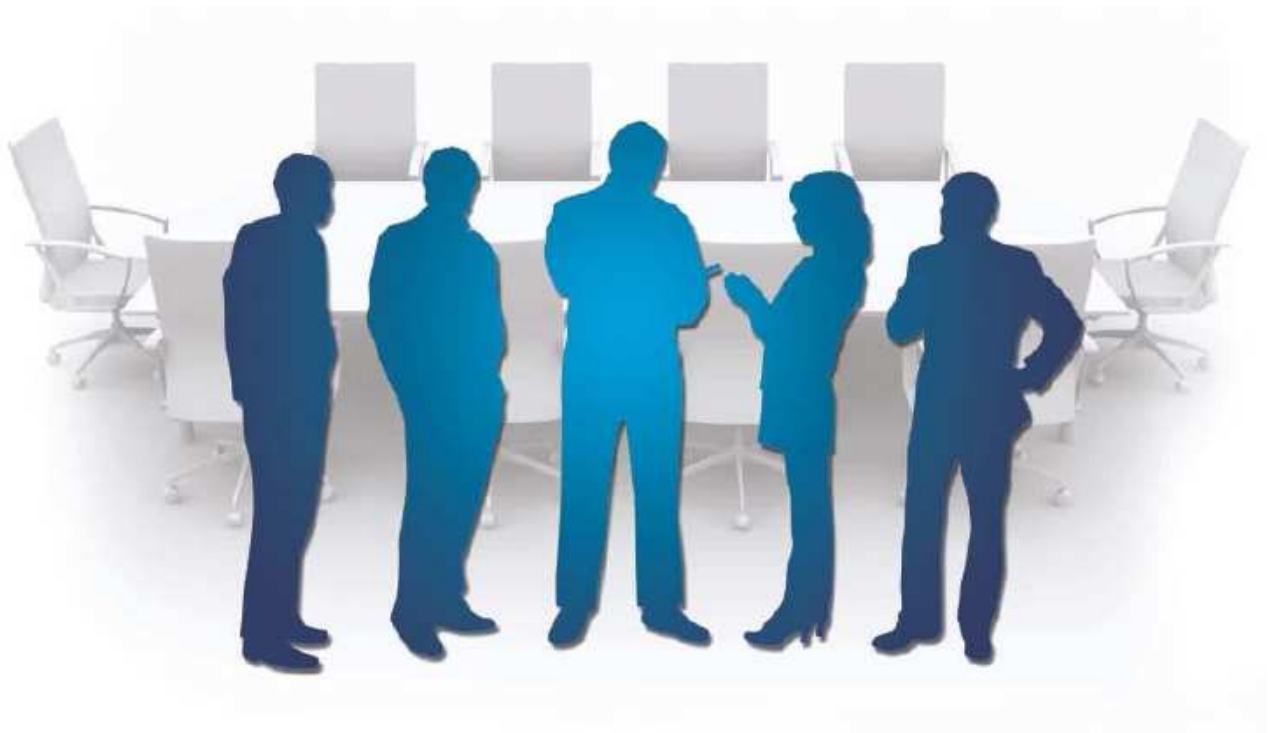


# ITGI facilita

l'adozione di ISO/IEC 38500:2008



## **Prefazione alla traduzione italiana**

La presente traduzione è stata realizzata da **Agatino Grillo**, CISA, CISSP, CISM.

Questo documento viene diffuso via web attraverso il sito <http://www.compliancenet.it/> in formato **pdf**, Microsoft **Word 97-2003** ed **Open Office 3.0** al fine di garantirne la massima diffusione.

Per contattare Agatino Grillo:

- [agatino.grillo@gmail.com](mailto:agatino.grillo@gmail.com)
- <http://www.agatinogrillo.it/>
- <http://www.linkedin.com/in/agatinogrillo>

La versione in lingua inglese (versione originale) di questo documento è liberamente scaricabile, in formato **pdf**, dal sito di ISACA a questo link:

<http://isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=47865>

## INDICE

<b>INDICE</b> .....	<b>I</b>
<b>INTRODUZIONE</b> .....	<b>1</b>
<b>L'APPROCCIO PROFESSIONALE DI ITGI</b> .....	<b>2</b>
<b>BENEFICI DELLO STANDARD ISO/IEC 38500</b> .....	<b>3</b>
<b>IN CHE MODO ITGI FACILITA L'ADOZIONE DELLO STANDARD</b> .....	<b>4</b>
I PRINCIPI DELLO STANDARD .....	4
<i>Principio 1 - Responsabilità</i> .....	4
<i>Principio 2 – Strategia</i> .....	5
<i>Principio 3 - Acquisizione</i> .....	6
<i>Principio 4 - Esecuzione</i> .....	7
<i>Principio 5 – Conformità</i> .....	8
<i>Principio 6 – Comportamento</i> .....	9
ADOZIONE DELLO STANDARD .....	12
IN CHE MODO ITGI FORNISCE UNA GUIDA PER LE “BUONE PRASSI” .....	13
<b>IN CHE MODO I PRODOTTI ITGI FACILITANO L'ADOZIONE DI ISO/IEC 38500</b> .....	<b>15</b>

## **IT Governance Institute®**

L'IT Governance Institute (ITGI™) (<http://www.itgi.org/>) è un ente di ricerca, indipendente e no-profit, che fornisce linee guida per la comunità di business internazionale sui temi legati alla *governance* degli asset IT. ITGI è stato creato dall'associazione no-profit **ISACA** (<http://www.isaca.org/>) nel 1998 per aiutare l'alta direzione ed i professionisti IT nella gestione dei rischi connessi all'erogazione dei servizi informatici garantendo l'allineamento degli stessi con gli obiettivi dell'azienda, l'allocazione propria delle risorse IT e la misurazione delle performance. ITGI ha anche sviluppato i *Control Objectives for Information and related Technology* (COBIT®) e Val IT™, ed offre risorse in formato elettronico, ricerche originali e casi di studio sia per assistere il top management ed il Consiglio di Amministrazione nelle attività di *IT Governance* sia per aiutare i professionisti IT ad erogare servizi informatici ad alto valore aggiunto.

## **Disclaimer**

ITGI ha ideato e realizzato questa pubblicazione, intitolata “*ITGI™ Enables ISO/IEC 38500:2008 Adoption*” (la “pubblicazione”), principalmente come risorsa di tipo “educativo”. ITGI e gli autori di questa pubblicazione non forniscono nessuna assicurazione che l'uso di queste linee guida e degli strumenti indicati in questa pubblicazione possano garantire di per sé la conformità alle norme né il successo nei risultati. La pubblicazione non deve essere considerata come comprendente ogni informazione, procedura, test che ragionevolmente può portare allo stesso risultato. Nella determinazione della proprietà di ogni specifico controllo, procedura o test, coloro che si occupano di test e controlli devono applicare il proprio giudizio sulle specifiche circostanze di controllo presenti nell'ambiente dell'*Information Technology* (IT) sotto verifica.

## **Diritti**

*Copyright © 2009 IT Governance Institute. All rights reserved.* Tutti i diritti riservati. Nessuna parte di questa pubblicazione può essere usata, copiata, riprodotta, modificata, distribuita, visualizzata, memorizzata in un sistema elettronico o trasmessa in qualsiasi forma e con qualsiasi mezzo (elettronico, meccanico, per mezzo di fotocopie, registrato in maniera elettronica o in altro modo) senza l'autorizzazione scritta preliminare dell'IT Governance Institute.

