



Leading the IT Governance Community

COBIT

4.1

**Versione
Italiana**

Framework
Control Objectives
Management Guidelines
Maturity Models

COBIT®

4.1

Traduzione italiana



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	Generali Business Solutions
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.



Sistemi informativi: averne fiducia e trarne valore

Milano Chapter

Pagina intenzionalmente bianca

COBIT 4.1

IT Governance Institute®

L'IT Governance Institute (ITGI™) (www.itgi.org) è stato fondato nel 1998 per sviluppare la cultura e gli standard internazionali per la direzione ed il controllo della funzione IT delle imprese. Un efficace governo dell'IT aiuta ad assicurare che la funzione IT contribuisca al raggiungimento degli obiettivi aziendali, ottimizzi gli investimenti aziendali nell'IT, e gestisca adeguatamente le opportunità tecnologiche ed i relativi rischi. ITGI propone ricerche originali, pubblicazioni in formato elettronico, casi di studio, per aiutare i leader delle imprese ed i consigli di amministrazione nel far fronte alle loro responsabilità per quanto riguarda l'IT Governance.

Disclaimer

ITGI (il "Proprietario") ha sviluppato e prodotto questa pubblicazione, intitolata COBIT®4.1 (il "Prodotto"), innanzitutto come una risorsa formative per i direttori della funzione IT, l'alta direzione, i responsabili intermedi della funzione IT, i *professional* del controllo. Il Proprietario non assicura alcun risultato dovuto all'utilizzo del Prodotto o di una sua parte. 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, i CIO, l'alta direzione, i responsabili intermedi della funzione IT, i *professional* del controllo devono valutare, sotto la propria responsabilità, la particolare circostanza influenzata dallo specifico sistema o dallo specifico ambito tecnologico.

Disclosure

Copyright © 2007 dell'IT Governance Institute. Tutti i diritti riservati. Nessuna parte di questa pubblicazione può essere usata, copiata, riprodotta, modificata, distribuita, riprodotta su video, registrata su un sistema di riproduzione, o trasmessa in qualsiasi forma e con qualsiasi mezzo (elettronico, meccanico, di fotocopiatura, registrazione o simili), senza la preventiva autorizzazione scritta di ITGI. La riproduzione di parti di questa pubblicazione, per uso interno e comunque non commerciale e per esclusivi scopi didattici, è permesso e deve comprendere un completo riferimento e attribuzione del materiale selezionato ad ITGI. Nessun altro diritto o permesso è autorizzato per questo Prodotto.

ISBN 1-933284-72-2

COBIT®4.1

Printed in the United States of America

RINGRAZIAMENTI

IT Governance Institute desidera ringraziare:**Gli Esperti che hanno realizzato e rivisto questa pubblicazione**

Mark Adler, CISA, CISM, CIA, CISSP, Allstate Ins. Co., USA
 Peter Andrews, CISA, CITP, MCFI, PJA Consulting, UK
 Georges Ataya, CISA, CISM, CISSP, MSCS, PBA, Solvay Business School, Belgio
 Gary Austin, CISA, CIA, CISSP, CGFM, KPMG LLP, USA
 Gary S. Baker, CA, Deloitte & Touche, Canada
 David H. Barnett, CISM, CISSP, Applera Corp., USA
 Christine Bellino, CPA, CITP, Jefferson Wells, USA
 John W. Beveridge, CISA, CISM, CFE, CGFM, CQA, Massachusetts Office of the State Auditor, USA
 Alan Boardman, CISA, CISM, CA, CISSP, Fox IT, UK
 David Bonewell, CISA, CISSP-ISSEP, Accomac Consulting LLC, USA
 Dirk Bruyndonckx, CISA, CISM, KPMG Advisory, Belgio
 Don Canilglia, CISA, CISM, USA
 Luis A. Capua, CISM, Sindicatura General de la Nación, Argentina
 Boyd Carter, PMP, Elegantsolutions.ca, Canada
 Dan Casciano, CISA, Ernst & Young LLP, USA
 Sean V. Casey, CISA, CPA, USA
 Sushil Chatterji, Edutech, Singapore
 Edward Chavannes, CISA, CISSP, Ernst & Young LLP, USA
 Christina Cheng, CISA, CISSP, SSCP, Deloitte & Touche LLP, USA
 Dharmesh Choksey, CISA, CPA, CISSP, PMP, KPMG LLP, USA
 Jeffrey D. Custer, CISA, CPA, CIA, Ernst & Young LLP, USA
 Beverly G. Davis, CISA, Federal Home Loan Bank of San Francisco, USA
 Peter De Bruyne, CISA, Banksys, Belgio
 Steven De Haes, University of Antwerp Management School, Belgio
 Peter De Koninck, CISA, CFSA, CIA, SWIFT SC, Belgio
 Philip De Picker, CISA, MCA, National Bank of Belgium, Belgio
 Kimberly de Vries, CISA, PMP, Zurich Financial Services, USA
 Roger S. Debreceny, Ph.D., FCPA, University of Hawaii, USA
 Zama Dlamini, Deloitte & Touche LLP, Sud Africa
 Rupert Dodds, CISA, CISM, FCA, KPMG, Nuova Zelanda
 Troy DuMoulin, Pink Elephant, Canada
 Bill A. Durrand, CISA, CISM, CA, Ernst & Young LLP, Canada
 Justus Ekeigwe, CISA, MBCS, Deloitte & Touche LLP, USA
 Rafael Eduardo Fabius, CISA, Republica AFAP S.A., Uruguay
 Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Svizzera
 Christopher Fox, ACA, PricewaterhouseCoopers, USA
 Bob Frelinger, CISA, Sun Microsystems Inc., USA
 Zhiwei Fu, Ph. D, Fannie Mae, USA
 Monique Garsoux, Dexia Bank, Belgio
 Edson Gin, CISA, CFE, SSCP, USA
 Sauvik Ghosh, CISA, CIA, CISSP, CPA, Ernst & Young LLP, USA
 Guy Groner, CISA, CIA, CISSP, USA
 Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgio
 Gary Hardy, IT Winners, Sud Africa
 Jimmy Heschl, CISA, CISM, KPMG, Austria
 Benjamin K. Hsaio, CISA, Federal Deposit Insurance Corp., USA
 Tom Hughes, Acumen Alliance, Australia
 Monica Jain, CSQA, Covansys Corp., US
 Wayne D. Jones, CISA, Australian National Audit Office, Australia
 John A. Kay, CISA, USA
 Lisa Kinyon, CISA, Countrywide, USA
 Rodney Kocot, Systems Control and Security Inc., USA
 Luc Kordel, CISA, CISM, CISSP, CIA, RE, RFA, Dexia Bank, Belgio
 Linda Kostic, CISA, CPA, USA
 John W. Lainhart IV, CISA, CISM, IBM, USA
 Philip Le Grand, Capita Education Services, UK.
 Elsa K. Lee, CISA, CISM, CSQA, AdvanSoft International Inc., USA
 Kenny K. Lee, CISA, CISSP, Countrywide SMART Governance, USA
 Debbie Lew, CISA, Ernst & Young LLP, USA
 Donald Lorete, CPA, Deloitte & Touche LLP, USA

RINGRAZIAMENTI (seguito)

Addie C.P. Lui, MCSA, MCSE, First Hawaiian Bank, USA
Debra Mallette, CISA, CSSBB, Kaiser Permanente, USA
Charles Mansour, CISA, Charles Mansour Audit & Risk Service, UK
Mario Micallef, CPAA, FIA, National Australia Bank Group, Australia
Niels Thor Mikkelsen, CISA, CIA, Danske Bank, Danimarca
John Mitchell, CISA, CFE, CITP, FBCS, FIIA, MIIA, QiCA, LHS Business Control, UK
Anita Montgomery, CISA, CIA, Countrywide, USA
Karl Muise, CISA, City National Bank, USA
Jay S. Munnelly, CISA, CIA, CGFM, Federal Deposit Insurance Corp., USA
Sang Nguyen, CISA, CISSP, MCSE, Nova Southeastern University, USA
Ed O'Donnell, Ph.D., CPA, University of Kansas, USA
Sue Owen, Department of Veterans Affairs, Australia
Robert G. Parker, CISA, CA, CMC, FCA, Robert G. Parker Consulting, Canada
Robert Payne, Trecor Services (Pty) Ltd., Sud Africa
Thomas Phelps IV, CISA, PricewaterhouseCoopers LLP, USA
Vitor Prisca, CISM, Novabase, Portogallo
Martin Rosenberg, Ph.D., IT Business Management, UK
Claus Rosenquist, CISA, TrygVesata, Danimarca
Jaco Sadie, Sasol, Sud Africa
Max Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Craig W. Silverthorne, CISA, CISM, CPA, IBM Business Consulting Services, USA
Chad Smith, Great-West Life, Canada
Roger Southgate, CISA, CISM, FCCA, CubeIT Management Ltd., UK
Paula Spinner, CSC, USA
Mark Stanley, CISA, Toyota Financial Services, USA
Dirk E. Steuperaert, CISA, PricewaterhouseCoopers, Belgio
Robert E. Stroud, CA Inc., USA
Scott L. Summers, Ph.D., Brigham Young University, USA
Lance M. Turcato, CISA, CISM, CPA, City of Phoenix IT Audit Division, USA
Wim Van Grembergen, Ph.D., University of Antwerp Management School, Belgio
Johan Van Grieken, CISA, Deloitte, Belgio
Greet Volders, Voqual NV, Belgio
Thomas M. Wagner, Gartner Inc., USA
Robert M. Walters, CISA, CPA, CGA, Office of the Comptroller General, Canada
Freddy Withagels, CISA, Capgemini, Belgio
Tom Wong, CISA, CIA, CMA, Ernst & Young LLP, Canada
Amanda Xu, CISA, PMP, KPMG LLP, USA

Il Consiglio di Amministrazione di ITGI

Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, Presidente Internazionale
Georges Ataya, CISA, CISM, CISSP, Solvay Business School, Belgium, Vice Presidente
William C. Boni, CISM, Motorola, USA, Vice Presidente
Avinash Kadam, CISA, CISM, CISSP, CBCP, GSEC, GCIH, Miel e-Security Pvt. Ltd., India, Vice Presidente
Jean-Louis Leignel, MAGE Conseil, France, Vice Presidente
Lucio Augusto Molina Focazzio, CISA, Colombia, Vice Presidente
Howard Nicholson, CISA, City of Salisbury, Australia, Vice Presidente
Frank Yam, CISA, FHKIoD, FHKCS, FFA, CIA, CFE, CCP, CFSA, Focus Strategic Group, Hong Kong, Vice Presidente
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Precedente Presidente Internazionale
Robert S. Roussey, CPA, University of Southern California, USA, Precedente Presidente Internazionale
Ronald Saull, CSP, Great-West Life and IGM Financial, Canada, Consigliere

Il Comitato per l'IT Governance

Tony Hayes, FCPA, Queensland Government, Australia, Presidente
Max Blecher, Virtual Alliance, Sud Africa
Sushil Chatterji, Edutech, Singapore
Anil Jogani, CISA, FCA, Tally Solutions Limited, UK
John W. Lainhart IV, CISA, CISM, IBM, USA
Rómulo Lomparte, CISA, Banco de Crédito BCP, Peru
Michael Schirnbrand, Ph.D., CISA, CISM, CPA, KPMG LLP, Austria
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada

Il Comitato strategico di COBIT

Roger Debreceeny, Ph.D., FCPA, University of Hawaii, USA, Presidente
Gary S. Baker, CA, Deloitte & Touche, Canada
Dan Casciano, CISA, Ernst & Young LLP, USA
Steven De Haes, University of Antwerp Management School, Belgio
Peter De Koninck, CISA, CFSA, CIA, SWIFT SC, Belgio
Rafael Eduardo Fabius, CISA, República AFAP SA, Uruguay
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Svizzera
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgio
Gary Hardy, IT Winners, Sud Africa
Jimmy Heschl, CISA, CISM, KPMG, Austria
Debbie A. Lew, CISA, Ernst & Young LLP, USA
Maxwell J. Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Dirk Steuperaert, CISA, PricewaterhouseCoopers LLC, Belgio
Robert E. Stroud, CA Inc., USA

I Consulenti di ITGI

Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Presidente
Roland Bader, F. Hoffmann-La Roche AG, Svizzera
Linda Betz, IBM Corporation, USA
Jean-Pierre Corniou, Renault, Francia
Rob Clyde, CISM, Symantec, USA
Richard Granger, NHS Connecting for Health, UK
Howard Schmidt, CISM, R&H Security Consulting LLC, USA
Alex Siow Yuen Khong, StarHub Ltd., Singapore
Amit Yoran, Yoran Associates, USA

Gli Enti affiliati ad ITGI e gli Sponsor

I Capitoli di ISACA
American Institute for Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association of Corporate Governance
FIDA Inform
Information Security Forum
The Information Systems Security Association
Institut de la Gouvernance des Systèmes d'Information
Institute of Management Accountants
ISACA
ITGI Japan
Solvay Business School
University of Antwerp Management School
Aldion Consulting Pte. Lte.
CA
Hewlett-Packard
IBM
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Symantec Corporation
Wolcott Group LLC
World Pass IT Solutions

SOMMARIO

Executive Overview.	5
Modello di riferimento di COBIT.	9
Pianificazione e Organizzazione.	29
Acquisizione e Realizzazione	73
Erogazione ed Assistenza	101
Monitoraggio e Valutazione	153
Appendice I—Tabelle di collegamento fra Obiettivi e Processi.	169
Appendice II—Mappatura dei processi IT sulle Aree della IT Governance, su COSO, sulle risorse IT di COBIT e sui criteri di valutazione delle informazioni di COBIT	173
Appendice III—Modello di strutturazione del Controllo Interno	175
Appendice IV— Le principali fonti di riferimento di COBIT 4.1.	177
Appendice V— Riferimenti incrociati fra COBIT 3 rd Edition e COBIT 4.1.	179
Appendice VI—Approccio definito per la ricerca e lo sviluppo.	187
Appendice VII—Glossario	189
Appendice VIII—COBIT e I prodotti della sua suite.	195

Le appendici si trovano nella versione originale in lingua inglese.

Ogni commento su COBIT 4.1 è benaccetto. Per inoltrare eventuali commenti utilizzare il seguente indirizzo www.isaca.org/cobitfeedback .

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.

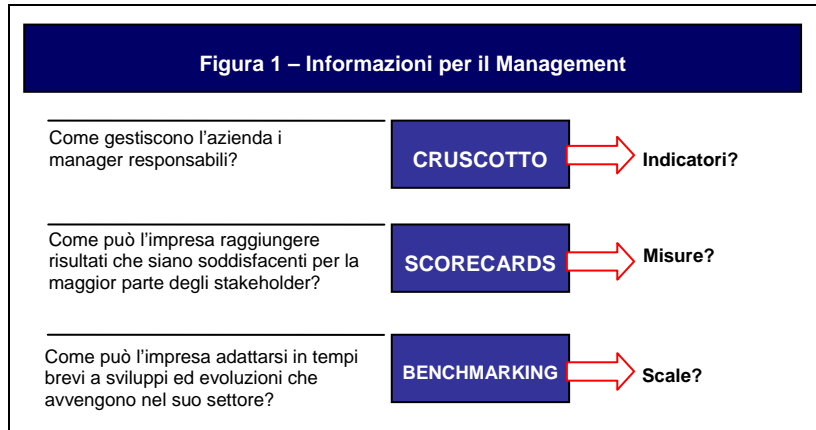
Ma l'impresa, come tiene l'IT sotto controllo in modo che esso fornisca le informazioni di cui l'impresa stessa necessita? Come gestisce il rischio e mantiene sicure le risorse IT da cui è così dipendente? Come fa l'impresa ad assicurare che l'IT raggiunga i propri obiettivi nel mentre supporta il business?

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.



