di imprese (*COBIT Quickstart* si rivolge alle piccole o medie imprese oppure alle grandi imprese che vogliono puntare direttamente sull'adozione di un modello di IT Governance pervasivo).