**La riproduzione di parte selezionate del documento per uso interno, non commerciale o accademico è permesso ma deve contenere l'attribuzione completa della fonte del materiale. Nessuna altro diritto, o permesso, è concesso rispetto a quest'opera.**

## **IT Governance Institute**

3701 Algonquin Road, Suite 1010  
Rolling Meadows, IL 60008 USA  
Phone: +1.847.660.5700  
Fax: +1.847.253.1443  
E-mail: [info@itgi.org](mailto:info@itgi.org)  
Web site: <http://www.itgi.org>

*ITGI™ Enables ISO/IEC 38500:2008 Adoption*  
Printed in the United States of America

## **Ringraziamenti**

L'IT Governance Institute desidera ringraziare:

### **Researcher**

Gary Hardy, CGEIT, IT Winners, South Africa

### **Expert Reviewers**

Gregory T. Grocholski, CISA, The Dow Chemical Company, USA

Tony Hayes, FCPA, Queensland Government, Australia

John W. Lainhart IV, CISA, CISM, CGEIT, IBM Business Consulting Services, USA

Howard Nicholson, CISA, CGEIT, City of Salisbury, Australia

Maxwell J. Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia

Robert E. Stroud, CA Inc., USA

John Thorp, CMC, I.S.P., The Thorp Network Inc., Canada

Wim Van Grembergen, Ph.D., University of Antwerp Management School and IT Alignment and Governance Research Institute, Belgium

Vatsaraman Venkatakrishnan, CISA, CISM, CGEIT, ACA, Emirates Airlines, UAE

### **ITGI Board of Trustees**

Lynn Lawton, CISA, FBCS, FCA, FIIA, KPMG LLP, UK, International President

George Ataya, CISA, CISM, CGEIT, CISSP, ICT Control SA, Belgium, Vice President

Yonosuke Harada, CISA, CISM, CAIS, InfoCom Research Inc., Japan, Vice President

Howard Nicholson, CISA, CGEIT, City of Salisbury, Australia, Vice President

Jose Angel Pena Ibarra, CGEIT, Consultoria en Comunicaciones e Info., SA & CV, Mexico, Vice President

Robert E. Stroud, CA Inc., USA, Vice President

Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Vice President

Frank Yam, CISA, CIA, CCP, CFE, CFSA, FFA, FHKCS, FHKIoD, Focus Strategic Group, Hong Kong, Vice President

Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President

Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President

### **IT Governance Committee**

Tony Hayes, FCPA, Queensland Government, Australia, Chair

Sushil Chatterji, Edutech Enterprises, Singapore

Kyung-Tae Hwang, CISA, Dongguk University, Korea

John W. Lainhart IV, CISA, CISM, CGEIT, IBM Business Consulting Services, USA

Hugh Penri-Williams, CISA, CISM, CCSA, CIA, Accenture Technology Services, France

Gustavo Adolfo Solis Montes, CISA, CISM, Grupo Cynthus, Mexico

Robert E. Stroud, CA Inc., USA

John Thorp, CMC, I.S.P., The Thorp Network Inc., Canada

Wim Van Grembergen, Ph.D., University of Antwerp Management School and IT Alignment and Governance Research Institute, Belgium

**ITGI Affiliates and Sponsors**

American Institute of Certified Public Accountants  
ASIS International  
The Center for Internet Security  
Commonwealth Association for Corporate Governance Inc.  
FIDA Inform  
Information Security Forum  
Information Systems Security Association  
Institut de la Gouvernance des Systemes d'Information  
Institute of Management Accountants Inc.  
ITGI Affiliates and Sponsors (cont.)  
ISACA  
ISACA chapters  
ITGI Japan  
Norwich University  
Socitm Performance Management Group  
Solvay Brussels School of Economics and Management  
University of Antwerp Management School  
Aldion Consulting Pte. Ltd.  
Analytix Holdings Pty. Ltd.  
B Wise B.V.  
CA Inc.  
Consult2Comply  
Hewlett-Packard  
IBM  
ITpreneurs Nederlands B.V.  
LogLogic Inc.  
Phoenix Business and Systems Process Inc.  
Project Rx Inc.  
Symantec Corp.  
TruArx Inc.  
Wolcott Group LLC  
World Pass IT Solutions

## INTRODUZIONE

**L'importanza sempre crescente delle informazioni e della tecnologia, in ogni aspetto del business e della vita pubblica, fa aumentare la necessità di ottenere maggior valore dagli investimenti IT e di gestire i rischi, sempre maggiori, correlati all'IT.**

**Una governance d'impresa efficace sull'IT produce una migliore performance e compliance nei confronti dei requisiti esterni.**

Nel 1998 ISACA<sup>1</sup> si è posta il problema di migliorare il modo nel quale le aziende governano l'*Information Technology* (IT) e, come risposta, ha deciso di creare l'*IT Governance Institute* (ITGI) un organismo di ricerca no-profit che ha la *mission* di facilitare e far progredire la ricerca e realizzare linee guida nell'ambito dell'*enterprise IT governance*. ITGI (<http://www.itgi.org/>) è stato fondato quindi per fornire riflessioni e linee guida per la valutazione, la gestione ed il monitoraggio dell'IT aziendale.

Oggi ITGI saluta con favore il rilascio da parte di ISO di un nuovo standard, ISO/IEC 38500:2008 *Corporate governance of information technology*, che segna il riconoscimento internazionale dell'importanza di questo tema e della necessità di arrivare ad una "formalizzazione" della sua adozione.

In un momento in cui è evidente intorno a noi l'importanza sempre crescente delle informazioni e della tecnologia in ogni aspetto del business e della vita pubblica, aumenta proporzionalmente la necessità di ottenere maggior valore dagli investimenti IT e di gestire i rischi, sempre maggiori, correlati all'IT. Anche l'aumento delle norme e della regolamentazione spinge verso una maggiore consapevolezza, in chi dirige l'azienda, dell'importanza di un ambiente IT ben controllato e della necessità di essere *compliant* rispetto alle norme legali, ai regolamenti di settore ed alle obbligazioni contrattuali. Una *governance* d'impresa efficace produce infatti una migliore *performance* e *compliance* nei confronti dei requisiti esterni.

L'ITGI ritiene che la definizione di standard internazionali possa facilitare lo sviluppo e l'adozione della *governance*, in particolare quando tali standard sono effettivamente applicabili in tutte le organizzazioni, dalla più piccola alla più grande, indipendentemente dagli obiettivi e dalla struttura organizzativa. Per una adozione efficace gli standard richiedono però il maggior supporto possibile; i prodotti e le pubblicazioni di ITGI sull'*IT Governance* possono fornire proprio tale supporto in modo personalizzabile per ogni tipo di azienda.

---

<sup>1</sup> ISACA® è stata fondata nel 1969 ed al momento ha oltre 86.000 iscritti in più di 160 diversi paesi. ISACA è leader riconosciuto in tutto il mondo nell'ambito dell'*IT governance*, dei controlli, della sicurezza e dell'*assurance*. Su questi temi ISACA sponsorizza conferenze internazionali, pubblica l'*ISACA Journal*® ed ha sviluppato standard di controllo internazionali sull'*information systems auditing* ed i controlli IT. L'associazione gestisce tre certificazioni professionali molto note: *Certified Information Systems Auditor*™ (CISA®), *Certified Information Security Manager*® (CISM®) e *Certified in the Governance of Enterprises IT*™ (CGEIT™).