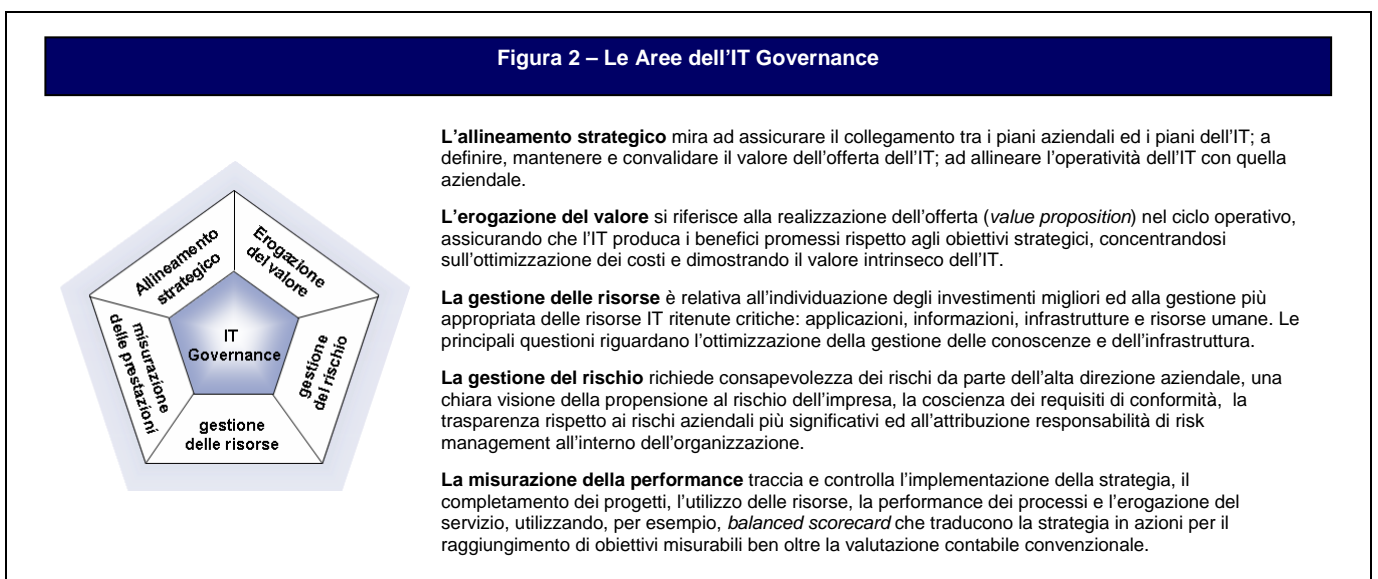
Una risposta a queste richieste di determinare e monitorare l'appropriato livello di controllo e di performance per l'IT si trova nelle definizioni che COBIT fornisce per:

- **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.



EXECUTIVE OVERVIEW

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.

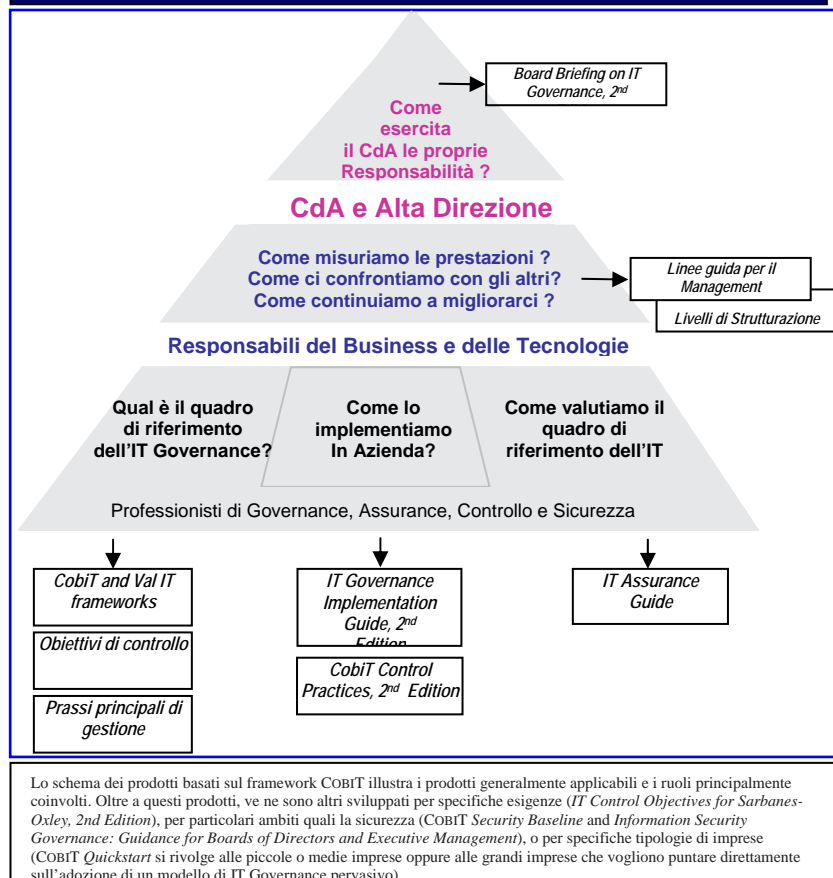
Le componenti di COBIT sono strutturate su tre livelli (vedi figura 3) progettate per aiutare:

- 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 perché 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.

Figura 3 – Schema dei contenuti di COBIT

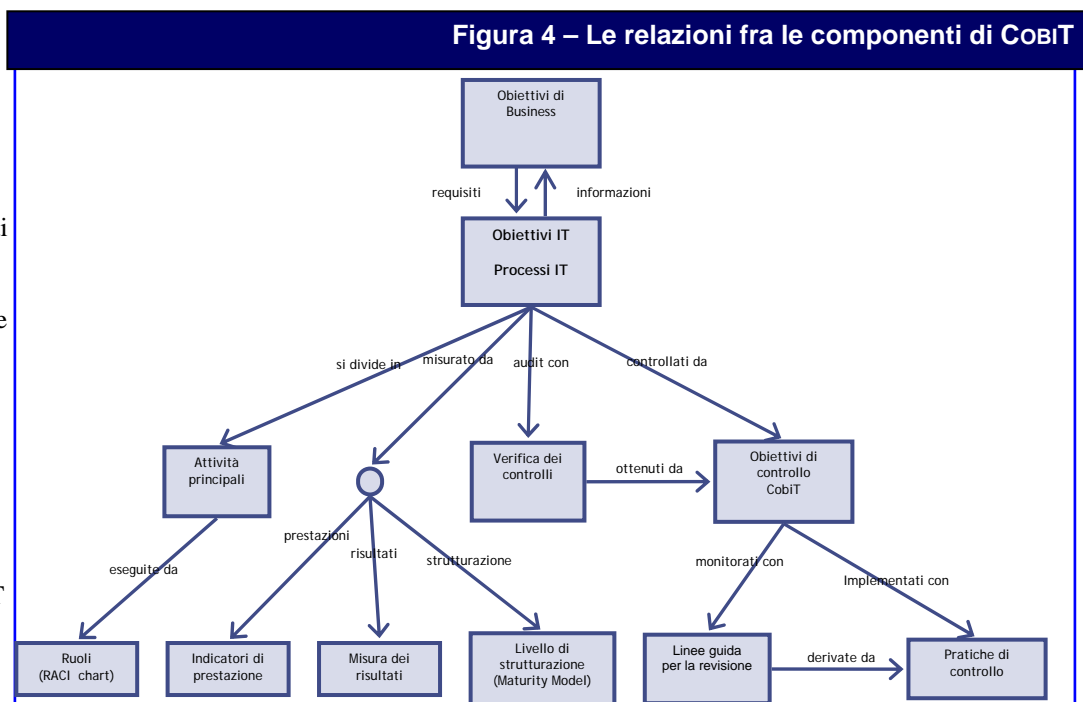


- *COBIT® Control practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition* – E' una guida per motivare l'introduzione dei controlli e per individuare le modalità più opportune per realizzarli
- *IT Assurance Guide: Using COBIT®* – Fornisce delle linee guida su come 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**.

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 good practice per il controllo dell'IT nelle aziende. COBIT è continuamente aggiornato ed armonizzato con gli altri standard e le



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.

IL MODELLO DI RIFERIMENTO DI COBIT

L'OBIETTIVO DI COBIT:

La ricerca, lo sviluppo, la divulgazione e la promozione di un modello di riferimento per l'IT governance che sia autorevole, aggiornato e accettato a livello internazionale, e che possa essere utilizzato dalle aziende, dalla direzione, dai professionisti IT e dagli auditors.

LA NECESSITÀ DI UN MODELLO DI CONTROLLO DI RIFERIMENTO PER L' IT GOVERNANCE

Un modello di controllo per l'IT governance definisce le ragioni per cui l'IT governance è necessaria, i suoi stakeholders e ciò che intende perseguire.

Perché

L'alta direzione comprende sempre più l'impatto significativo che l'informazione può avere sul successo dell'impresa. Il management si aspetta una maggiore comprensione del modo in cui si fa funzionare l'information technology (IT) e della possibilità che ha di essere sfruttato con successo per un vantaggio competitivo. In particolare, l'alta direzione deve sapere se l'impresa gestisce l'informazione in modo da:

- avere la probabilità di raggiungere i propri obiettivi
- essere abbastanza flessibile per imparare ed adattarsi
- gestire con criterio i rischi che incontra
- riconoscere appropriatamente le opportunità, ed agire di conseguenza

Le imprese di successo comprendono i rischi e si avvantaggiano dei benefici dell'IT e trovano il modo di :

- gestire l'allineamento della strategia IT con la strategia aziendale
- fornire ad investitori ed azionisti adeguate garanzie a conferma che l'organizzazione pone la "dovuta attenzione" riguardo la mitigazione dei rischi IT
- calare la strategia e gli obiettivi IT all'interno dell'impresa
- ottenere valore dagli investimenti IT
- fornire strutture organizzative che facilitano l'implementazione di strategie ed obiettivi
- creare relazioni costruttive e comunicazioni efficaci tra l'azienda e l'IT, e con i partner esterni
- misurare la performance dell'IT.

Le imprese non possono rispondere efficacemente a tali requisiti aziendali e di governo senza adottare ed implementare uno schema di governo e controllo per l'IT per:

- creare un collegamento con i requisiti aziendali
- dare trasparenza alla performance rispetto a questi requisiti
- organizzare le proprie attività in un modello di processo generalmente accettato
- identificare le principali risorse da attivare
- definire gli obiettivi di controllo di gestione da prendere in considerazione.

Inoltre, gli schemi di riferimento per il governo ed il controllo stanno diventando parte delle best practice dell'IT management e sono un fattore facilitante per stabilire il governo IT e conformarsi con le sempre crescenti richieste della normativa.

Le good practice dell'IT sono diventate importanti grazie ad alcuni fattori:

- i manager e gli organi direttivi dell'azienda si aspettano un maggior ritorno dagli investimenti in IT, cioè che l'IT fornisca i servizi di cui l'azienda ha bisogno per incrementare il valore per gli stakeholder
- la preoccupazione relativa all'aumento generalizzato del livello di spesa per l'IT
- l'esigenza di soddisfare le richieste della normativa per i controlli IT in aree quali la privacy e la predisposizione del bilancio (per esempio il Sarbanes-Oxley Act, Basilea II) ed in settori specifici come quelli finanziario, farmaceutico e della sanità.
- la selezione dei fornitori di servizi e la gestione dell'esternalizzazione e dell'acquisizione dei servizi
- la crescente complessità dei rischi correlati all'IT come la sicurezza delle reti
- le iniziative di IT governance che includono l'adozione di quadri di controllo di riferimento e best practice che aiutino il monitoraggio ed il miglioramento delle attività critiche di IT per incrementare il valore aziendale e ridurre i rischi
- l'esigenza di ottimizzare i costi seguendo, dove possibile, approcci standardizzati piuttosto che metodi sviluppati appositamente
- la crescente maturità e la conseguente accettazione di schemi di riferimento affermati quali COBIT, ITIL, ISO 17799, ISO 9001, CMM e PRINCE2, PMBOK
- l'esigenza per le imprese di valutare le proprie prestazioni sia rispetto a standard generalmente accettati che nei confronti dei propri concorrenti (benchmarking)

Chi

Uno schema di riferimento per il governo ed il controllo deve essere in grado di soddisfare diversi stakeholder interni ed esterni, ognuno dei quali ha specifiche esigenze:

- Stakeholder interni all'impresa che hanno interesse a generare valore dagli investimenti in IT
 - chi prende le decisioni di investimento
 - chi decide i requisiti
 - chi utilizza i servizi IT
- Stakeholder interni ed esterni che forniscono i servizi IT
 - chi gestisce l'organizzazione ed i processi dell'IT
 - chi sviluppa le competenze
 - chi gestisce i servizi
- Stakeholder interni ed esterni che hanno responsabilità sui rischi/controlli
 - chi ha responsabilità in materia di sicurezza, privacy e/o rischi
 - chi svolge funzioni di verifica della conformità
 - chi richiede o fornisce servizi di assurance

Cosa

Al fine di raggiungere i requisiti sopra elencati, lo schema di riferimento per il governo ed il controllo dell'IT deve soddisfare le seguenti specifiche generali:

- offrire una prospettiva centrata sull'azienda in modo da facilitare l'allineamento tra gli obiettivi dell'azienda e dell'IT
- stabilire un orientamento dei processi per definire l'ambito e l'entità della copertura, con una struttura definita in modo da consentire di navigare con facilità tra i contenuti
- essere generalmente accettabile rimanendo coerente con le best practice e gli standard di IT ed indipendente da tecnologie specifiche
- utilizzare un linguaggio comune con termini e definizioni che siano generalmente comprensibili da tutti gli stakeholder
- aiutare a rispettare i requisiti normativi rimanendo in linea con gli standard di corporate governance generalmente accettati (es., COSO) e con i controlli IT richiesti dai supervisor e dai revisori esterni.

COME COBIT RISPONDE A QUESTE ESIGENZE

A fronte delle esigenze descritte nella sezione precedente, allo schema di riferimento del COBIT sono state attribuite fin dalla sua creazione le seguenti caratteristiche principali: è focalizzato sull'azienda, orientato ai processi, basato sui controlli e determinato dalle misurazioni.

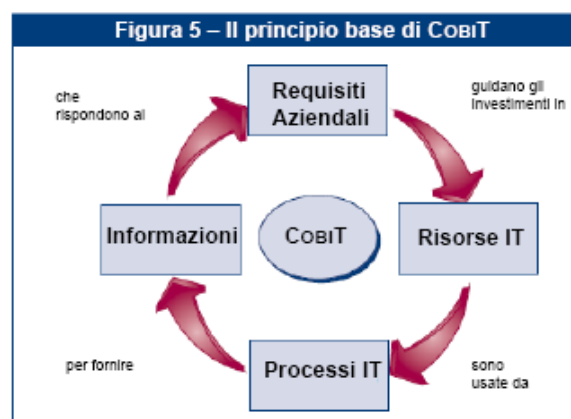
Orientato al business

L'orientamento al business è il principale tema di COBIT, che non è stato disegnato per essere utilizzato solo da fornitori di servizi IT, utenti e revisori, ma anche, e prima ancora, per essere una guida completa per i manager ed i responsabili dei processi aziendali.

Lo schema di riferimento di COBIT è basato sul seguente Principio (Figura 5):

per poter fornire le informazioni di cui l'impresa ha bisogno per raggiungere i propri obiettivi, l'azienda deve poter gestire e controllare le risorse IT utilizzando un insieme strutturato di processi per erogare i servizi informativi richiesti.

La gestione e il controllo delle informazioni sono al centro del modello di controllo COBIT e aiutano ad assicurare l'allineamento agli obiettivi aziendali.