## L'APPROCCIO PROFESSIONALE DI ITGI

**Le linee guida dell'ITGI, centrate sui framework COBIT e Val IT, aiutano i manager a meglio comprendere come dirigere e gestire l'IT.**

All'inizio degli anni 90 ISACA si è resa conto che gli auditor, che avevano le loro proprie checklist per valutare l'esistenza e l'efficacia dei controlli IT, usavano un linguaggio diverso da quello usato dai business manager e dai professionisti IT. Per colmare questo gap di comunicazione fu realizzato COBIT un framework sui controlli IT rivolto ai business manager, agli IT manager ed agli auditor basato su un insieme di processi IT, processi che fossero generali ma anche significativi sia per i professionisti IT sia per il management.

Facendo leva sulla base di iscritti di ISACA, base formata da professionisti di *IT governance*, controlli, sicurezza ed *assurance* e sulle esperienze pratiche di centinaia di esperti nel mondo, ITGI ha creato, a partire dai framework COBIT e Val IT™, nuove linee guida che forniscono un linguaggio ed un approccio comune per le aziende per comprendere e gestire in pratica i principi dell'*IT governance*.

Essendo una organizzazione no-profit, ITGI ha creato "buone prassi" generali che sono indipendenti da ogni tecnologia specifica, dai prodotti commerciali ed ha reso liberamente disponibili tali linee guida. Ciò aiuta il Consiglio di Amministrazione, la dirigenza, ed il management ad implementare strutture, processi e *tool* che solo loro d'ausilio per comprendere e gestire i requisiti più importanti relativi all'*Information Technology*, a monitorare e valutare e attività critiche per l'IT e a prendere le giuste decisioni.

Le aziende hanno bisogno di poter contare sull'affidabilità dei sistemi informative e delle informazioni da questi prodotte. Esse devono poter contare sul ritorno degli investimenti fatti sull'IT. Le linee guida dell'ITGI, centrate sui framework COBIT e Val IT, aiutano i manager ed i direttori delle aziende a meglio comprendere come dirigere e gestire l'uso dell'IT e degli standard sulle "buone prassi" che dovrebbero essere utilizzate dai fornitori di servizi IT. COBIT e Val IT forniscono gli strumenti per gestire e supervisionare tutte le attività relative all'IT.

Una descrizione di tutti i prodotti di *IT governance* realizzati da ITGI è fornita alla fine di questa pubblicazione.

## **BENEFICI DELLO STANDARD ISO/IEC 38500**

L'adozione in azienda della nuova norma ISO/IEC 38500 (lo standard) induce numerosi benefici quali:

- enfatizza l'importanza dell'*IT governance* per gestire i rischi impliciti quando si effettuano significativi investimenti nell'IT;
- incoraggia le aziende all'uso appropriato degli standard per rafforzare la propria *governance* dell'IT;
- fornisce un framework basato su sei principi per la direzione aziendale da usare nella valutazione, gestione e monitoraggio dell'IT aziendale; seguire tali principi è di aiuto alla direzione aziendale per bilanciare i rischi e sfruttare le opportunità che nascono dall'utilizzo dell'IT;
- è applicabile a tutte le aziende indipendentemente dalle loro dimensioni, dagli obiettivi di business, dalla struttura organizzativa;
- rende chiaro che l'uso corretto dell'*IT enterprise governance* è di ausilio alla direzione nell'assicurare la *compliance* con i requisiti normativi (regolamenti, leggi, standard, obblighi contrattuali) che hanno a che fare con l'uso dell'IT e migliora il contributo dell'IT alle performance dell'azienda;
- rende più chiaro, infine, che sistemi IT inadeguati possono esporre al rischio di non essere *compliant* con l'ampio *range* di norme in continua evoluzione ed in rapido aumento.

Per implementare in modo efficace tale norma possono essere utilizzate le pubblicazioni e le linee guida realizzate da ITGI.

## IN CHE MODO ITGI FACILITA L'ADOZIONE DELLO STANDARD

Quanto segue è una sintesi di come COBIT, Val IT e le relative linee facilitano l'adozione dei principi dello standard ISO/IEC 38500:2008. Per gli approfondimenti e per avere maggiori informazioni alla fine di questo documento è disponibile una lista delle pubblicazioni realizzate da ITGI con l'indicazione dei link sul web.

Il nuovo standard, ISO/IEC 38500:2008 - *Corporate governance of information technology*, si basa su sei principi chiave.

Di seguito sono indicate le implicazioni pratiche di ciascun principio insieme con le indicazioni su come le linee guida e le pubblicazioni di ITGI possono essere di ausilio.

### I PRINCIPI DELLO STANDARD<sup>2</sup>

**Per l'IT governance sono richieste appropriate strutture organizzative e di di governance con ruoli e responsabilità ben chiare. È necessario che vi sia un preciso mandato da parte dell'alta direzione, mandato che deve assegnare una chiara ownership ed accountability per le decisioni ed i compiti più importanti.**

#### Principio 1 - Responsabilità

**Cosa significa in pratica:** Il business (il cliente) e l'IT (il fornitore) devono collaborare mediante l'adozione di un modello di *partnership* che si basi su una comunicazione efficace, su una relazione di fiducia e su regole chiare in relazione alle responsabilità ed *accountability*.

Per le imprese più grandi è opportuno istituire un comitato formato dagli IT *executive*, comitato a cui spesso ci si riferisce con il termine di *IT strategy committee*; tale comitato deve agire a nome del Consiglio di Amministrazione ed essere guidato da un membro del Consiglio stesso. Il Comitato è un meccanismo molto efficace per valutare, indicare la direzione e monitorare l'uso dell'IT in azienda e per fungere da *advisor* sui temi critici legati all'IT.

Le piccole e medie imprese (PMI), che hanno una struttura di controllo più semplice ed una linea di comando più corta, hanno bisogno di un approccio più diretto quando supervisionano le attività IT.

In entrambi i casi, però, sono richieste appropriate strutture organizzative di *governance*, chiarezza nei ruoli e nelle responsabilità e che vi sia un preciso mandato da parte dell'alta direzione, mandato che deve tradursi in una chiara *ownership* ed *accountability* per le decisioni ed i compiti più importanti compreso tutto ciò che riguarda i rapporti con le terze parti chiave fornitrici di servizi IT.

#### **In che modo le linee guida ITGI facilitano le "buone pratiche":**

- *Il Board Briefing on IT Governance and Unlocking Value: An Executive Primer on the Critical Role of IT Governance*, 2° edizione fornisce linee guida sui ruoli e le responsabilità per l'*IT governance* nel business e per la

<sup>2</sup> Per le definizioni dei sei principi discussi in questa sezione si faccia riferimento allo standard ISO/IEC 38500-2008 che può essere acquistato dagli enti autorizzati quali ANSI, 25 West 43rd Street, New York, NY 10036, USA, +1.212.642.4900, <http://webstore.ansi.org> o altri rivenditori autorizzati.

- funzione IT, sia che quest'ultima sia *in-house* sia che sia in *outsourcing*, e descrive come instaurare un *IT executive (strategy) committee* efficace.
- I framework COBIT e Val IT comprendono i diagrammi RACI<sup>3</sup> che mostrano esempi di formalizzazione di ruoli e responsabilità per i membri del Consiglio di Amministrazione ed il management di tutti i processi e le attività chiave legate all'IT.
  - L'*IT Governance Implementation Guide: Using COBIT® and Val IT™*, 2° edizione spiega le responsabilità degli *stakeholder* e delle altre parti coinvolte quando si implementa o si migliora un accordo di *IT governance*.
  - I processi del dominio COBIT "*Monitor and Evaluate (ME)*" illustrano il ruolo dell'alta direzione nel monitoraggio e nella valutazione dell'*IT governance* e dell'*IT performance* attraverso un metodo generale che permette di stabilire fini, obiettivi e relative metriche. ME4 "*Monitor and evaluate IT governance*" si focalizza in modo specifico sulla supervisione delle attività di *IT governance*.

## Principio 2 - Strategia

**Cosa significa in pratica:** la pianificazione IT strategica è una attività complessa e critica che richiede uno stretto coordinamento sia all'interno dell'azienda tra le business unit, sia, nel caso di gruppi e multinazionali, tra le varie aziende. È vitale indicare le priorità delle azioni riportate nel piano indicando quelle che hanno più probabilità di raggiungere i benefici desiderati ed allocare di conseguenza le risorse necessarie. Gli obiettivi di alto livello devono essere tradotti in piani tattici effettivamente conseguibili in modo da evitare sorprese e minimizzare i rischi.

L'obiettivo è generare valore a supporto degli obiettivi strategici tenendo conto dei rischi che devono essere proporzionali alla "predisposizione al rischio" (*appetite*) del Consiglio di Amministrazione. È importante che il piano sia articolato in attività di dettaglio secondo una sequenza *top-down*; i piani devono essere abbastanza flessibili ed adattabili per adeguarsi facilmente ai cambiamenti del business, ad eventuali nuovi requisiti e alle opportunità create dall'IT.

Inoltre il piano deve prendere in considerazione le effettive capacità IT (*IT capabilities*) in modo trasparente. Deve essere incluso un *assessment* della capacità dell'infrastruttura IT attuale, prese in considerazione le risorse umane disponibili per supportare i requisiti di business futuri e valutati i possibili sviluppi tecnologici futuri che potrebbero portare a vantaggi competitivi e/o ottimizzare i costi. Le risorse IT includono le relazioni con i *vendor* di prodotti esterni ed i *service provider*, alcuni dei quali probabilmente giocano un ruolo chiave nel supporto del business.

La *governance* delle fonti strategiche è dunque un attività strategica molto significativa che richiede la supervisione e la gestione dell'alta direzione aziendale.

### **In che modo le linee guida ITGI facilitano le "buone pratiche":**

- Il *Board Briefing on IT Governance*, 2° edizione e *Unlocking Value: An Executive Primer on the Critical Role of IT Governance* sono due

<sup>3</sup> I diagrammi RACI evidenziano chi è Responsabile, Accountable, Consultato e Informato in relazione ad un certo *task*

L'obiettivo è produrre valore a supporto degli obiettivi strategici tenendo conto dei rischi che devono essere proporzionali alla "predisposizione al rischio" (*appetite*) del Consiglio di Amministrazione.

pubblicazioni che spiegano come l'*IT executive (strategy) committee* deve far sì che la pianificazione strategica IT sia allineata con la pianificazione strategica generale dell'azienda e come i dirigenti IT e quelli di business devono lavorare insieme per conseguire risultati di successo.

- Val IT fornisce linee guida specifiche sulla gestione degli investimenti IT (più in particolare nel dominio dell'*Investment Management [IM]*) e su come gli obiettivi strategici devono essere supportati da *business case* appropriati.
- Il dominio di COBIT "*Plan and Organise (PO)*" spiega i processi richiesti per una pianificazione efficace e per l'organizzazione delle risorse IT interne ed esterne, compresa la pianificazione strategica, la pianificazione della tecnologia e delle architetture infrastrutturali, la pianificazione organizzativa, la pianificazione degli investimenti, il *risk management*, la gestione della qualità e dei progetti. È spiegato anche l'allineamento del business e degli obiettivi IT, con esempi generali che mostrano il supporto degli obiettivi strategici per tutti i processi legati all'IT sulla base di ricerche condotte nelle imprese di tutto il mondo.
- *Identifying and Aligning Business Goals and IT Goals* presenta un approfondimento delle relazioni "a cascata" tra gli obiettivi di business, gli obiettivi IT ed i processi IT. La ricerca presenta una lista di 17 obiettivi generali di business e di 18 obiettivi generali IT, validati e con indicazione delle priorità secondo i diversi settori. Insieme con le informazioni di collegamento tra i due, la ricerca fornisce una buona base sulla quale costruire una relazione a cascata generale a partire dagli obiettivi di business fino agli obiettivi IT. Viene indicata una lista degli obiettivi di business ed IT più importanti tra i diversi settori e sono svolte ulteriori analisi per settore e per area geografica con l'identificazione delle deviazioni più rilevanti che aumentano la rilevanza pratica per le aziende che operano in settori specifici e che vogliono usare tali liste per facilitare l'identificazione di un buon *set* di obiettivi di business ed IT.
- *Understanding How Business Goals Drive IT Goals* è un *white paper* che sintetizza il materiale presenter nella ricerca *Identifying and Aligning Business Goals and IT Goals*.

**L'implementazione di un soluzione IT non è solo una problematica tecnologica ma piuttosto una combinazione di cambiamenti organizzativi, rivisitazione dei processi di business, formazione e capacità di "abilitare" il cambiamento.**

### **Principio 3 - Acquisizione**

**Cosa significa in pratica:** esistono molteplici soluzioni IT per supportare i processi di business e quindi deve essere adottata una cura particolare nella fase di "acquisizione" delle soluzioni, dei progetti o dei servizi "tecnologici". Infatti una scelta inappropriata per quanto riguarda l'architetture tecnologica, errori nella gestione delle tecnologie o l'assenza di risorse umane opportunamente skillate possono portare al fallimento delle iniziative e dei progetti informatici o all'incapacità di sostenere in modo appropriato il business e alla riduzione del valore generato. L'acquisizione di risorse IT adeguate deve essere considerata come parte integrante del progetto di cambiamento del business attraverso l'acquisizione di nuovo IT. Il nuovo IT infine deve essere integrato con i processi di business già esistenti e con le infrastrutture già operanti. L'implementazione delle nuove soluzioni IT non è solo una problematica tecnologica ma viceversa

implica una combinazione di cambiamenti organizzativi, la rivisitazione dei processi di business, la formazione e la capacità di “abilitare” il cambiamento. Quindi i progetti IT devono essere considerati come parte di un più ampio programma di cambiamento a livello di intera azienda, programma che include altri progetti che soddisfano il *range* completo delle attività richieste per garantire il raggiungimento degli obiettivi desiderati.