I CRITERI DI VALUTAZIONE DELLE INFORMAZIONI

Per perseguire gli obiettivi aziendali, le informazioni devono soddisfare determinati criteri che nella metodologia COBIT sono chiamati requisiti aziendali per le informazioni. Partendo dai requisiti più ampi di qualità, affidabilità e sicurezza, sono stati identificati sette criteri distinti, certamente sovrapponibili, definiti come segue:

- **L'efficacia** riguarda le informazioni, che debbono essere rilevanti e pertinenti rispetto ai processi aziendali e devono poter essere rese disponibili tempestivamente, senza errori, in modo coerente ed utilizzabile.
- **L'efficienza** riguarda la gestione delle informazioni attraverso l'uso ottimale delle risorse (sia dal punto di vista della maggiore produttività che della economicità)
- **La riservatezza** riguarda la protezione delle informazioni sensibili da possibili accessi non autorizzati

IL MODELLO DI RIFERIMENTO DI COBIT

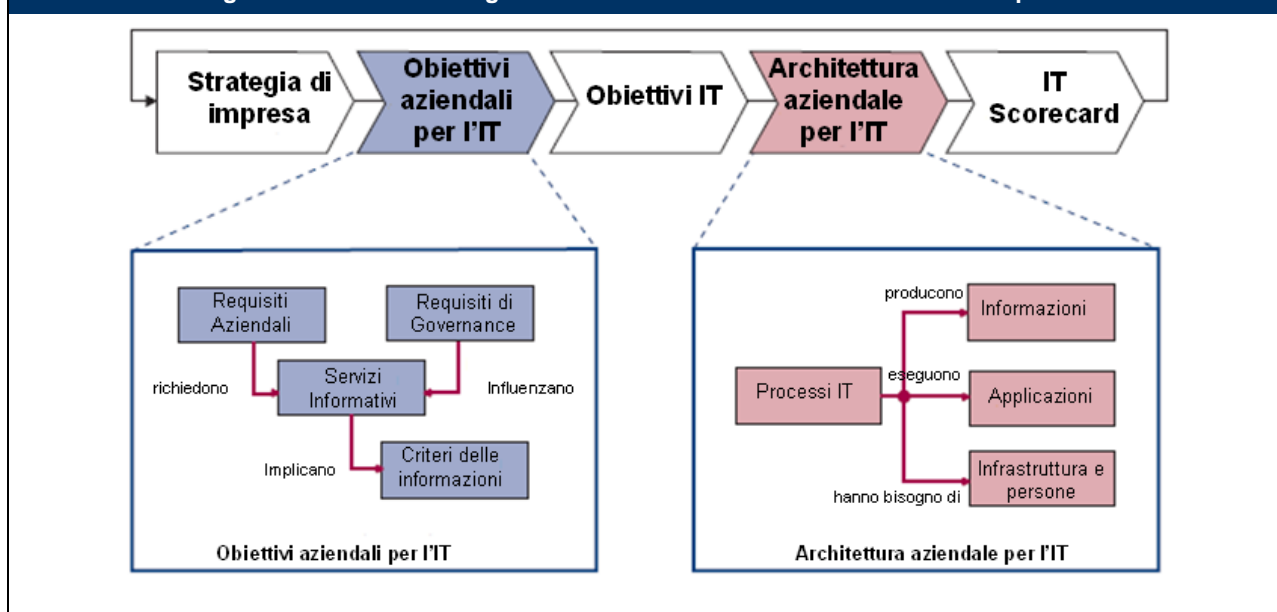
- **L'integrità** riguarda l'accuratezza e la completezza delle informazioni come pure la loro validità nel rispetto dei valori e delle aspettative aziendali
- **La disponibilità** è riferita al fatto che le informazioni devono essere disponibili quando richiesto dai processi aziendali, sia nel presente che nel futuro. Riguarda inoltre la salvaguardia delle risorse necessarie e delle relative capacità e funzionalità
- **La conformità** riguarda il rispetto di leggi, regolamenti ed accordi contrattuali cui è soggetto il processo aziendale, cioè vincoli aziendali imposti dall'esterno e politiche interne
- **L'affidabilità** riguarda la fornitura di informazioni appropriate, che permettano alla direzione di gestire l'azienda ed esercitare le proprie responsabilità come organi fiduciari e di governo.

OBIETTIVI AZIENDALI E OBIETTIVI IT

Mentre i criteri di valutazione delle informazioni forniscono un metodo generico per la definizione dei requisiti aziendali, la definizione di un insieme di obiettivi aziendali ed IT generici offre all'azienda un punto di partenza più preciso per definire i requisiti aziendali e sviluppare le metriche che consentono la misurazione di questi obiettivi. Tutte le imprese utilizzano l'IT per rendere possibili le iniziative di business, che diventano per l'IT degli obiettivi aziendali. Nell'Appendice I viene riportata una matrice degli obiettivi aziendali ed IT generici e di come essi si rapportano ai criteri di valutazione delle informazioni. Questi esempi di massima possono essere usati come guida nella determinazione di requisiti aziendali, obiettivi e metriche specifici per l'impresa.

Se l'IT fornisce con successo i propri servizi a supporto della strategia dell'impresa, l'azienda (il cliente) deve avere una chiara proprietà ed un preciso controllo dei requisiti oltre ad una chiara comprensione di cosa le debba fornire l'IT (il fornitore) e come. La **figura 6** illustra come la strategia d'impresa debba essere tradotta dall'azienda in obiettivi per consentire l'utilizzo degli strumenti predisposti dall'IT (gli obiettivi aziendali per l'IT). Questi obiettivi, a loro volta, devono portare ad una chiara definizione delle mete proprie dell'IT (gli obiettivi dell'IT) e, successivamente, definire le risorse e le capacità dell'IT (l'architettura aziendale dell'IT) che sono necessarie per svolgere con successo il proprio ruolo nella strategia dell'impresa¹.

Figura 6 – Definizione degli obiettivi dell'IT e dell'architettura aziendale per l'IT



Dopo aver provveduto all'allineamento degli obiettivi, è necessario un monitoraggio per assicurare che i servizi erogati corrispondano alle aspettative. Ciò può essere raggiunto mediante l'utilizzo di metriche derivate dagli obiettivi e riportate in una IT Scorecard.

Tutti questi obiettivi e le relative metriche devono essere espressi in termini di business rilevanti per il cliente. Tutto ciò, combinato con un efficace allineamento dei rispettivi obiettivi e delle loro priorità, potrà sicuramente portare l'azienda a confermare che l'IT è in grado di supportare gli obiettivi dell'impresa.

L'Appendice I fornisce una visione complessiva di come degli obiettivi aziendali generici si rapportino con gli obiettivi IT, i processi IT ed i criteri di valutazione delle informazioni. Le tabelle aiutano a dimostrare l'ambito considerato in COBIT e la relazione complessiva tra COBIT e i driver aziendali. Come illustrato dalla **figura 6**, tali driver derivano dal business e dal governo dell'azienda, il primo concentrandosi più sulla funzionalità e velocità di messa in esercizio, il secondo più sull'economicità, Return on Investment (ROI) e conformità normativa.

¹ Va notato che la definizione ed implementazione di un'architettura IT aziendale crea, anche degli obiettivi IT interni che contribuiscono agli obiettivi di business ma non ne derivano direttamente

LE RISORSE IT

Nell'ambito di questi obiettivi, l'organizzazione IT opera con un insieme chiaramente definito di processi che, utilizzando le competenze del personale e le infrastrutture tecnologiche, gestiscono le applicazioni aziendali automatizzate sulla base delle informazioni aziendali. Queste risorse, insieme ai processi, costituiscono l'architettura aziendale dell'IT, come mostrato in **figura 6**.

Per rispondere ai requisiti aziendali per l'IT, l'impresa ha la necessità di investire nelle risorse richieste al fine di creare un'adeguata capacità tecnica (ad esempio, un sistema ERP) per supportare una possibile funzione aziendale (ad esempio, l'implementazione di un ciclo acquisti) che porti al risultato desiderato (ad esempio, l'incremento delle vendite e dei benefici economici).

Le risorse IT identificate da COBIT possono essere definite come segue:

- **Applicazioni:** sono costituite dai sistemi automatizzati e dalle procedure manuali che elaborano le informazioni.
- **Informazioni:** sono i dati in tutte le loro forme, quando sono inseriti, elaborati e prodotti dai sistemi informativi, in qualsiasi forma utilizzata dall'azienda.
- **Infrastruttura:** è rappresentata dalla tecnologia e dagli strumenti (hardware, sistema operativo, sistemi di gestione dei database, reti, supporti
- multimediali, ecc., e l'ambiente che li ospita e li supporta) che consentono il funzionamento delle applicazioni.
- **Risorse Umane:** sono il personale richiesto per pianificare, organizzare, acquisire, implementare, erogare, supportare, controllare e valutare i sistemi informativi ed i servizi. Possono essere interne, esterne, o a contratto, se richiesto.

La **figura 7** sintetizza come gli obiettivi aziendali per l'IT influenzano il modo in cui le risorse IT devono essere gestite dai processi IT per raggiungere gli obiettivi dell'IT.

Orientato ai processi

COBIT definisce le attività IT in un modello generale di processi all'interno di quattro domini. Questi domini sono Pianificazione e Organizzazione, Acquisizione e Implementazione, Erogazione e Assistenza, e Monitoraggio e Valutazione. I domini si riferiscono alle tradizionali aree di responsabilità dell'IT di pianificazione, costruzione, esecuzione e controllo.

Lo schema di COBIT fornisce un modello di processo di riferimento ed un linguaggio comune per tutti quelli che nell'azienda controllano e gestiscono le attività IT. Incorporando un modello operativo ed un linguaggio comune per tutte le componenti aziendali coinvolte nell'IT, COBIT è uno dei passi iniziali e più importanti verso una buona *governance*. Inoltre fornisce uno schema per misurare e controllare le prestazioni dell'IT, comunicando con i fornitori di servizi e integrando le best practice di gestione. Un modello di processo incoraggia la proprietà dei processi, facilitando la definizione delle responsabilità ai vari livelli.

Per governare l'IT efficacemente è importante comprendere le attività ed i rischi che devono essere gestiti all'interno dell'IT. Questi vengono normalmente ordinati nei domini di responsabilità relativi alla pianificazione, sviluppo (*build*), esercizio (*run*) e monitoraggio. All'interno del modello di controllo COBIT, questi domini, come mostrato in **figura 8** sono chiamati:

- **Pianificazione e Organizzazione (PO)**—Fornisce direzione allo sviluppo di soluzioni (AI) e allo sviluppo dei servizi (DS)
- **Acquisizione ed implementazione (AI)**—Fornisce le soluzioni e ne consente la trasformazione in servizi.
- **Erogazione e supporto (DS)**—Riceve le soluzioni e le rende utilizzabili dagli utenti finali.
- **Monitoraggio e valutazione (ME)**—Controlla tutti i processi per assicurare che siano seguite le direttive fornite.

PIANIFICAZIONE E ORGANIZZAZIONE (PO)

Questo dominio si riferisce agli aspetti strategici e tattici, e riguarda l'identificazione del modo in cui l'IT può meglio contribuire al raggiungimento degli obiettivi aziendali. Inoltre la realizzazione della visione strategica ha bisogno di essere pianificata, comunicata e gestita da differenti punti di vista. Infine deve essere costituita un'appropriata organizzazione così come una valida infrastruttura tecnologica. Questo dominio riguarda le seguenti domande del management:

- La strategia dell'IT e quella aziendale sono allineate?
- L'impresa sta ottenendo il massimo dalle proprie risorse?
- All'interno della azienda tutti comprendono gli obiettivi dell'IT?

Figura 7 – La gestione delle risorse IT per raggiungere gli obiettivi dell'IT

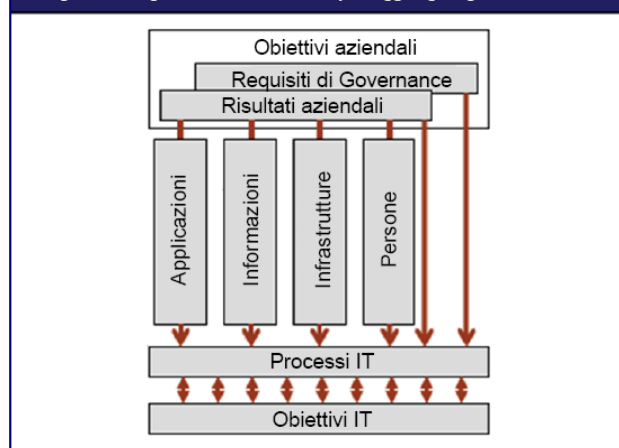


Figura 8 – I quattro domini correlati di COBIT



- I rischi IT sono capiti e gestiti?
- La qualità dei sistemi IT è adeguata alle esigenze aziendali?

ACQUISIZIONE ED IMPLEMENTAZIONE (AI)

Per realizzare la strategia IT, le soluzioni IT devono essere identificate, sviluppate o acquistate, come pure realizzate ed integrate nei processi aziendali. Inoltre rientrano in questo dominio le modifiche e la manutenzione delle applicazioni esistenti per assicurare che le soluzioni continuino a soddisfare gli obiettivi aziendali. Questo dominio riguarda le seguenti domande del management:

- I nuovi progetti sono in grado di garantire soluzioni che soddisfino le esigenze aziendali?
- E' possibile realizzare i nuovi progetti nel rispetto dei tempi e del budget?
- I nuovi sistemi funzionano correttamente dopo l'implementazione?
- I cambiamenti verranno fatti senza impattare sulle operazioni aziendali correnti?

EROGAZIONE E SUPPORTO (DS)

In questo dominio si fa riferimento all'erogazione dei servizi richiesti, che includono l'erogazione del servizio vero e proprio, la gestione della sicurezza e della continuità, il servizio di assistenza agli utenti e la gestione dei dati e le infrastrutture operative. Questo dominio risponde alle seguenti domande del management:

- I servizi IT vengono erogati in linea con le priorità aziendali?
- I costi dell'IT sono ottimizzati?
- La forza lavoro è in grado di utilizzare i sistemi IT in modo produttivo ed in sicurezza?
- Sono adeguatamente garantite riservatezza, integrità e disponibilità?

MONITORAGGIO E VALUTAZIONE (ME)

Tutti i processi IT devono essere regolarmente valutati nel tempo sotto l'aspetto della qualità e della conformità ai requisiti di controllo. Questo dominio, che riguarda la gestione delle prestazioni, la verifica del sistema di controllo interno, la conformità ai regolamenti ed il soddisfacimento dei requisiti di governo, risponde alle seguenti domande del management:

- Le prestazioni dell'IT sono misurate al fine di individuare i problemi prima che sia troppo tardi?
- L'alta direzione assicura che i controlli interni operino in modo efficace ed efficiente?
- La performance dell'IT può essere ricollegata agli obiettivi aziendali?
- Sono attivati controlli adeguati in materia di riservatezza, integrità e disponibilità ai fini della sicurezza delle informazioni?

Attraverso questi quattro domini, COBIT identifica 34 processi IT tipicamente adottati (fare riferimento alla **figura 23** per la lista completa). Se molte aziende hanno definito formalmente le responsabilità per la pianificazione, sviluppo, esercizio e controllo dell'IT, e molte hanno gli stessi processi chiave, poche hanno la stessa struttura di processi o applicano tutti e 34 i processi COBIT. Il COBIT fornisce una lista completa di processi che possono essere utilizzati per verificare la completezza delle attività e delle responsabilità. Tuttavia, non è necessaria la completa adozione di tale lista e i processi possono essere integrati a seconda delle necessità di ciascuna azienda.

Per ciascuno dei 34 processi, viene fornito un collegamento tra obiettivi di business ed obiettivi IT. Sono fornite anche informazioni su come misurare gli obiettivi, chi sono i relativi responsabili, quali sono le attività chiave ed i principali risultati (deliverables).

Basato sui controlli

COBIT definisce obiettivi di controllo per tutti e 34 i processi, ma anche per i relativi controlli di processo e applicativi.

I PROCESSI DEVONO ESSERE CONTROLLATI

Per controllo intendiamo l'insieme delle politiche, procedure, prassi e strutture organizzative atte ad assicurare con ragionevole certezza il raggiungimento degli obiettivi aziendali e l'identificazione e correzione degli eventi indesiderati.