**In che modo le linee guida ITGI facilitano le “buone pratiche”:**

- Nel dominio IM, Val IT fornisce linee guida per il governo e la gestione dell'IT per essere in grado di “abilitare” gli investimenti di business attraverso il loro ciclo di vita completo (acquisizione, implementazione, procedure e dismissioni). Il dominio del *Portfolio Management* (PM) spiega come gestire i progetti per mezzo di un *portfolio* efficace ed il *program management* degli investimenti.
- Il dominio PO di COBIT fornisce linee guida per la pianificazione dell'acquisizione quali il planning degli investimenti, il *risk management*, il planning, il *project management* e la qualità.
- Il dominio “*Acquire and Implement* (AI)” di COBIT fornisce linee guida sui processi richiesti per acquisire ed implementare le soluzioni IT compresa la definizione dei requisiti, l'identificazione delle soluzioni possibili, la preparazione della documentazione, il *training* ed indica come rendere gli utilizzatori capaci di utilizzare le soluzioni e le procedure per mettere in produzione i nuovi sistemi. Inoltre sono fornite linee guida per fornire aiuto ad assicurare che le soluzioni siano testate e controllate in modo corretto dato che il cambiamento viene applicato sia al business operativo sia all'ambiente IT.
- Il dominio ME comprende linee guida su come l'alta direzione può monitorare e valutare il processo di acquisizione e sui controlli interni che garantiscono che le acquisizioni sono gestite ed eseguite in modo corretto.

**Due fattori critici di successo sono l'approvazione degli obiettivi da parte degli stakeholder e l'accettazione dell'*accountability* per il raggiungimento degli obiettivi da parte dell'alta direzione e dei manager.**

**Principio 4 - Esecuzione**

**Cosa significa in pratica:** la misurazione efficace delle *performance* dipende dalla gestione di due aspetti chiave: la chiara definizione degli obiettivi di performance e lo stabilire metriche efficaci per monitorare il raggiungimento degli obiettivi. Un processo di misurazione delle performance è richiesto anche per assicurare che le performance siano monitorate in modo coerente ed affidabile. Una *governance* efficace è raggiunta quando gli obiettivi sono definiti con un approccio *top down* ed allineati con gli obiettivi di business di alto livello ma solo se le metriche sono definite e condivise con un approccio *bottom up* ed allineate in modo che abilitino il raggiungimento degli obiettivi che devono essere monitorati per ciascun livello di *management*.

Due fattori critici di successo sono: l'approvazione degli obiettivi da parte degli *stakeholder* e l'accettazione dell'*accountability* per il raggiungimento degli obiettivi da parte dell'alta direzione e dei manager. L'IT è una tematica complessa e tecnica; tuttavia è importante garantire trasparenza attraverso la definizione e comunicazione di obiettivi, metriche e report di performance espressi in un

linguaggio utile e significativo per gli *stakeholder* così che le azioni opportune possano esser emesse in pratica.

**In che modo le linee guida ITGI facilitano le “buone pratiche”:**

- I framework COBIT e Val IT forniscono esempi generali di obiettivi e e metriche per l'intero *range* dei processi connessi all'IT e mostrano come questi si relazionano agli obiettivi di business, rendendo capaci le aziende di adattarli secondo le loro necessità specifiche.
- COBIT fornisce strumenti per la gestione e linee guida per la definizione degli obiettivi IT e per l'allineamento con gli obiettivi di business e descrive come monitorare le *performance* di tali obiettivi usando le metriche. La capacità (*capability*) può essere oggetto di *benchmarking* usando i modelli di maturità (*maturity model*) e gli obiettivi di controllo.

Due processi chiave COBIT forniscono linee guida specifiche:

- PO1 “*Define a strategic IT plan*” si focalizza sulla definizione degli obiettivi.
- *Deliver and Support* (DS) 1 “*Define a manage service level*” si focalizza sulla definizione dei servizi appropriati, degli obiettivi e della loro formalizzazione nei *service level agreement*.

Nel processo ME1 “*Monitoring and evaluating IT performance*” COBIT fornisce linee guida sulle responsabilità dell'alta direzione per questa attività.

COBIT fornisce linee guida sul monitoraggio dell'IT *governance* stessa nel processo ME4 “*Monitoring and evaluating IT governance*”.

- Val IT fornisce linee guida specifiche ed esempi per il monitoraggio delle *performance* di un investimento IT lungo il suo intero ciclo di vita a partire dal *business case* fino alla realizzazione pratica dei benefici.
- L'IT *Assurance Guide: Using COBIT* spiega come i professionisti che si occupano di *assurance* possono fornire una *assurance* indipendente all'alta direzione per quanto riguarda l'IT *performance*.

**Principio 5 – Conformità**

**Cosa significa in pratica:** Nel mercato odierno caratterizzato dalla globalizzazione e dall'innovazione tecnologica sempre più spinta, mercato che si è sviluppato anche grazie ad Internet e all'IT, le aziende devono essere conformi rispetto ad un numero sempre crescente di norme e requisiti.

A causa degli scandali aziendali e dei fallimenti in ambito finanziario degli ultimi anni c'è una sempre maggiore consapevolezza nei consigli di amministrazione della necessità di essere *compliant* rispetto a leggi e regolamentazioni sempre più severe. Gli *stakeholder* richiedono una maggiore *assurance* che le aziende siano *compliant* con le leggi e le regolamentazioni e conformi rispetto alle “buone pratiche” di *corporate governance* nei loro ambiti operativi.

Infine dato che l'IT ha permesso di estendere i processi di business anche tra aziende diverse c'è una crescente necessità di assicurare che i contratti, gli accordi e le *partnership* comprendano i requisiti relativi all'IT in aree critiche quali la *privacy*, la riservatezza dei dati, la proprietà intellettuale e la sicurezza. L'alta direzione ha bisogno dell'assicurazione che sia rispettata la *compliance* con i requisiti esterni e che essa sia gestita come parte integrante dei processi aziendali

**L'implementazione di ogni cambiamento basato sull'IT, inclusa l'IT *governance* stessa, richiede significativi cambiamenti culturali e di comportamento all'interno dell'azienda così come nei confronti dei clienti e dei business partner.**

e della pianificazione strategica piuttosto che come un semplice e costoso ripensamento *a posteriori*. La direzione ha la responsabilità di stabilire il giusto “*tone at the top*” e definire politiche e procedure che il management e lo staff devono seguire per garantire che gli obiettivi delle aziende siano effettivamente realizzati, i rischi siano minimizzati e la *compliance* sia garantita. Il *top management* deve attuare un effettivo bilanciamento tra le *performance* e la conformità assicurando che gli obiettivi di *performance* non causino una *compliance* a macchia di leopardo e, di conseguenza, che il processo di *compliance* sia appropriato e non limiti eccessivamente le attività di business.

**In che modo le linee guida ITGI facilitano le “buone pratiche”:**

- Gli obiettivi di controllo e le “*control practice*” di COBIT forniscono la base per definire un appropriato ambiente di controllo e valutare l’adeguatezza dei controlli IT in azienda. I modelli di maturità abilitano il management a valutare e fare *benchmark* delle *capability* dei processi IT.
- Il processo COBIT PO1 “*Define a strategic IT plan*” aiuta ad assicurare che esista un allineamento tra la pianificazione IT e gli obiettivi di business generali compresi i requisiti di *governance*.
- Il processo COBIT ME2 “*Monitor and evaluate IT controls*” permette all’alta direzione di valutare se i controlli sono adeguati per soddisfare i requisiti di *compliance*.
- Il processo COBIT ME3 “*Ensure compliance with external requirements*” aiuta ad assicurare che i requisiti “esterni” di *compliance* siano identificati, che la direzione indichi la direzione per la *compliance* e che anche l’*IT compliance* sia monitorata, valutata e oggetto di reporting in quanto parte del più ampio progetto di *compliance* ai requisiti normativi dell’impresa.
- L’*IT Assurance Guide: Using COBIT* spiega come gli auditor possono fornire una *assurance* indipendente sulla *compliance* e sul rispetto delle politiche interne che derivano dalle direttive interne o da requisiti esterni di tipo legale, regolatorio o contrattuale confermando che qualsiasi azione correttiva deve gestire i possibili gap con la *compliance* e che i responsabili dei processi devono agire in modo tempestivo.
- La conformità riguarda anche le decisioni sugli investimenti. Val IT, in modo specifico attraverso *Value Governance* (VG) 1 e 3, PM1 e 4, e *Investment Management* (IM) 4, assicura che gli investimenti relativi alla *compliance* bilancino il valore della conformità rispetto al rischio ed al costo della non-conformità.