Gli obiettivi di controllo IT forniscono un set completo di requisiti di alto livello che devono essere considerate dalla direzione per l'efficace controllo di tutti i processi IT. Essi:

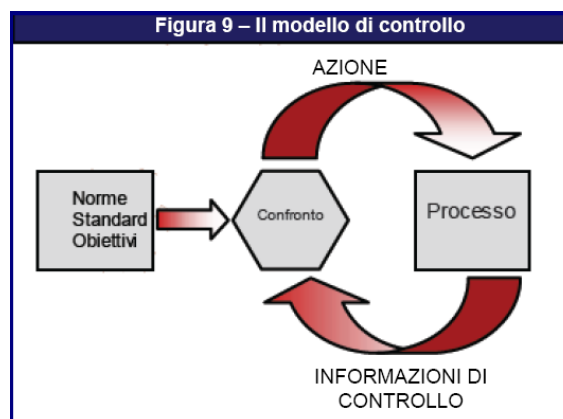
- Sono linee guida di azioni manageriali per aumentare il valore o ridurre il rischio.
- Consistono di politiche, procedure, prassi e strutture organizzative
- Sono disegnate per fornire ragionevole certezza che gli obiettivi di business saranno raggiunti e che eventi indesiderati saranno prevenuti o identificati e corretti.

La direzione aziendale deve prendere delle decisioni relativamente a questi obiettivi di controllo:

- Selezionando quelli applicabili.
- Decidendo quelli che dovranno essere implementati
- Scegliendo come implementarli (frequenza, ambito, livello di automazione ecc.)
- Accettando l'eventuale rischio di non implementare i controlli necessari.

Un'indicazione proviene dal modello di controllo standard riportato in **figura 9**, che applica i principi che sono evidenziati dalla seguente analogia: quando la temperatura di una stanza (standard) è regolata da un sistema di riscaldamento (processo), il sistema controllerà continuamente (confronto) la temperatura (informazione di controllo) e darà segno (azione) al sistema di riscaldamento di fornire più o meno calore.

La gestione operativa utilizza i processi per organizzare e gestire tutte le normali attività IT. COBIT fornisce un modello generale che rappresenta tutti i processi normalmente presenti nelle funzioni IT, e rappresenta un modello di riferimento comune comprensibile sia ai manager operativi dell'IT che a quelli dell'azienda. Per ottenere una governance efficace, i controlli devono essere implementati dai manager operativi all'interno di uno schema di riferimento definito e valido per tutti i processi IT. Visto che gli obiettivi di controllo IT di COBIT sono stati organizzati per relativo processo, lo schema di riferimento fornisce chiari legami tra requisiti di governo, processi e controlli dell'IT.



Ogni processo IT di COBIT ha un obiettivo di controllo di alto livello ed una serie di obiettivi di controllo di dettaglio che, nel loro insieme, costituiscono le caratteristiche di un processo ben gestito.

Gli obiettivi di controllo di dettaglio sono identificati da due lettere che fanno riferimento al dominio (PO, AI, DS e ME), dal numero del processo e dal numero dell'obiettivo di controllo. Oltre agli obiettivi di controllo di dettaglio, ogni processo di COBIT è accompagnato da requisiti di controllo generici che sono identificati dalla sigla PCn, che sta per Process Control number (numero del controllo di processo). Essi devono essere considerati congiuntamente agli obiettivi di controllo di dettaglio per avere una visione completa dei requisiti di controllo.

PC1 Scopi ed obiettivi di processo

Definisce e comunica scopi ed obiettivi specifici, misurabili, fattibili, realistici, orientati al risultato e tempestivi (SMARTT) per l'efficace esecuzione di ogni processo IT. Assicura inoltre che siano legati agli obiettivi di business e supportati da metriche adeguate.

PC2 Referente del processo

Assegna un referente ad ogni processo IT e definisce chiaramente i ruoli e responsabilità di tale referente. Ad esempio, vengono inclusi la responsabilità per il disegno del processo, la sua interazione con altri processi, la responsabilità per il risultato finale nonché la misurabilità della performance di processo e l'identificazione di opportunità di miglioramento.

PC3 Ripetibilità di processo

Definisce e stabilisce ogni processo IT in modo che sia ripetibile e produca i risultati attesi in modo coerente. Fornisce una sequenza di attività logica e ripetibile che porti ai risultati desiderati e sia sufficientemente agile da gestire eccezioni ed emergenze. Utilizza processi standard, ove possibile, e li personalizza solo quando ciò sia inevitabile.

PC4 Ruoli e responsabilità

Definisce le attività chiave e risultati finali del processo. Assegna e comunica ruoli e responsabilità non ambigue per l'efficace ed efficiente esecuzione delle attività chiave e la loro documentazione, onochè la responsabilità per il processo e relativi risultati.

PC5 Politiche, Piani e Procedure

Definisce e comunica come le politiche, i piani e le procedure che gestiscono un processo IT debbano essere documentati, revisionati, mantenuti, approvati, archiviati e utilizzati per la formazione. Assegna responsabilità per ognuna di queste attività e, ad intervalli stabiliti, il monitoraggio della loro corretta esecuzione. Assicura che le politiche, piani e procedure siano accessibili, corrette, comprese e aggiornate.

PC6 Miglioramento delle prestazioni di processo

Identifica una serie di metriche che forniscono una visione dei risultati e prestazioni di processo. Stabilisce obiettivi che si riflettono sugli obiettivi di processo e sui relativi indicatori che abilitano il raggiungimento degli obiettivi di processo. Definisce come devono essere ottenuti i dati. Confronta misurazioni rilevate con quelle attese e persegue opportune azioni sulle eventuali deviazioni. Allinea le metriche, gli obiettivi e i metodi con l'approccio complessivo al monitoraggio dell'IT.

Dei controlli efficaci riducono il rischio, aumentano la possibilità di produrre valore e migliorano l'efficienza in quanto si verificheranno meno errori e l'approccio del management sarà più coerente.

Inoltre, per ogni processo il COBIT fornisce esempi descrittivi, e quindi non rigorosi o esaustivi, di:

- Input e risultati(output) generici
- Tabelle RACI con attività e indicazioni di ruoli e responsabilità
- Obiettivi principali (le cose più importanti da fare)
- Metriche

Oltre a ciò, per comprendere quali controlli siano necessari, i responsabili di processo devono capire quali input devono ricevere dagli altri e quali devono ricevere gli altri da quel processo. COBIT fornisce un esempio generico dei principali input dei risultati di ogni processo, inclusi quelli richiesti dall'esterno. Ci sono alcuni risultati che rappresentano degli input in tutti gli altri processi, e sono contrassegnati con "ALL" nelle tabelle degli output, ma non vengono citati come input in tutti i processi: tipicamente si tratta di standard di qualità e requisiti di misurazione, il quadro di riferimento dei processi IT, ruoli e responsabilità documentati, il quadro di riferimento per il controllo dell'IT da parte dell'azienda, le politiche IT ed i ruoli e le responsabilità del personale.

La comprensione dei ruoli e delle responsabilità per ogni processo è un aspetto cruciale per un governo efficace. COBIT fornisce una tabella RACI (acronimo di *Responsible, Accountable, Consulted and Informed*) per ogni processo. "Accountable" si riferisce al soggetto che fornisce direttive ed autorizza un'attività. "Responsible" si riferisce al soggetto che fa eseguire un lavoro. Gli altri due ruoli ("Consulted" e "Informed") assicurano che il processo preveda la partecipazione ed il coinvolgimento di tutti quelli che ne hanno necessità.

CONTROLLI AZIENDALI E CONTROLLI IT

Il sistema di controllo interno dell'azienda ha un triplice impatto sull'IT:

- A livello di alta direzione, si definiscono gli obiettivi aziendali, si stabiliscono le politiche e si prendono decisioni su come distribuire e gestire le risorse per mettere in pratica le strategie dell'impresa. In generale, l'approccio alla governance ed al controllo è definito dal consiglio di amministrazione e comunicato a tutta l'impresa. L'ambiente di controllo IT è guidato da questo insieme di obiettivi e politiche di alto livello.
- A livello di processo aziendale, i controlli sono applicati a specifiche attività aziendali. La maggior parte dei processi aziendali sono automatizzati ed integrati con sistemi applicativi dell'IT, il che implica che molti dei controlli effettuati a questo livello sono anch'essi automatizzati. Tali controlli sono conosciuti come controlli applicativi. Tuttavia, alcuni controlli, quali l'autorizzazione delle transazioni, la separazione dei compiti e le riconciliazioni manuali, all'interno del processo aziendale continuano ad essere effettuati manualmente. Pertanto, i controlli a livello di processo aziendale sono una combinazione di controlli manuali svolti dall'azienda, controlli aziendali e controlli applicativi automatizzati. Sono tutti responsabilità dell'azienda, che li definisce e li gestisce, anche se è necessario il supporto dell'IT per progettare e sviluppare i controlli applicativi.
- Per supportare i processi aziendali, l'IT fornisce i propri servizi, solitamente condivisi tra più processi aziendali, in quanto molti dei processi IT, sia di sviluppo che operativi, sono erogati all'intera impresa e buona parte dell'infrastruttura IT fornisce servizi comuni (per esempio le reti, i database, i sistemi operativi e le unità di memorizzazione). I controlli relativi a tutte le attività dei servizi IT sono conosciuti come controlli generali IT. L'affidabilità del funzionamento di tali controlli generali è necessaria per porre fiducia nei controlli applicativi. Per esempio, una scarsa gestione del cambiamento potrebbe mettere a rischio (accidentalmente o per azione deliberata) l'affidabilità dei controlli di integrità automatizzati.

CONTROLLI GENERALI E CONTROLLI APPLICATIVI DELL'IT

I controlli generali sono quei controlli contenuti nei processi e nei servizi IT, quali per esempio:

- Sviluppo dei sistemi
- Gestione del cambiamento
- Sicurezza
- Esercizio dei sistemi

I controlli integrati nei processi aziendali si definiscono solitamente controlli applicativi. Come esempi possiamo citare:

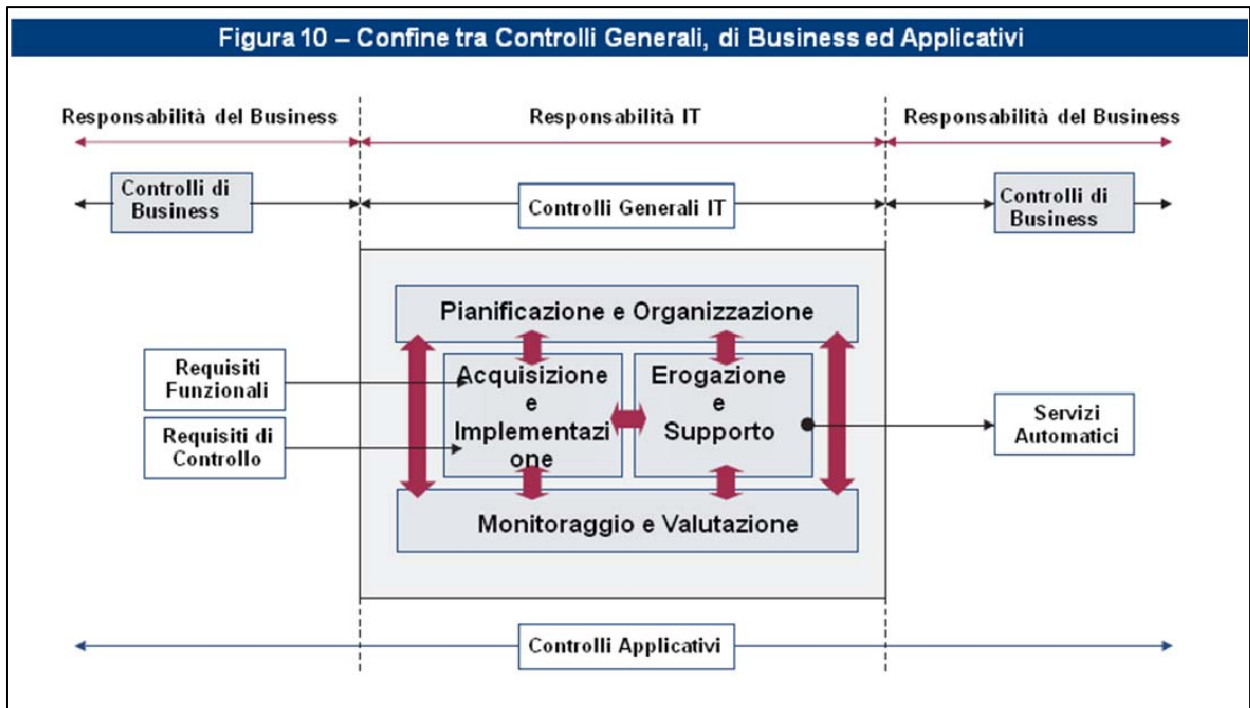
- Completezza
- Accuratezza
- Validità
- Autorizzazione
- Separazione dei compiti

COBIT presuppone che la progettazione e l'implementazione dei controlli applicativi automatizzati siano responsabilità dell'IT, descritti nel dominio Acquisizione e Implementazione, e si basano sui requisiti aziendali definiti utilizzando i criteri di valutazione delle informazioni di COBIT, come illustrato in **figura 10**. La responsabilità per la gestione operativa ed il controllo dei controlli applicativi non è dell'IT, ma del referente del processo aziendale.

Perciò, la responsabilità dei controlli applicativi è congiunta (end-to-end) tra il business e l'IT, ma la natura della responsabilità si differenzia come di seguito descritto:

- Il business è responsabile di:
 - Definire i requisiti funzionali e di controllo
 - Utilizzare servizi automatizzati
- IT è responsabile di:
 - Automatizzare ed implementare i requisiti funzionali e di controllo stabiliti dal business
 - Stabilire i controlli atti a mantenere l'integrità dei controlli applicativi

Per questa ragione i processi IT di COBIT coprono i controlli generali IT, ma solo per quanto concerne gli aspetti attinenti allo sviluppo dei controlli applicativi; la responsabilità per l'attuazione e la definizione di tali controlli nella prassi è di competenza delle aree operative (di business).



La seguente lista fornisce un insieme degli obiettivi dei controlli applicativi raccomandati. Sono identificati dal codice ACn, che sta per Controllo Applicativo ed il progressivo relativo.

AC1 Autorizzazione e preparazione dei dati

Provvedere affinché i documenti con le informazioni in input siano preparati da personale qualificato seguendo procedure formalizzate, in un contesto di adeguata segregazione funzionale riferita all'origine e dall'approvazione dei documenti. Errori o omissioni devono essere ridotti da un buon design degli schemi di input. Rilevare errori e anomalie in modo tale da consentirne la registrazione e la correzione.

AC2 Raccolta ed inserimento dei dati

L'introduzione dei dati è svolta in modo puntuale da personale autorizzato e competente. La correzione e la reintroduzione di dati erroneamente introdotti dovrebbe essere svolta senza compromettere i livelli di autorizzazione originariamente assegnati alle transazioni. Laddove necessario per la tracciatura delle operazioni, conservare i documenti originari per un intervallo di tempo adeguato.

AC3 Controlli di autorizzazione, accuratezza e completezza

Assicurare l'accuratezza delle transazioni, la loro completezza e validità. Sono predisposte procedure per assicurare che i dati inseriti siano convalidati o respinti quanto più possibile vicino al punto in cui sono originati.

AC4 Validità ed integrità dell'elaborazione dei dati

Sono in atto procedure per assicurare che l'integrità e la validità dei dati attraverso l'intero ciclo di elaborazione. La rilevazione di transazioni errate non pregiudica l'elaborazione delle transazioni valide.

AC5 Revisione dei dati prodotti, riconciliazione e trattamento degli errori

Sono in atto procedure e relative responsabilità, per assicurare che sia mantenuta la sicurezza dei report prodotti, che siano consegnati ai destinatari corretti e che siano protetti durante la trasmissione. Inoltre sono predisposte procedure per identificare e trattare gli errori contenuti nell'output e per accertare che le informazioni generate in input siano effettivamente utilizzate.