**Principio 6 – Comportamento**

**Cosa significa in pratica:** L’implementazione di ogni cambiamento basato sull’IT, inclusa l’*IT governance* stessa, di solito richiede significativi cambiamenti culturali e di comportamento all’interno dell’azienda così come nei confronti dei clienti e dei *business partner*. Questo può creare timori e incomprensioni all’interno dello staff e dunque i cambiamenti hanno bisogno di essere gestiti con cura così che il personale reagisca in modo positivo ai nuovi impegni richiesti. La direzione deve comunicare in modo chiaro gli obiettivi e si deve percepire come elemento positivo il supporto ai cambiamenti proposti. Il *training* ed il rafforzamento degli *skill* del personale sono elementi chiave del cambiamento –

**Problematiche come la privacy e le frodi stanno aumentando le preoccupazioni delle persone; questi ed altri rischi analoghi devono essere gestiti per evitare la mancanza di fiducia nei sistemi IT.**

specialmente data la rapidità dei cambiamenti tecnologici. Le persone sono coinvolte dall'IT a tutti i livelli in azienda, come *stakeholder*, manager ed utilizzatori, o come specialisti che forniscono servizi di tipo IT e soluzioni al business. Oltre all'azienda, l'IT ha effetto sui clienti e sui *business partner* ed abilita sempre più le transazioni *self service* ed automatizzate tra le aziende dentro e fuori i confini dei singoli paesi. Se i processi di business portano nuovi benefici ed opportunità essi introducono anche nuovi rischi. Problematiche come la privacy e le frodi stanno aumentando le preoccupazioni degli individui rispetto a questi ed altri rischi e devono essere gestite per evitare che le persone perdano la fiducia nei sistemi IT che essi usano. I sistemi informativi possono anche avere un effetto potente sui modi di lavorare ad esempio automatizzando le procedure manuali.

**In che modo le linee guida ITGI facilitano le “buone pratiche”:**

Sette processi Val IT e COBIT forniscono linee guida sui requisiti relative ai comportamenti del personale:

- Val IT capitolo 6, "*Functional Accountabilities and Responsibilities*" enfatizza la necessità di comprendere i cambiamenti richiesti in relazione alla *governance* degli investimenti e ai cambiamenti connessi direttamente all'IT.
- Il processo COBIT PO4 "*Define the IT organisation and relationships*" spiega come l'organizzazione IT ed i relativi processi devono essere sviluppati e mantenuti in modo appropriato per soddisfare i requisiti dello staff a tutti i livelli.
- Il processo COBIT PO6 "*Communicate management aims and direction*" si focalizza su come assicurare che gli obiettivi siano chiaramente comunicati e che sia promossa una cultura del fare insieme alla giusta attitudine nei confronti dei rischi e dei controlli.
- Il processo COBIT PO7 "*Manage IT human resources*" spiega come la performance dei singoli individui deve essere allineata con gli obiettivi aziendali e come gli skill degli specialisti IT devono essere mantenuti nel tempo e come i ruoli e le responsabilità devono essere definiti.
- Il processo COBIT AI2 "*Acquire and maintain application software*" aiuta nella progettazione delle applicazioni in modo tale da soddisfare sia le procedure del personale sia l'uso dei requisiti.
- Il processo COBIT AI4 "*Enable operation and use helps*" assicura che gli utilizzatori siano capaci di usare i sistemi in modo efficace.
- Il processo COBIT DS7 "*Educate and train users*" spiega come possono essere definite le necessità formative degli utilizzatori e come le si può soddisfare assicurando così l'uso efficace dei sistemi IT.
- Il processo COBIT ME2 "*Monitor and evaluate internal controls*" aiuta l'alta direzione a monitorare i controlli interni e, in modo specifico, a monitorare le performance del personale per mezzo delle *review* dei supervisori.

ISACA gestisce inoltre tre certificazioni professionali per chi ricopre un ruolo chiave in relazione alla *IT governance*:

- *Certified in the Governance of Enterprise IT™* (CGEIT™)

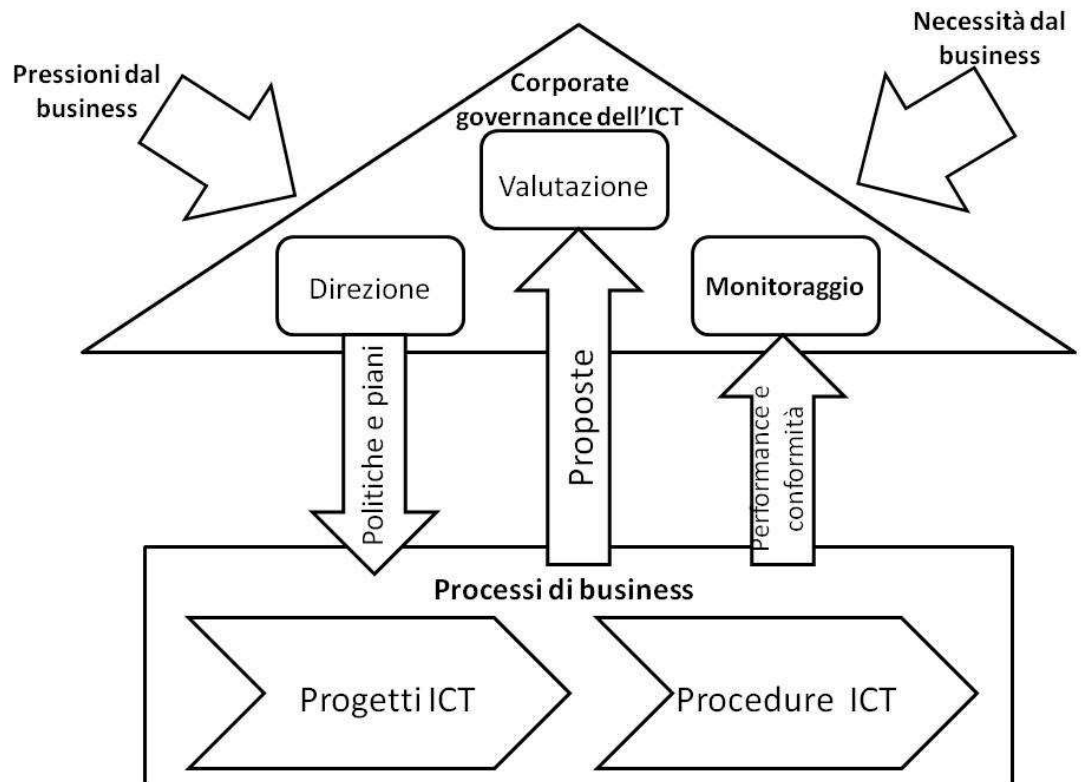
- *Certified Information Systems Auditor*<sup>TM</sup> (CISA®)
- *Certified Information Security Manager*® (CISM®)

Coloro che hanno conseguito tali certificazioni hanno elevate capacità per ricoprire ruoli nell'ambito della *IT governance*.

ADOZIONE DELLO STANDARD

Figura 1 – Modello per la IT Corporate Governance

Le “buone pratiche” in COBIT rappresentano un approccio comune al controllo IT – approccio implementato dai manager sia IT sia di business e basato sugli stessi principi degli auditor.



Fonte: © ISO. Questo materiale è riprodotto da ISO/IEC 38500:2008 con l'autorizzazione dell'*American National Standards Institute* (ANSI) per conto dell'*International Organisation for Standardisation* (ISO). Nessuna parte di questo materiale può essere copiato o riprodotto in qualsiasi forma, compresi sistemi informatici di memorizzazione e *retrieval* o analoghi mezzi né reso disponibile su Internet, su una rete pubblica, o per mezzo di satelliti od altro senza la preventiva autorizzazione scritta dell'ANSI e dei suoi rappresentanti autorizzati. Copie di questo standard possono essere acquistate da ANSI, 25 West 43rd Street, New York, NY 10036, USA, +1.212.642.4900, <http://webstore.ansi.org> o dai rivenditori autorizzati.

ISO/IEC 38500 raccomanda che la direzione governi l'IT per mezzo di tre *task* principali come mostrato nella **figura 1**:

- Valutazione
- Direzione
- Monitoraggio

**Cosa significa in pratica:**

L'implementazione di un approccio efficace di *IT governance* è reso più facile ed efficace quando:

- è allineato con gli standard e le prassi “accettate” di *corporate governance*
- è allineato con l'approccio aziendale alla *governance*
- copre tutti gli aspetti delle attività aziendali connessi all'IT
- è basato su principi ed obiettivi che possono essere compresi ed applicati da tutti gli *stakeholder*.

Riferimenti ai framework già disponibili, standard e “buone pratiche” e la loro adozione ed uso (personalizzati per riflettere la cultura, i requisiti e le capacità di ciascuna azienda) possono supportare l'azienda più efficacemente ed efficientemente nell'individuare e rendere operativo il proprio approccio di *IT governance*.

**IN CHE MODO ITGI FORNISCE UNA GUIDA PER LE “BUONE PRASSI”**

Il seguente materiale ITGI supporta i tre principali *task* raccomandati da ISO/IEC 38500.

**Valutazione:**

- Il *Board Briefing on IT Governance*, 2° edizione e *Unlocking Value: An Executive Primer on the Critical Role of IT Governance* descrive cosa deve fare il Consiglio di Amministrazione riguardo l'*IT governance*, cosa essa includa, quali questioni bisogna porsi, e come confrontare la propria azienda con le *best practice*.
- COBIT e Val IT forniscono una base per valutare l'adeguatezza dei controlli IT e delle “*management practices*” e facilitano il management nella valutazione e nel *benchmark* della *capability* dei processi IT.
- La fase “*Identify Needs and Envision Solution*” dell'*IT Governance Implementation Guide: Using COBIT® and Val IT*, 2° edizione spiega come focalizzare la valutazione dell'IT sulle necessità di business e sui processi IT critici ed anche come realizzare una *gap analysis* rispetto alle “buone pratiche”.
- *COBIT® Quickstart™*, 2° edizione fornisce linee guida sia per le piccole imprese sia per le grandi aziende che desiderano valutare i loro controlli e la *governance* dell'IT usando una *baseline* predefinita.
- *Enterprise Value: Governance of IT Investments, Getting Started With Value Management* aiuta ad identificare i *trigger* (indicatori) e a valutare le necessità di business necessarie per gestire meglio gli investimenti relativi all'IT.
- *Enterprise Value: Governance of IT Investments, The Business Case* aiuta a creare un *business case* per il miglioramento dell'*IT governance*.

- L'*IT Assurance Guide: Using COBIT®* facilita i professionisti che si occupano di *assurance* a fornire al management una valutazione indipendente e fornisce un metodo e test di esempio per condurre audit e *review*.

#### **Direzione:**

- Il *Board Briefing on IT Governance*, 2° edizione e *Unlocking Value: An Executive Primer on the Critical Role of IT Governance* descrivono cosa devono fare i consigli di amministrazione riguardo la *IT governance* e spiegano come essa debba essere realizzata in pratica.
- COBIT e Val IT forniscono linee guida per l'implementazione nella forma di obiettivi di controllo e "*key management practice*" che devono essere prese in considerazione (sulla base dei principi generalmente accettati, degli standard internazionali e delle *best practice*) per rendere possibile una buona *IT governance*.
- Le fasi "*Plan Solution*" e "*Implement Solution*" dell'*IT Governance Implementation Guide: Using COBIT® and Val IT*, 2° edizione spiegano come dare priorità, pianificare e progettare le azioni di miglioramento dell'*IT governance*.
- *COBIT® Quickstart™*, 2° edizione fornisce una *baseline* di controlli sia per le piccole imprese sia per le grandi aziende che desiderano muovere i primi passi verso una buona *IT governance*.
- Per le aziende dove la sicurezza è una area chiave che richiede miglioramenti, *COBIT® Security Baseline™*, 2° edizione fornisce una linea guida di facile utilizzo per imprimere la giusta direzione all'implementazione dei controlli chiave di sicurezza *IT security* in allineamento con gli standard di sicurezza ISO/IEC 27002.

#### **Monitoraggio:**

- Il *Board Briefing on IT Governance*, 2° edizione e *Unlocking Value: An Executive Primer on the Critical Role of IT Governance* descrivono cosa i consigli di amministrazione devono fare per monitorare in modo efficace l'*IT enterprise governance*.
- COBIT fornisce le linee guida sotto forma di processi IT raccomandati per il monitoraggio e la valutazione dell'*IT* (dominio ME) occupandosi di misurazione delle *performance*, efficacia del controllo interno, *compliance* con i requisiti esterni e raggiungimento di una *governance* globale ed efficace.
- La fase "*Operationalise Solution*" dell'*IT Governance Implementation Guide: Using COBIT® and Val IT*, 2° edizione spiega come integrare l'*IT governance* nelle normali operazioni di business e come monitorare e misurare il successo dei miglioramenti di *IT governance*.
- L'*IT Assurance Guide: Using COBIT®* facilita i professionisti che si occupano di *assurance* che devono fornire al management opinion indipendenti sulla *performance* e sulla conformità e fornisce un metodo e test di esempio per condurre audit e *review*.

COBIT è stato sviluppato come framework liberamente distribuibile ed oggi viene sempre più utilizzato in tutto il mondo; costituisce lo standard *de facto* per il modello di controllo.

Val IT è stato introdotto per estendere le linee guida di ITGI nell'area degli investimenti "abilitati dall'IT".

La combinazione di Val IT e COBIT fornisce una base completa e coerente per stabilire una efficace *governance* delle attività IT dell'azienda.

## IN CHE MODO I PRODOTTI ITGI FACILITANO L'ADOZIONE DI ISO/IEC 38500

La **figura 2** mostra come le pubblicazioni ed i prodotti ITGI facilitano l'adozione di ISO/IEC 38500.