AC6 Integrità ed autenticazione delle transazioni

Procedure per il controllo dell'autenticità dell'origine, dell'integrità del contenuto e dell'esatto indirizzamento assicurano la correttezza del trasferimento dei dati dalle applicazioni interne verso le funzioni di business (sia interne che esterne all'azienda). Durante la trasmissione ed il trasporto si pongono in essere adeguate misure di protezione contro accessi non autorizzati, modifiche o errori di indirizzo.

Basato sulla misurazione

Una necessità fondamentale per ogni impresa è comprendere lo stato del proprio sistema IT e decidere di quale livello di gestione e controllo abbia bisogno. Per decidere correttamente, il management dovrebbe chiedersi: Quanto lontano dobbiamo andare, i benefici giustificheranno i costi?

Non è però facile ottenere una visione oggettiva del livello della performance della propria impresa. Cosa deve essere misurato e come? L'impresa ha bisogno di valutare dove si trova e dove sono necessari dei miglioramenti, ed implementare strumenti di gestione per monitorare questi miglioramenti.

COBIT tratta questi argomenti fornendo:

- Modelli di maturità che consentono il confronto e l'identificazione dei necessari miglioramenti della capacità
- Obiettivi e metriche per le prestazioni dei processi IT, che dimostrano come i processi soddisfino gli obiettivi aziendali e dell'IT e siano utilizzati per misurare la performance dei processi interni basandosi sul principio della *balanced scorecard*
- Obiettivi delle attività per permettere una performance efficace dei processi

I MODELLI DI MATURITÀ

All'alta direzione delle imprese pubbliche e private è sempre più spesso richiesto di considerare la qualità della gestione dell'IT. In risposta a ciò, si richiedono lo sviluppo ed il miglioramento dei casi aziendali ed il raggiungimento di un appropriato livello di gestione e di controllo dell'infrastruttura IT.

Per quanto pochi oserebbero sostenere che ciò non è cosa buona, si devono considerare il rapporto costi-benefici e le seguenti domande:

- Cosa stanno facendo le imprese concorrenti, e come siamo posizionati rispetto a loro?
- Quale è una best practice accettabile nel nostro settore e come siamo posizionati rispetto a questa prassi?
- Sulla base di tali confronti, si può dire che stiamo facendo abbastanza?
- Come identifichiamo che cosa è necessario fare per raggiungere un adeguato livello di gestione e controllo dei nostri processi IT?

Può essere difficile dare risposte significative a queste domande. Il management di IT è costantemente alla ricerca di strumenti di confronto e autovalutazione per rispondere all'esigenza di sapere cosa fare in modo efficiente. Partendo dai processi e dagli obiettivi di controllo di alto livello di COBIT, il referente del processo dovrebbe essere in grado di sviluppare progressivamente i confronti con gli obiettivi di controllo. Ciò soddisfa tre

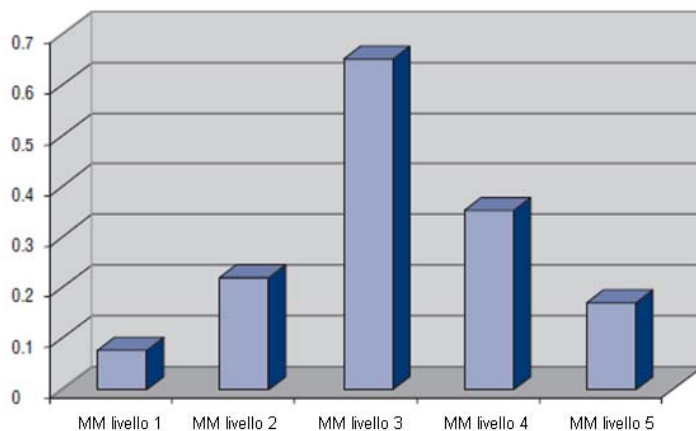
esigenze:

- 1 una valutazione relativa di dove si trovi l'impresa
- 2 un modo per decidere efficientemente dove andare
- 3 uno strumento per misurare i progressi rispetto all'obiettivo

La definizione di modelli di maturità per la gestione ed il controllo dei processi IT è basata su un metodo di autovalutazione dell'organizzazione, che può valutare il proprio livello da non esistente (0) a ottimizzato (5). Questo approccio è derivato dal modello di maturità che il Software Engineering Institute (SEI) ha definito per la maturità della capacità di sviluppo del software. Nonostante sia stato seguito l'approccio SEI, l'implementazione di COBIT si è diversificata da quest'ultima che è orientata ai principi di ingegneria del software, cercando di portare l'organizzazione verso l'eccellenza in queste aree ed ad una valutazione formale dei livelli di maturità in modo da ottenere una certificazione dello sviluppo del software. In COBIT, è fornita una definizione generale di grado di maturità, che è simile al CMM ma rivista in funzione della natura dei processi di gestione IT di COBIT. Qualsiasi sia il modello, le scale non devono essere troppo granulari, in quanto ciò renderebbe il sistema difficile da utilizzare e suggerirebbe un grado di precisione non giustificabile; in generale, infatti, l'obiettivo è identificare dove sono gli aspetti critici e come attribuire le priorità per migliorarli. L'obiettivo non è di valutare il livello di aderenza agli obiettivi di controllo.

I livelli di maturità sono intesi come profili dei processi IT che un'azienda potrebbe riconoscere come descrizioni dei possibili stati presenti e futuri. Non sono stati predisposti per essere utilizzati come modelli soglia, in cui non ci si può spostare al livello superiore senza aver soddisfatto tutte le condizioni del livello precedente. Con il modello di maturità di COBIT, diversamente dall'approccio originale SEI CMM, non c'è l'intenzione di misurare i livelli con precisione o provare a certificare un preciso livello raggiunto. Una verifica secondo il modello di maturità di COBIT equivale ad identificare un profilo in cui molte condizioni rilevanti dei livelli di maturità siano raggiunte, come illustrato nel disegno di **figura 11**.

Figura 11 – Possibile Livello di Maturità di un Processo IT



Possibili livelli di maturità di un processo IT. L'esempio illustra un processo che è largamente posizionato ad un livello 3 ma persistono alcuni problemi di compliance con bassi livelli di requisiti malgrado l'investimento in misurazioni delle performance (livello 4) e ottimizzazione (livello 5)

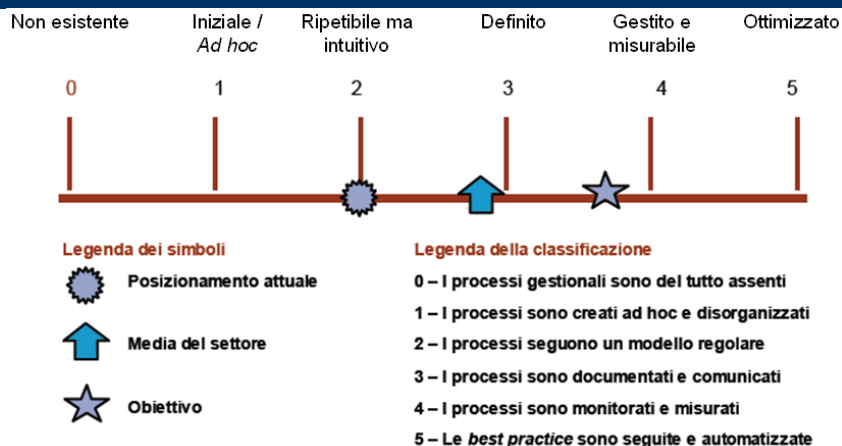
Questo perché quando si verifica la maturità attraverso i modelli di COBIT, capita spesso che qualche attività sia operante in modo incompleto o insufficiente tra diversi livelli. Questo punto di forza può essere usato per migliorare il grado di maturità. Per esempio, alcune parti del processo possono essere ben definite mentre altre possono risultare mancanti o incomplete.

Utilizzando i modelli di maturità sviluppati per ognuno dei 34 processi di COBIT, il management può identificare:

- l'effettiva performance dell'impresa – dove si trova oggi l'impresa
- lo stato attuale del settore di attività – il confronto
- l'obiettivo dell'impresa per il proprio sviluppo – dove l'impresa vuole andare
- il percorso necessario per andare dalla situazione attuale (as-is) a quella desiderata (to-be)

Per fare in modo che i risultati siano facilmente utilizzabili negli incontri del management, in cui tali risultati saranno presentati a supporto del caso aziendale in vista di una pianificazione futura, è necessario fornire un metodo di presentazione grafica (figura 12).

Figura 12 – Rappresentazione grafica dei modelli di maturità



Lo sviluppo si è basato sulle descrizioni dei modelli generici di maturità indicati nella figura 13.

COBIT è uno schema di riferimento sviluppato per la gestione dei processi IT orientati particolarmente al controllo. Queste scale devono essere semplici da applicare e ragionevolmente facili da comprendere. Il tema della gestione dei processi IT è intrinsecamente complesso e soggettivo e, quindi, si può affrontare più facilmente attraverso valutazioni facilitate che mirino ad aumentare il livello di consapevolezza, ottengano ampio consenso e motivino il miglioramento. Queste valutazioni possono essere fatte sia rispetto alle descrizioni dei livelli di maturità nel loro insieme o con più rigore rispetto alle singole affermazioni fatte nelle varie descrizioni. In ogni caso è necessario avere esperienza nel processo aziendale sotto analisi.

Il vantaggio di un approccio basato sul modello di maturità è che è relativamente facile per il management posizionarsi sulla scala e valutare le implicazioni se è richiesto un miglioramento della performance. La scala include il valore 0 perché è possibile che non esista alcun processo. La scala da 0 a 5 è basata su una semplice scala di maturità che mostra come un processo si evolve da una capacità non esistente ad una ottimizzata.

IL MODELLO DI RIFERIMENTO DI COBIT

Tuttavia, la capacità di gestione del processo non corrisponde alla prestazione del processo. La capacità richiesta, così come determinata dagli obiettivi aziendali ed IT, potrebbe non dover essere applicata allo stesso livello nell'intero ambiente IT, ma per esempio in modo non sistematico o limitatamente ad un numero ristretto di sistemi o unità. La misurazione della prestazione, come descritto nel paragrafo successivo, è essenziale nella determinazione di quale sia l'effettiva performance dell'impresa rispetto ai suoi processi IT.

Figura 13 – Modello di maturità generale o Gradi di strutturazione generali

0 Non esistente - Assenza completa di qualsiasi processo riconoscibile. L'impresa non si è nemmeno resa conto che esiste un problema da affrontare.

1 Iniziale / Ad hoc - C'è evidenza che l'impresa ha riconosciuto che i problemi esistono e che devono essere affrontati. Tuttavia non esistono processi standardizzati, bensì approcci *ad hoc* che tendenzialmente vengono applicati su base individuale o caso per caso. L'approccio complessivo alla gestione non è organico.

2 Ripetibile ma intuitivo - I processi sono stati sviluppati fino allo stadio in cui le persone che svolgono la stessa attività adottano procedure simili. Non esiste un processo formale di formazione o di comunicazione delle procedure standard, e la responsabilità è lasciata ai singoli. Si fa grande affidamento sulle conoscenze dei singoli e, conseguentemente, gli errori sono probabili.

3 Definito - Le procedure sono state standardizzate, documentate e comunicate nel corso di sessioni di formazione. E' obbligatorio applicare questi processi, tuttavia è abbastanza improbabile che le deroghe siano individuate. Le procedure stesse non sono sofisticate, ma rappresentano la formalizzazione delle prassi esistenti.

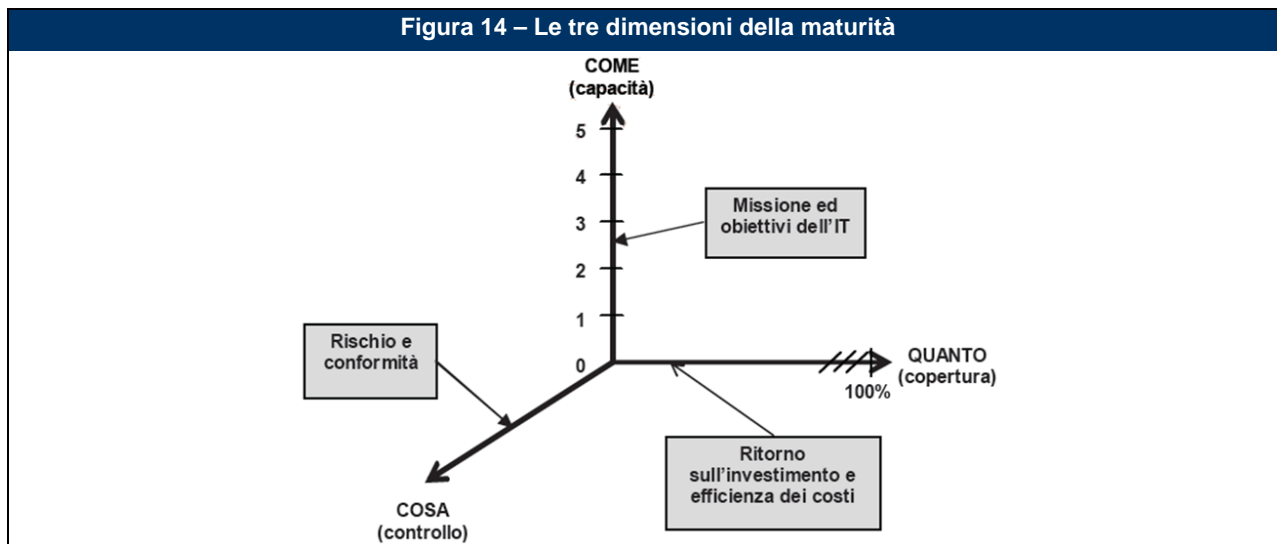
4 Gestito e Misurabile - Il management misura e monitora la conformità alle procedure e adotta misure correttive nel caso in cui i processi non funzionino efficacemente. I processi sono sottoposti ad un costante miglioramento e forniscono buone prassi. L'uso dell'automazione e degli strumenti è limitato o frammentario.

5 Ottimizzato - I processi sono stati portati ad un livello di *good practice*, basandosi sui risultati di un continuo miglioramento e confrontando il grado di strutturazione con altre imprese. L'IT è utilizzato in modo integrato per automatizzare il workflow, fornire strumenti per migliorare qualità ed efficacia e rendere l'impresa più veloce nell'adattarsi ai cambiamenti.

Sebbene una capacità applicata in modo appropriato sia già in grado di ridurre i rischi, un'impresa deve comunque analizzare i controlli necessari per assicurare che il rischio sia mitigato e che si ottenga valore rimanendo in linea con la propensione al rischio e gli obiettivi dell'azienda. Tali controlli sono indicati dagli obiettivi di controllo di COBIT. L'Appendice III fornisce un modello di maturità sul controllo interno che illustra la maturità di un'impresa per quanto riguarda la creazione e la performance del controllo interno. Spesso, tale analisi viene effettuata in risposta a sollecitazioni esterne, ma idealmente dovrebbe essere istituzionalizzata, come documentato dai processi di COBIT P06 *Comunicare gli obiettivi ed indirizzi della direzione* e ME2 *Monitorare e valutare il controllo interno*.

Capacità, prestazione e controllo rappresentano gli aspetti della maturità del processo, come illustrato nella **figura 14**.

Figura 14 – Le tre dimensioni della maturità



Il modello di maturità è un modo per misurare il livello dei processi sviluppati dal management, cioè quanto siano effettivamente adeguati. Il livello di sviluppo o l'adeguatezza che dovrebbero raggiungere dipendono innanzitutto dagli obiettivi IT e dalle esigenze aziendali che essi devono supportare. Quanto di quella capacità è effettivamente impiegata dipende in larga parte dal ritorno che un'impresa vuole dai propri investimenti. Per esempio, ci potrebbero essere processi e sistemi critici che necessitano una gestione della sicurezza maggiore e più accurata rispetto a quella richiesta da quelli meno critici. D'altro lato, il grado e la sofisticazione dei controlli che devono essere applicati in un processo sono influenzati principalmente dalla propensione al rischio dell'impresa e dai requisiti di conformità applicabili.