**Figura 2 – Relazione tra i prodotti ITGI e ISO/IEC 38500**

Prodotti ITGI	Aree ISO/IEC 38500								
	Responsabilità	Strategia	Acquisizione	Performance	Conformità	Comportamento	Valutazione	Direzione	Monitoraggio
Board Briefing on IT Governance, 2ª edizione	√	√				√	√	√	√
Unlocking Value: An Executive Primer on the Critical Role of IT Governance	√	√				√	√	√	√
COBIT®	√	√	√	√	√	√	√	√	√
Val IT™	√	√	√	√	√	√	√	√	√
IT Governance Implementation Guide: Using COBIT® and Val IT, 2ª edizione							√	√	√
IT Assurance Guide: Using COBIT®				√	√		√		√
COBIT® Quickstart™, 2ª edizione							√	√	
Enterprise Value: Governance of IT Investments, Getting Started With Value Management							√		
COBIT® Security Baseline™, 2ª edizione	√						√	√	
Enterprise Value: Governance of IT Investments, The Business Case			√	√			√	√	√

Le "buone pratiche" nell'area COBIT forniscono un approccio comune per il controllo dell'IT implementato dai manager del business e dall'IT ed utilizzano le stesse basi ed approccio degli auditor. Nel corso degli anni COBIT è stato sviluppato come framework liberamente distribuibile ed oggi viene sempre più utilizzato in tutto il mondo e costituisce lo standard *de facto* per il modello di controllo dell'IT e per dimostrare una effettiva *IT governance*.

Di recente è stato anche introdotto Val IT che estende le linee guida di ITGI nell'area degli investimenti "abilitati dall'IT" (*IT enabled investment*). La

combinazione di Val IT e COBIT fornisce una base completa e coerente per stabilire una efficace *governance* rispetto alle attività IT dell'azienda.

Il framework COBIT, giunto alla versione 4.1, è formato da:

- framework – spiega in che modo COBIT gestisce l'*IT governance*, gli obiettivi di controllo e le “buone pratiche” per mezzo dei domini e dei processi IT e come questi sono collegati ai requisiti di business;
- descrizione dei processi – comprende 34 processi IT che coprono le aree di responsabilità IT dall'inizio alla fine;
- obiettivi di controllo – forniscono “*best practice*” generali sugli obiettivi di management per i processi IT;
- *management guideline* – forniscono strumenti per aiutare nell'assegnazione delle responsabilità e nella misurazione delle performance;
- modelli di maturità – forniscono profili dei processi IT che descrivono il posizionamento attuale e futuro dal punto di vista della maturità del processo.

Da quando è stato rilasciato i contenuti di COBIT sono stati continuamente sviluppati ed aggiornati ed il numero dei documenti correlati ha sempre continuato a crescere.

Di seguito sono riportate le pubblicazioni derivate da COBIT:

- *Unlocking Value: An Executive Primer on the Critical Role of IT Governance* – fornisce al top management un inquadramento generale sul perché l'*IT governance* sia importante e su come essa può creare valore per l'azienda;
- *Board Briefing on IT Governance*, seconda edizione – aiuta l'alta direzione a meglio comprendere i concetti dell'*IT governance*, quali siano i concetti fondamentali ed in che modo gestire le relative problematiche;
- COBIT Online® - permette di utilizzare una versione personalizzata di COBIT adattata alle caratteristiche della propria azienda e di memorizzare e modificare le personalizzazioni come meglio desiderato. Fornisce survey online e real-time, *frequently asked question*, *benchmarking* e strumenti per facilitare la discussione e condividere le esperienze, i dubbi e le soluzioni;
- *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance*, seconda edizione – fornisce linee guida sui rischi da evitare e sul valore che si può ottenere grazie all'implementazione degli obiettivi di controllo nonché le istruzioni su come implementare in pratica tali obiettivi;
- *IT Assurance Guide: Using COBIT®* - fornisce le linee guida su come COBIT può essere usato come supporto ad una gran varietà di attività di *assurance* ed offre piani di test di dettaglio per gli obiettivi di controllo ed i processi IT COBIT; è anche utile per sviluppare *self-assessment* in relazione agli obiettivi di controllo di COBIT 4.1;

- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting*, seconda edizione - fornisce le linee guida su come assicurare la *compliance* dell'ambiente IT sulla base degli obiettivi di controllo COBIT; **questa pubblicazione è disponibile anche in lingua italiana**<sup>4</sup>;
- *IT Control Objectives for Basel II – The Importance of Governance and Risk Management for Compliance* - fornisce le linee guida per le banche per i rischi operativi relativi all'IT
- *IT Governance Implementation Guide: Using COBIT® and Val IT*, seconda edizione – fornisce una “road map” generale per l'implementazione dell'IT governance usando le risorse COBIT e Val IT ed i relativi tool kit di supporto;
- *COBIT® Quickstart™*, seconda edizione – fornisce una *baseline* di controllo per le piccole imprese e un elenco di “primi passi” per le aziende più grandi;
- *COBIT® Security Baseline™*, seconda edizione – si focalizza sui passi necessari per implementare la sicurezza delle informazioni in azienda;
- *COBIT Mappings* – disponibili in <http://www.isaca.org/downloads>:
  - *Aligning COBIT® 4.1, ITIL v3 and ISO/IEC 27002 for Business Benefit*
  - *COBIT® Mapping: Overview of International IT Guidance*, seconda edizione
  - *COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of ISO/IEC 17799:2000 With COBIT®*, seconda edizione
  - *COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of ITIL With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of NIST SP800-53 With COBIT® 4.1*
  - *COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of SEI's CMM for Software With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0*
- *Information Security Governance: Guidance for Boards of Directors and Executive Management*, seconda edizione – presenta il tema dell'*information security* dal punto di vista del *management* e di chi si occupa di *business* e fornisce strumenti e suggerimenti su come gestire i problemi aziendali di sicurezza.

Val IT è l'insieme delle pubblicazioni relative al *Val IT framework*.

Al momento le pubblicazioni Val IT sono:

---

<sup>4</sup> <http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=45766> (pdf, 904 K, 120 pp)

- *Enterprise Value: Governance of IT Investments, Getting Started With Value Management* – questa pubblicazione fornisce una guida “facile da seguire” per iniziare un progetto “Value IT” e si rivolge all’alta direzione e agli *IT executive*;
- *Enterprise Value: Governance of IT Investments - The Val IT Framework 2.0*, spiega come un’azienda può ottenere “valore” a partire dagli investimenti “basati sull’IT” e si basa a sua volta sul COBIT framework. **In italiano è disponibile “Val IT 2.0 - FAQ in italiano”<sup>5</sup>**  
Val IT 2.0 si divide in:
  - *Three processes - Value Governance, Portfolio Management and Investment Management*,
  - *IT key management practices* – le “prassi” di management più importanti per indirizzare in maniera efficace le attività volte al raggiungimento del risultato desiderato; tali prassi supportano i processi Val IT e giocano pressappoco lo stesso ruolo degli obiettivi di controllo di COBIT;
- *Enterprise Value: Governance of IT Investments - The Business Case*, si focalizza su uno degli elementi chiave del processo di gestione degli investimenti.

Per una panoramica più completa ed aggiornata su COBIT, Val IT e dei relativi prodotti, *case study*, training, newsletter e tutte le altre informazioni relative ai framework, si può consultare <http://www.isaca.org/cobit> e <http://www.isaca.org/valit>.

---

<sup>5</sup> Val IT 2.0 - FAQ in italiano <http://www.agatinogrillo.it/content/val-it-20-faq-italiano>