I livelli del modello di maturità aiuteranno gli specialisti a spiegare ai manager dove esistano carenze nella gestione dei processi IT e a fissare gli obiettivi da raggiungere. Il corretto livello di maturità sarà influenzato dagli obiettivi aziendali dell'impresa, dall'ambiente operativo e dalle prassi del settore. Precisamente, il livello di maturità della gestione dipenderà dalla dipendenza dell'impresa dall'IT, dalla complessità della propria tecnologia e, soprattutto, dal valore delle proprie informazioni.

Un punto di riferimento strategico per l'impresa che intende migliorare la gestione ed il controllo dei processi IT si può trovare negli standard internazionali emergenti e nelle best practice. Le prassi che sono oggi emergenti potranno rappresentare un domani il livello atteso della performance e per questo sono utili nella pianificazione delle aziende che vogliono essere in anticipo sui tempi.

I modelli di maturità sono costruiti a partire dal modello qualitativo generico (vedi **figura 13**), cui si aggiungono in maniera crescente con l'aumentare del livello i criteri derivanti dai seguenti attributi:

- Consapevolezza e comunicazione
- Politiche, piani e procedure
- Strumenti ed automazione
- Esperienza e competenze
- Responsabilità e accountability
- Definizione e misurazione degli obiettivi

La tabella degli attributi di maturità mostrata in **figura 15** elenca le caratteristiche delle modalità di gestione dei processi IT e descrive come si evolvono dallo stato di "non esistente" a quello di "ottimizzato". Questi attributi possono essere utilizzati per valutazioni più complessive, analisi delle varianze e pianificazione dei miglioramenti.

In sintesi, i modelli di maturità forniscono un profilo generico degli stadi attraverso cui l'impresa evolve per la gestione ed il controllo dei processi IT, e sono:

- un insieme di requisiti e gli aspetti abilitanti ai vari livelli di maturità
- una scala che permette di misurare facilmente le differenze
- una scala che si presta ad un confronto pragmatico
- una base per definire la posizione attuale ("as-is") e quella desiderata ("to-be")
- un supporto per l'analisi delle varianze per determinare cosa debba essere fatto al fine di raggiungere il livello prescelto
- nel loro insieme, una visione delle modalità di gestione dell'IT nell'impresa.

I modelli di maturità di COBIT si focalizzano sulla capacità, ma non necessariamente sulla performance. Non sono numeri da raggiungere, né sono stati pensati per presentare livelli soglia ufficiali difficili da passare ai fini di una certificazione. Comunque sono stati pensati per essere sempre applicabili, ed i loro livelli forniscono descrizioni tra le quali l'impresa può riconoscere quella che più si adatta ai propri processi. Il livello giusto è determinato dal tipo di impresa, dal suo ambiente e dalla sua strategia.

Il grado di copertura, il dettaglio del controllo, e come la capacità sia utilizzata e fornita, sono decisioni soggette ad una analisi costi-benefici. La performance, o il modo di utilizzare più o meno efficacemente le capacità, dipendono da decisioni basate sul rapporto costi-benefici. Per esempio, un alto livello di gestione della sicurezza può doversi concentrare solo sui sistemi maggiormente critici.

Infine, mentre il controllo sul processo aumenta con l'aumentare del livello di maturità, l'impresa ha ancora bisogno di analizzare quale meccanismo di controllo debba applicare, sulla base di fattori di rischio e di valore. In tale analisi, un aiuto proviene dagli obiettivi generici dell'azienda e dell'IT definiti in questo schema di riferimento. I meccanismi di controllo sono guidati dagli obiettivi di controllo di COBIT e si concentrano sui contenuti del processo, mentre i modelli di maturità si concentrano principalmente sulla qualità della gestione del processo. L'Appendice III fornisce un modello di maturità generico che illustra lo stato dell'ambiente di controllo interno e l'istituzione dei controlli interni di un'azienda.

L'ambiente di controllo può risultare implementato in modo appropriato una volta che si siano presi in considerazione tutti e tre gli aspetti della maturità (capacità, performance e controllo). Il miglioramento della maturità riduce il rischio e migliora l'efficienza, in quanto porta a ridurre gli errori, avere processi più prevedibili ed utilizzare le risorse con una efficienza dei costi.

MISURAZIONE DELLA PERFORMANCE

Obiettivi e metriche sono definiti in COBIT su tre livelli:

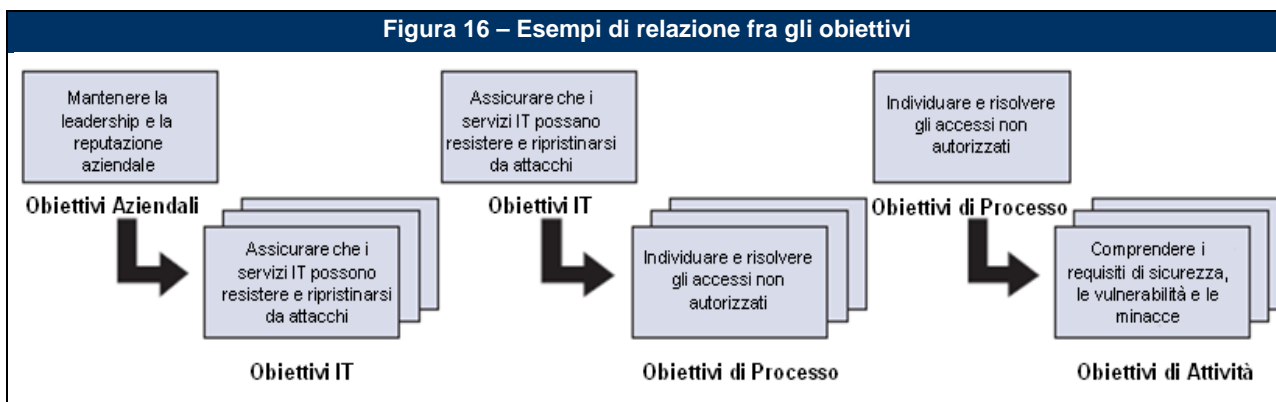
- obiettivi IT e metriche che definiscono cosa il business si aspetta dall'IT e come misurarli
- obiettivi di processo e metriche che definiscono cosa deve produrre il processo IT per supportare gli obiettivi dell'IT e come misurarli
- obiettivi delle attività e metriche in modo che sia stabilito cosa è necessario accadere all'interno del processo per ottenere la performance richiesta e come misurare tutto ciò

IL MODELLO DI RIFERIMENTO DI COBIT

Figura 15 – Tabella degli attributi di maturità

Conspicuità e Comunicazione	Politiche, standard e procedure	Strumenti ed automazione	Competenze ed esperienze	Responsabilità e accountability	Definizione e misurazione degli obiettivi
<p>1 Cresce il riconoscimento della necessità del processo.</p> <p>Comunicazione non così attiva da problemi.</p>	<p>Ci sono approcci ad hoc a processi e prassi.</p> <p>I processi e le politiche non sono definiti.</p>	<p>Possiamo esistere alcuni strumenti, ma si usano de facto ad hoc.</p> <p>No n vi è alcun approccio pianificato per l'uso di strumenti.</p>	<p>Le competenze richieste per i processi non sono identificate.</p> <p>No n esiste un piano di formazione né viene svolta attività formale di formazione.</p>	<p>Non c'è alcuna definizione di responsabilità e di accountability, intesa come capacità di rendere conto del proprio operato e permettere la tracciabilità delle proprie azioni. Le persone si assumono responsabilità in modo reattivo e per iniziativa personale.</p>	<p>Gli obiettivi non sono chiari e non viene effettuata alcuna misurazione.</p>
<p>2 Con consapevolezza della necessità di operare.</p> <p>Il management comunica le questioni generali.</p>	<p>Emergono processi simili e comuni, ma sono largamente intuitive e basati sulle conoscenze del singolo.</p> <p>Alcuni aspetti di processi sono ripetibili grazie alle conoscenze individuali ed è possibile che esistano documentazioni e una conoscenza informale di politiche e procedure.</p>	<p>Esistono metodologie comuni per l'utilizzo degli strumenti, ma si basano su soluzioni sviluppate da persone chiave.</p> <p>Forse si sono acquistati dei software sul mercato, ma probabilmente non vengono utilizzati correttamente o vengono addirittura lasciati inutilizzati.</p>	<p>Per le aree critiche si sono identificati requisiti minimi di competenza.</p> <p>La formazione viene effettuata in risposta alle necessità, piuttosto che sulla base di un piano concordato, e viene offerta "sul campo" in modo informale.</p>	<p>Un individuo si assume le proprie responsabilità e di solito è tenuto a rispondere, anche se ciò non è concordato formalmente. C'è confusione nell'attribuire la responsabilità in presenza di problemi e tende ad affermarsi la cultura della condanna.</p>	<p>Sono definiti alcuni obiettivi, sono stabilite alcune misure finanziarie, ma solo l'alta direzione è al corrente. Aree isolate sono soggette a monitoraggi discontinui.</p>
<p>3 Si comprende la necessità di operare.</p> <p>Il management è più formale e strutturato nelle proprie comunicazioni.</p>	<p>Cresce l'utilizzo di buone prassi.</p> <p>Processi, politiche e procedure sono definite e documentate per tutte le attività principali.</p>	<p>E' stato definito un piano per l'utilizzo e la standardizzazione di strumenti per automatizzare il processo.</p> <p>Gli strumenti sono utilizzati per le loro finalità di base, ma non sono necessariamente in linea con il piano concordato o integrati tra loro.</p>	<p>I requisiti di competenza sono definiti e documentati per ogni area.</p> <p>Un piano formale di formazione è stato sviluppato, ma l'attività formativa è ancora basata su iniziative personali.</p>	<p>Sono definite la responsabilità e la tracciabilità dei processi ed i referenti degli stessi sono stati identificati. E' improbabile che il referente del processo abbia piena autorità per esercitare la responsabilità.</p>	<p>Si sono definiti alcuni obiettivi ed misurazioni dell'efficacia ma non sono stati comunicati, e c'è un chiaro collegamento con gli obiettivi aziendali. Si usano processi di valutazione, ma sono applicati in modo discontinuo. In alcune aree si adottano le idee derivanti da bilanci scorrevoli, mentre l'applicazione dell'analisi delle cause principali rimane occasionale ed intuitiva.</p>
<p>4 Si comprendono tutti i requisiti.</p> <p>Sono utilizzate tecniche mature di comunicazione e vengono impiegati strumenti standard di comunicazione.</p>	<p>Il processo è affidabile e completo, vengono applicate best practice interne.</p> <p>Tutti gli aspetti del processo sono documentati e ripetibili. Le politiche sono state approvate e sottoscritte al management.</p> <p>Sono adottati e seguiti standard per lo sviluppo e la manutenzione dei processi e delle procedure.</p>	<p>Gli strumenti sono sviluppati sulla base di un piano standardizzato ed alcuni sono stati integrati con altri strumenti correlati.</p> <p>Gli strumenti sono usati nelle aree principali per automatizzare la gestione dei processi e monitorare attività e controlli critici.</p>	<p>I requisiti di competenza sono aggiornati e riferiti per tutte le aree, si assicurano alti livelli di competenza per tutte le aree critiche e si incoraggia la certificazione.</p> <p>Si applicano tecniche di formazione mature secondo il piano di formazione e si incoraggia la condivisione delle conoscenze. Si coinvolgono tutti gli esperti di dominio interni e si verifica l'efficacia di piano di formazione.</p>	<p>La responsabilità e la tracciabilità di processi sono definite e lavorano in modo che il referente del processo possa scaricare completamente la propria responsabilità. E in essere una cultura per niente che motiva le azioni positive.</p>	<p>L'efficacia e l'efficienza sono misurate e comunicate, collegate agli obiettivi aziendali ed al piano strategico IT. Si implementa il balanced scorecard di IT in alcune aree nelle quali il management ha riscontrato delle eccezioni e si sta standardizzando l'analisi delle cause principali. Si evidenzia un miglioramento continuo.</p>
<p>5 La comprensione dei requisiti è avanzata e prospettica.</p> <p>Esiste una comunicazione proattiva delle questioni basata sui trend evolutivi. Si utilizzano tecniche di comunicazione mature e si impiegano strumenti integrati di comunicazione.</p>	<p>Sono applicate best practice e standard esterni.</p> <p>La documentazione dei processi si è evoluta in un workflow automatico. Processi, politiche e procedure sono standardizzati ed integrati per consentire una gestione ed un miglioramento completi.</p>	<p>In tutta l'azienda si utilizzano strumenti di automazione standardizzati.</p> <p>Gli strumenti sono pienamente integrati con altri strumenti correlati per consentire un supporto completo ai processi.</p> <p>Gli strumenti sono utilizzati per supportare lo sviluppo dei processi ed individuare automaticamente le eccezioni da controllare.</p>	<p>L'azienda incontra regolarmente il continuo miglioramento delle proprie competenze, in base ad obiettivi chiari.</p> <p>Formazione ed istruzione supportano best practice esterne e l'uso di tecniche avanzate. La cultura di conoscenza e parte della cultura aziendale vengono sviluppati sistemi basati sulla conoscenza. Ci si vale della guida di esperti e leader di settore.</p>	<p>I referenti dei processi sono autorizzati a prendere decisioni ed agire. L'assegnazione delle responsabilità è messa a cascata ai vari livelli dell'organizzazione in modo coerente.</p>	<p>E' stato predisposto un sistema integrato di misurazione delle prestazioni che collega la performance IT con gli obiettivi aziendali applicando a livello globale l'IT balance ed scorecard. Le eccezioni sono registrate dal management regolarmente a livello globale si eseguono analisi delle cause principali. Il miglioramento continuo è un <i>modus operandi</i>.</p>

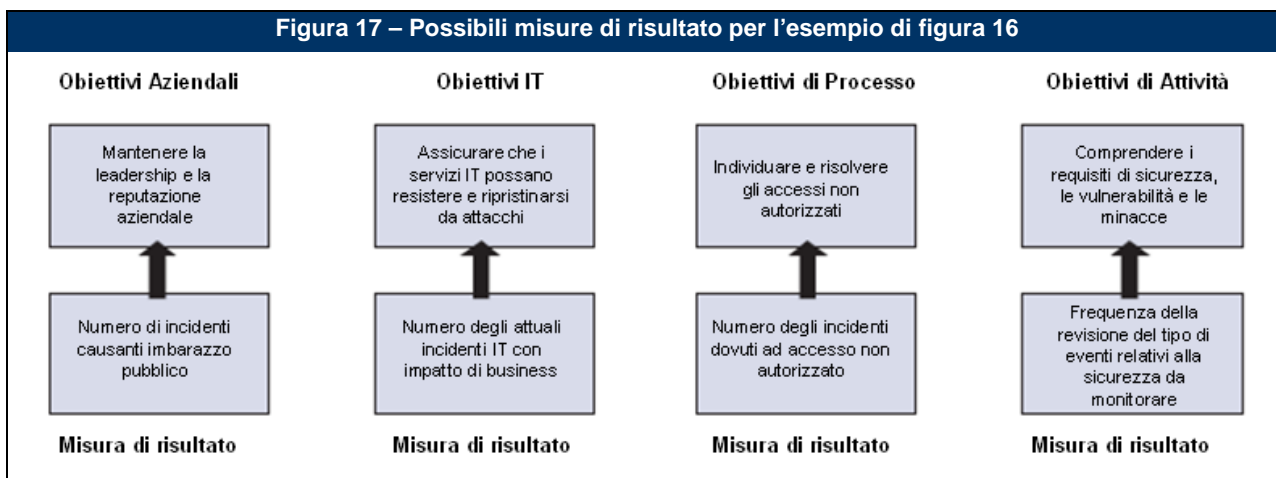
Gli obiettivi sono definiti top-down in modo tale che un obiettivo aziendale determina gli obiettivi IT che lo supportano. Un obiettivo IT è conseguito da un processo o dall'interazione di più processi. Pertanto, gli obiettivi IT aiutano a definire gli obiettivi dei processi. Similmente, ogni obiettivo di processo necessita di un certo numero di attività, di conseguenza definisce gli obiettivi delle attività. La **Figura 16** fornisce degli esempi di relazione tra gli obiettivi aziendali, IT, di processo e di attività.



I termini KGI e KPI, usati nelle precedenti versioni di COBIT, sono stati sostituiti con due tipi di metriche:

- Indicatori di risultato, precedentemente chiamati *indicatori chiave degli obiettivi* (KGI), definiscono se gli obiettivi sono stati conseguiti. Questi indicatori possono essere utilizzati solo a consuntivo dopo l'esecuzione della fase, e perciò sono chiamati "*lag indicators*" (indicatori "a posteriori" o "ex post").
- Indicatori di performance, precedentemente chiamati *indicatori chiave della performance* (KPI), definiscono se gli obiettivi saranno raggiunti. Questi indicatori possono essere utilizzati prima che il risultato sia ottenuto, e perciò sono chiamati "*lead indicators*" (indicatori di tendenza o "ex ante").

La **figura 17** illustra delle possibili misurazioni dei risultati e degli obiettivi degli esempi utilizzati.



Le misurazioni di risultato di un livello inferiore diventano indicatori di performance di un livello superiore. Come nell'esempio di **figura 16**, la misurazione di risultato che identifica la rilevazione e la risoluzione di un accesso non autorizzato, sia anche un indicatore per verificare se un servizio IT possa resistere ed essere ripristinato, in caso di attacco. Da cui, la misurazione di risultato diventa un indicatore di performance per l'obiettivo del livello superiore. La **figura 18** illustra come le misurazioni di risultato nell'esempio diventano metriche di performance.

Le misurazioni di risultato definiscono misure che dicono al management – a consuntivo – se una funzione, processo o attività IT ha raggiunto i propri obiettivi. Le misure di risultato delle funzioni IT sono solitamente espresse in termini di criteri di valutazione delle informazioni:

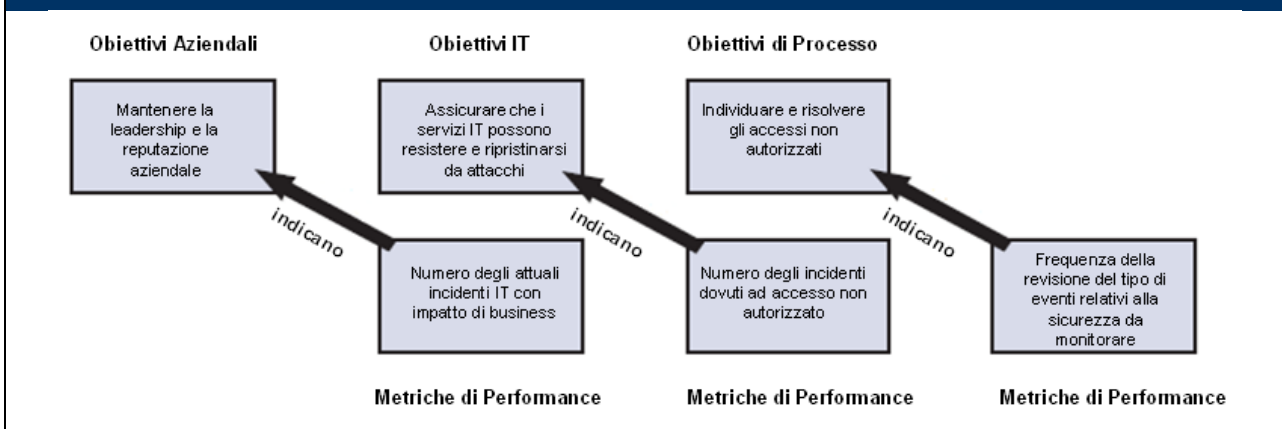
- disponibilità delle informazioni necessarie per supportare le esigenze aziendali
- assenza di rischi per l'integrità e la riservatezza
- efficienza dei costi di processi ed operazioni
- conferma di affidabilità, efficacia e conformità.

Gli indicatori di performance definiscono misure che determinano come il processo IT sta operando per consentire il raggiungimento degli obiettivi. Costituiscono i principali indicatori della probabilità che un obiettivo possa essere raggiunto o meno, pertanto indirizzando gli obiettivi di livello superiore. Spesso misurano la disponibilità di una adeguata capacità, esperienza e competenza, e del risultato delle sottostanti attività. Per esempio, un servizio fornito dall'IT è un obiettivo per l'IT stesso ma è un

IL MODELLO DI RIFERIMENTO DI COBIT

indicatore di performance e di capacità per il business. Ecco perché gli indicatori di performance sono talvolta indicati come *performance drivers*, soprattutto nelle *balanced scorecard*.

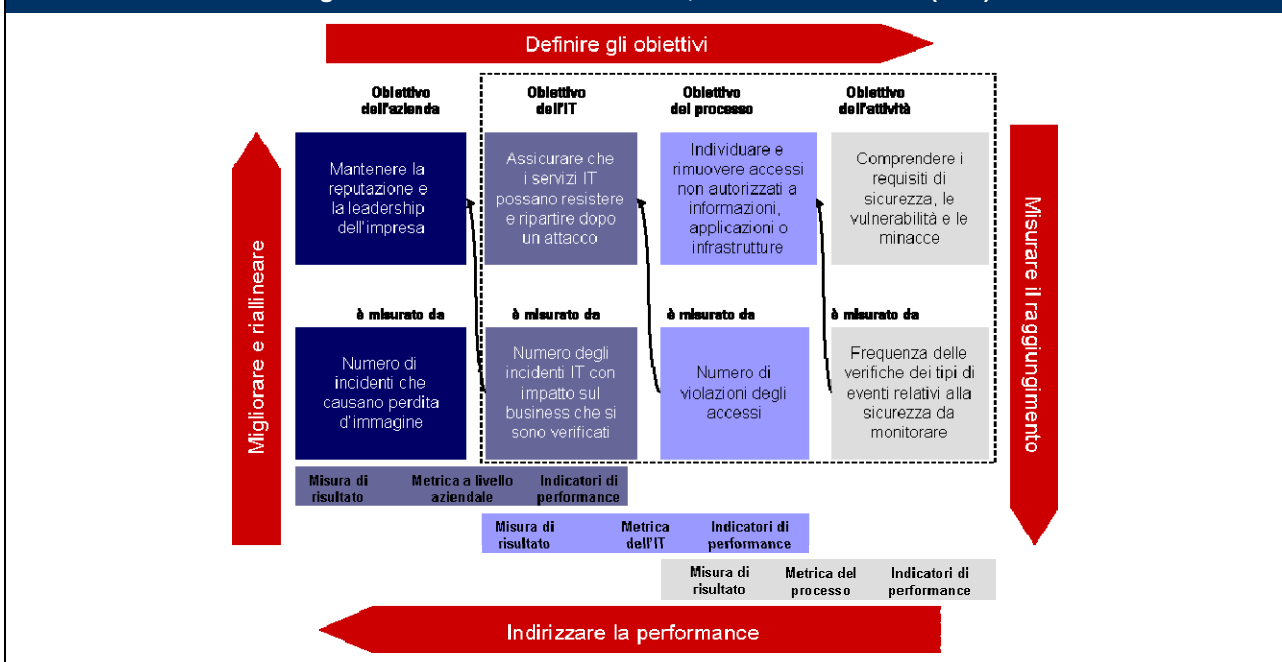
Figura 18 – Possibili Indicatori di Performance relative all'esempio in figura 16



Pertanto, le metriche fornite sono sia una misura di risultato delle funzioni IT, dei processi IT o degli obiettivi di attività che misurano, sia anche un indicatore di performance che supporta gli obiettivi di alto livello aziendali, delle funzioni IT o del processo IT.

La **figura 19** illustra la relazione tra gli obiettivi aziendali, dell'IT, dei processi e delle attività, e le varie metriche. Da sinistra in alto a destra in alto, sono illustrati gli obiettivi in cascata. Sotto l'obiettivo si trova la sua misurazione di risultato. La frecce sottili indicano che la stessa metrica è anche un indicatore di performance per l'obiettivo di livello superiore.

Figura 19 – Relazione tra Processi, Obiettivi e Metriche (DS5)



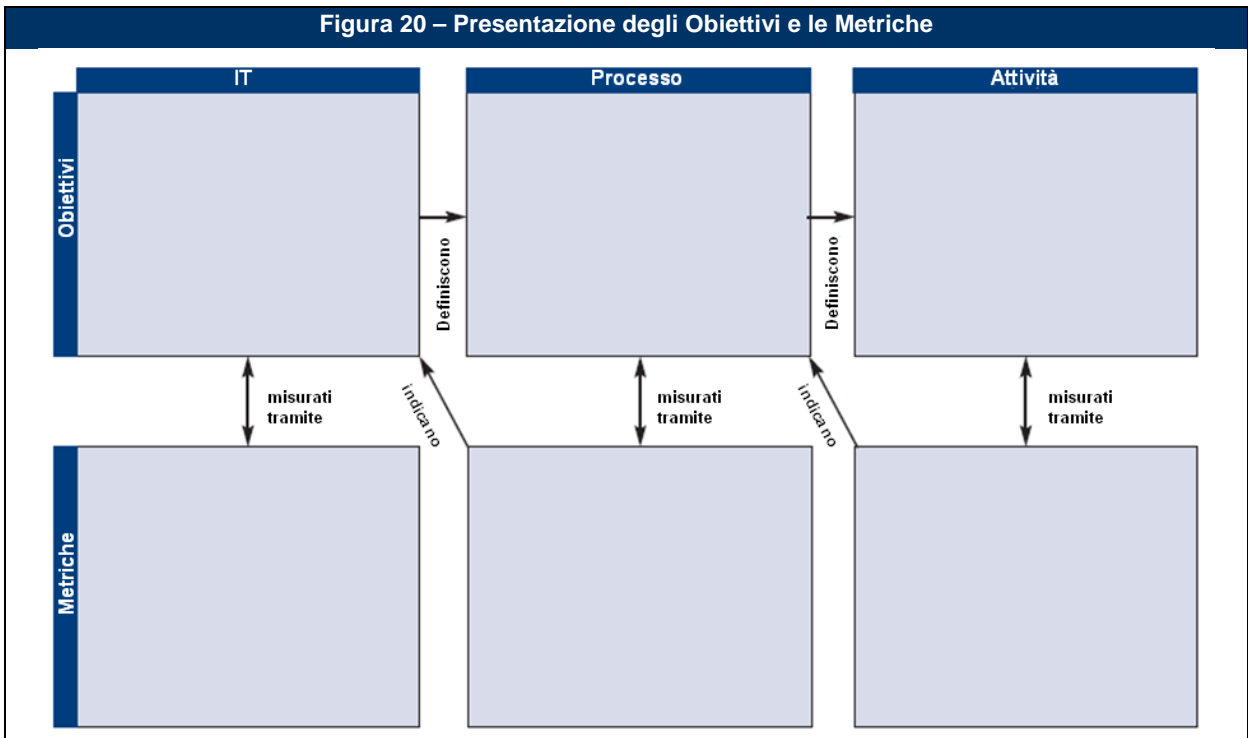
L'esempio è tratto dal processo "DS5 Assicurare la Sicurezza dei sistemi". COBIT fornisce metriche solo fino ai risultati degli obiettivi IT, come delimitato dalle linee tratteggiate. Anche se sono indicatori di performance per gli obiettivi di business per l'IT, COBIT non fornisce misure di risultato per gli obiettivi di business.

Gli obiettivi IT e di business utilizzati nella sezione delle metriche ed obiettivi di COBIT, comprese le rispettive relazioni, sono riportati nell'appendice I. Per ciascun processo IT di COBIT, sono illustrati gli obiettivi e le metriche, come si può osservare nella **figura 20**.

Le metriche sono state sviluppate considerando le seguenti caratteristiche:

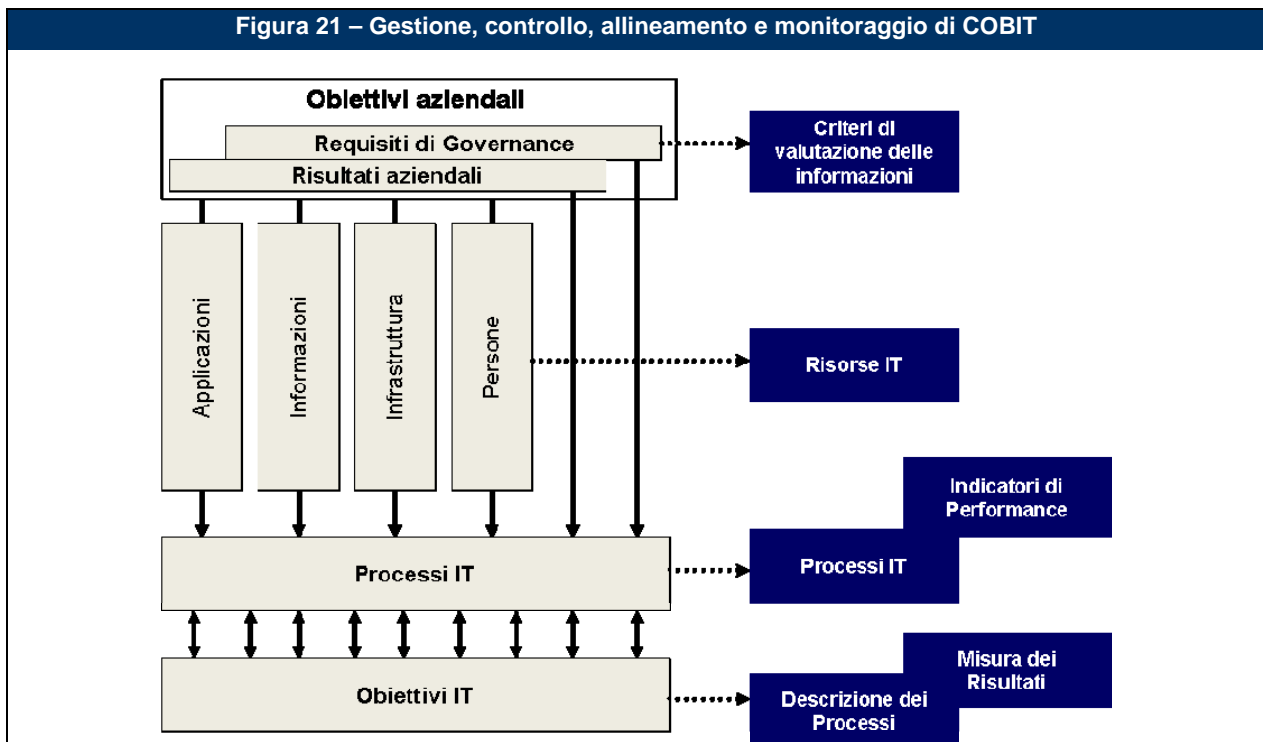
- Un elevato rapporto *insight-to-effort*, (cioè la concentrazione sulla performance e sul conseguimento dell'obiettivo a confronto dell'impegno per raggiungerlo)
- confrontabili internamente (per esempio, in percentuale rispetto ad una soglia o a valori nel tempo)
- confrontabili esternamente, a prescindere dalla dimensione dell'impresa o dal settore di attività

- meglio avere poche metriche buone (se ne può avere anche una sola molto buona, che può essere influenzata da fonti diverse) piuttosto che una lunga lista di metriche di qualità inferiore
- facile da misurare, e non essere confusa con gli obiettivi.

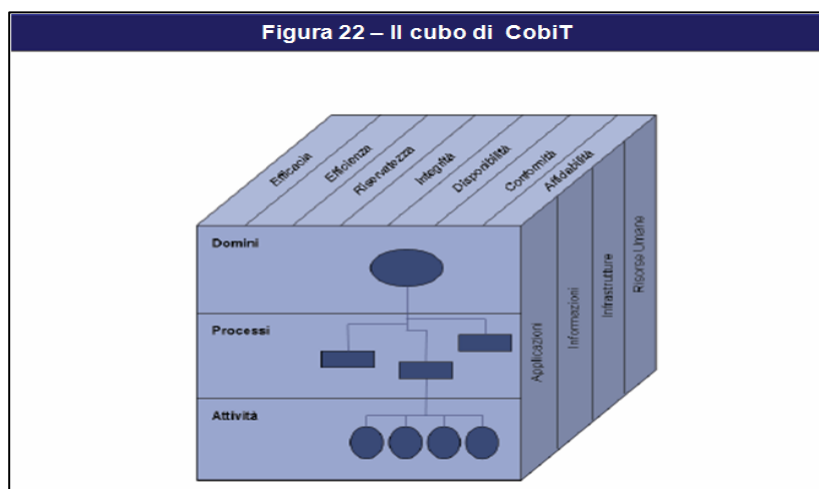


IL MODELLO DEL QUADRO DI RIFERIMENTO DI COBIT

Il quadro di riferimento di COBIT, pertanto, collega i requisiti informativi e di governo dell'azienda con gli obiettivi della funzione IT. Il modello di processo di COBIT permette di gestire e controllare adeguatamente le attività IT e le risorse che le supportano, basandosi sugli obiettivi di controllo di COBIT, permette di mantenerle allineate al business e monitorate utilizzando gli obiettivi e le metriche di COBIT, come mostrato nella **figura 21**.



In sintesi, le risorse IT sono gestite da processi IT per conseguire obiettivi IT che soddisfano requisiti aziendali. Questo è il principio base del modello di COBIT, come illustrato nel cubo di COBIT (figura 22).



Più in dettaglio, il quadro di riferimento di COBIT può essere rappresentato graficamente nel suo insieme come nella figura 23, con il modello di processo di COBIT strutturato in quattro domini, che raggruppano 34 processi generalizzati, e gestiscono le risorse IT per fornire all'azienda informazioni in linea con i requisiti aziendali e di governance.

L'accettabilità generale di COBIT

COBIT è basato sull'analisi e sull'armonizzazione degli standard IT e delle good practice esistenti ed è conforme ai principi di governo generalmente accettati. Si posiziona ad un alto livello, si basa sui requisiti aziendali, copre l'intera gamma delle attività dell'IT, e si concentra sugli obiettivi (*cosa*) da raggiungere piuttosto che sulle modalità (*come*) per raggiungere una governance, una gestione ed un controllo efficaci. Perciò, funge da integratore delle prassi di governance dell'IT e si rivolge all'alta direzione, alla direzione aziendale e dell'IT, ai *professional* delle aree governance, assurance/certificazione e sicurezza, così come ai *professional* dell'audit e del controllo informatico. È stato disegnato per essere complementare ad altri standard e good practice, ed essere usato assieme ad essi.

L'implementazione delle good practice deve essere coerente con il modello di riferimento per il governo ed il controllo dell'impresa, adeguata all'organizzazione, ed integrata con altri metodi e prassi in uso. Standard e good practice non sono una panacea e la loro efficacia dipende da come sono stati effettivamente implementati e mantenuti aggiornati. Risultano molto utili soprattutto quando sono applicati come espressione di un insieme di principi e come punto di partenza per predisporre procedure specifiche su misura. Per evitare che tali pratiche restino inutilizzate, il management e lo staff dovrebbero comprendere cosa fare, come farlo e perché è importante.

Per raggiungere l'allineamento delle good practice ai requisiti aziendali, si raccomanda di utilizzare COBIT al più alto livello, fornendo un modello di riferimento globale basato su un modello di processo IT che deve genericamente andare bene per ogni impresa. Prassi e standard specifici relativi ad aree diverse possono essere rilevati facendo riferimento a COBIT, fornendo così una serie di materiali strutturati da utilizzare come guida.

COBIT si rivolge a vari tipi di utenti:

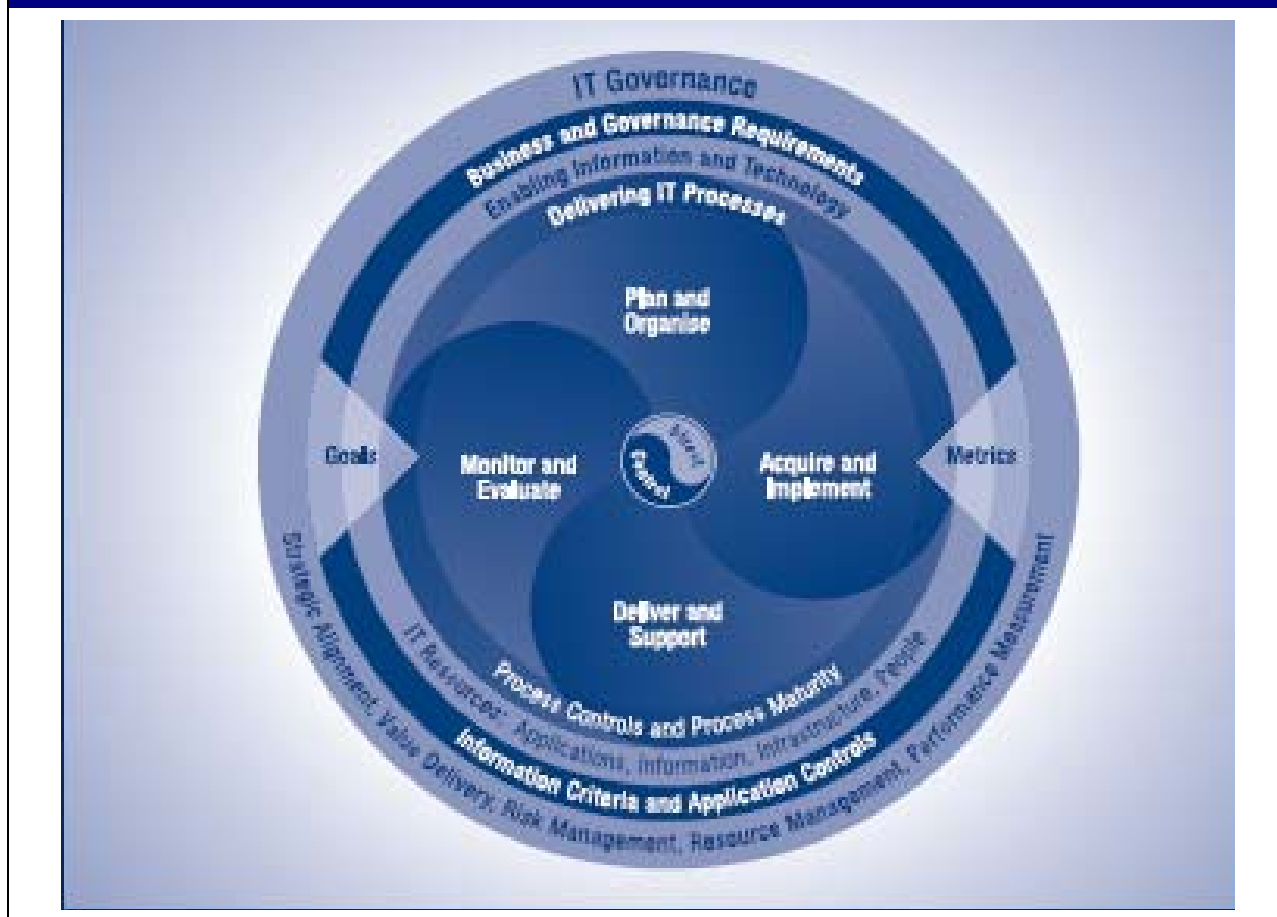
- **Alta Direzione (executive management)** – per ottenere valore dagli investimenti in IT e bilanciare i rischi e gli investimenti in controlli in un ambiente IT spesso imprevedibile
- **Dirigenti dell'azienda (business management)** – per ottenere assicurazioni sulla gestione e sul controllo dei servizi IT forniti da strutture interne o da terze parti
- **Dirigenti dell'IT (IT management)** – per fornire i servizi IT, richiesti dall'azienda per supportare la propria strategia, in modo controllato e gestito
- **Revisori (auditors)** – per sostanziare le loro opinioni e/o fornire raccomandazioni ai dirigenti in tema di controlli interni.

COBIT è stato sviluppato ed è gestito da un istituto di ricerca indipendente senza scopo di lucro, che si avvale dell'esperienza dei membri dei capitoli ad essa affiliati, degli esperti del settore, e di specialisti in materia di controlli e sicurezza. Il suo contenuto è basato sulla continua ricerca nelle good practice dell'IT ed è continuamente tenuto aggiornato, costituendo così una risorsa oggettiva e concreta per tutti i tipi di utente.

COBIT è orientato agli obiettivi e all'ambito del governo dell'IT, assicurando che il suo schema di riferimento per i controlli sia completo, allineato con i principi di governance dell'impresa e, perciò, accettabile da parte di consigli di amministrazione,

direzione, revisori e organismi di controllo. L'Appendice II riporta una mappatura di come gli obiettivi di controllo di COBIT si pongano nei confronti delle cinque aree della governance dell'IT e delle attività di controllo del COSO.

Figura 23 – Il quadro generale di riferimento di COBIT



La **figura 24** riassume come i diversi elementi dello schema di riferimento di COBIT si rapportano alle aree principali della governance dell'IT.

Figura 24 – Il quadro di riferimento di COBIT e le principali aree della Governance dell'IT

	Obiettivi	Metriche	Prassi	Modelli di maturità
Allineamento strategico	P	P		
Erogazione del valore		P	S	P
Gestione del rischio		S	P	S
Gestione delle risorse		S	P	P
Misurazione delle prestazioni	P	P		S

P = fattore primario S = fattore secondario

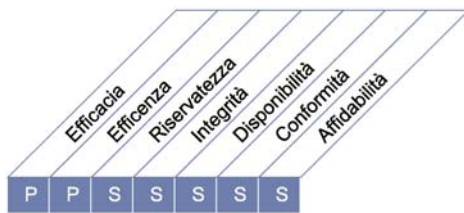
COME USARE QUESTO LIBRO

La navigazione attraverso lo schema di riferimento di COBIT

Per ognuno dei processi IT del COBIT si definisce un obiettivo di controllo di alto livello, che viene presentato insieme agli obiettivi chiave ed alle metriche in una struttura a cascata (figura 25).

Figura 25 – La navigazione nel modello di COBIT

Nell'ambito di ciascun processo, gli obiettivi di controllo sono presentati utilizzando descrizioni di azioni generalizzate del livello minimo di good practice di gestione tali da assicurare che il processo sia mantenuto sotto controllo.



Il controllo del processo IT :

titolo del processo

che soddisfa i requisiti aziendali per l'IT di

sintesi dei più importanti obiettivi IT pertinenti

ponendo l'attenzione su

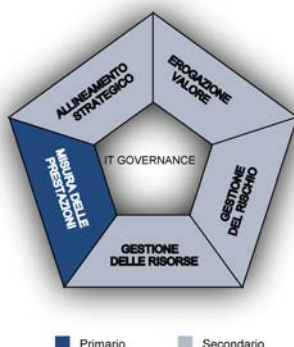
sintesi dei più importanti obiettivi del processo

è ottenuto tramite

obiettivi delle attività

e viene misurato tramite

metriche principali



Indice dei componenti principali di COBIT

Lo schema di riferimento di COBIT è popolato dai componenti principali, indicati nel corso di questa pubblicazione e organizzati nei 34 processi IT, che forniscono un quadro completo di come controllare, gestire, e misurare ogni processo. Ogni processo è sviluppato in quattro sezioni, ciascuna di circa una pagina, come segue:

- la Sezione 1 (Figura 25) contiene la descrizione del processo e la sintesi degli obiettivi, la descrizione è presentata attraverso un paradigma “a cascata”. Questa pagina inoltre mostra il rapporto tra il processo e i criteri di valutazione delle informazioni, le risorse IT e le relative aree di governo dell’IT indicando con una P le relazioni principali e con una S quelle secondarie.
- la Sezione 2 contiene gli obiettivi di controllo per questo processo.
- la Sezione 3 contiene gli input e output del processo, una tabella RACI, gli obiettivi e le metriche.
- la Sezione 4 contiene il modello di strutturazione del processo.

Un altro modo di vedere il contenuto della performance del processo è:

- Gli input di processo sono quelli che il referente del processo ha bisogno di ricevere dagli altri.
- Gli obiettivi di controllo descrivono quello che il referente del processo deve fare.
- Gli output di processo sono i risultati che il referente del processo deve produrre.
- Gli obiettivi e le metriche illustrano come il processo deve essere misurato.
- La tabella RACI definisce cosa deve essere delegato ed a chi.
- Il modello di strutturazione mostra cosa deve essere fatto per migliorare il processo.

I ruoli presenti nella tabella RACI sono classificati per tutti i processi come:

- Amministratore delegato o Direttore Generale (Chief Executive Officer – CEO)
- Direttore Amministrativo (Chief Financial Officer – CFO)
- Dirigenti aziendali – Direttori utenti del servizio IT
- Direttore dell’IT (Chief Information Officer – CIO)
- Referente del processo aziendale (Business Process Owner)
- Responsabile operativo
- Responsabile architetture IT
- Responsabile dello sviluppo IT
- Responsabile amministrativo dell’IT (per le imprese di grandi dimensioni, il responsabile di funzioni quali risorse umane, budgeting e controllo interno)
- La funzione o il Responsabile della gestione dei progetti (PMO)
- Conformità, audit, rischio e sicurezza (gruppi con responsabilità di controllo che non hanno responsabilità operative nell’IT)

Alcuni processi specifici prevedono ulteriori funzioni specializzate, come il service desk o l’incident manager nel DS8.

È bene precisare che mentre il materiale è stato raccolto da centinaia di esperti, a seguito di ricerche e verifiche rigorose, gli input, gli output, le responsabilità, le metriche e gli obiettivi sono elementi puramente descrittivi e quindi per loro natura non vincolanti o esaustivi. Essi forniscono una base di conoscenze di alto livello da cui ogni azienda può trarre quelle che più le si adattano in termini di efficacia ed efficienza, in base alla strategia, agli obiettivi e alle politiche che si è data.

Utilizzatori dei componenti di COBIT

La direzione può usare il supporto di COBIT per valutare i processi IT utilizzando gli obiettivi aziendali e gli obiettivi IT dettagliati nell’appendice I, per chiarire gli obiettivi dei processi IT ed il modello di strutturazione del processo per valutare le performance attuali.

Chi definisce i processi e gli auditor possono identificare dei pratici requisiti di controllo dagli obiettivi di controllo e le responsabilità dalle attività e dalle relative tabelle RACI.

Tutti i potenziali utilizzatori possono beneficiare dei componenti di COBIT per un generico approccio alla gestione ed al governo dell’IT, unitamente ad altri standard specifici quali:

- ITIL per la gestione dei servizi (service delivery)
- CMM per lo sviluppo delle soluzioni (solution delivery)
- ISO/IEC 27002:2005 per la sicurezza delle informazioni (information security)
- PMBOK o PRINCE2 per la gestione dei progetti (project management)

Appendici

Le seguenti sezioni contenenti riferimenti aggiuntivi sono riportate alla fine del libro:

- I. Tabelle di collegamento fra gli Obiettivi Aziendali a quelli dell’IT (tre tabelle)
- II. Mappatura dei Processi IT rispetto alle Aree della Governance, al COSO, alle Risorse IT di COBIT e ai Criteri di Valutazione delle Informazioni di COBIT
- III. Il modello di strutturazione del Controllo Interno
- IV. Le principali fonti di riferimento di COBIT 4.1
- V. I riferimenti incrociati tra COBIT® 3rd Edition® e COBIT 4.1
- VI. Approccio definito per la ricerca e lo sviluppo
- VII. Glossario
- VIII. COBIT ed i prodotti della sua suite.

COBIT®

4.1

Traduzione italiana



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



Sistemi informativi: averne fiducia e trarne valore

Milano Chapter