

# Val IT & Case Study COBIT.

Sessione di studio AIEA

Padova, 29 ottobre 2009

Leonardo Nobile  
Director – Deloitte ERS Enterprise Risk Services  
[lnobile@deloitte.it](mailto:lnobile@deloitte.it)



# Agenda

- Le esigenze espresse dalle aziende
- Il framework Val IT
- Un esempio di applicazione di COBIT Quickstart per aziende di medie dimensioni

Le esigenze espresse dalle  
aziende



# Le esigenze

- Le aziende di qualunque settore produttivo continuano ad effettuare :
  - investimenti specifici e limitati all'ambito Information Technology
  - investimenti nei quali la componente IT è un fattore abilitante al cambiamento del Business.
- In entrambe i casi, tali investimenti si caratterizzano da un sempre crescente livello di complessità e rischiosità.
- La generazione del valore da parte di questi investimenti dipende dall'applicazione di un efficace framework di governance, che spazi dalle fasi di ideazione a quella di realizzazione e messa in produzione.
- Obiettivo di questo framework è aiutare l'organizzazione ad ottenere un ritorno da un investimento correlato all'IT ad un costo accettabile con un livello di rischio conosciuto e accettato.

# Le esigenze

- Tra le principali criticità percepite come “critiche” dai Financial Officer, vi sono:
  - Prioritizing Technology Investments
  - Identify the appropriate level of technology spending
  - Evaluating or measuring the return on technology investments

# Le esigenze

- Le principali esigenze dei C-Level Executives possono essere quindi così riassunte:
  - La creazione del valore derivante dagli investimenti di business correlati all'IT, la sua misurazione e la relativa gestione e ottimizzazione
  - La definizione di linee guida generalmente accettate relative al processo decisionale e alla realizzazione dei benefici connessi ad investimenti di business connessi all'IT.

# Il Framework Val IT



# Il framework Val IT

- Il framework **Val IT** è una metodologia per la valutazione dei **processi di governo** degli investimenti IT
- Vali It è applicabile a tutte le imprese e tengono in considerazione sia gli aspetti di **valutazione e controllo di un investimento IT** sia i principi finanziari per la conduzione dell'ambiente tecnologico aziendale.
- L'approccio Val It è applicabile anche alle **piccole e medie imprese**, adattandolo alla specifica realtà.
  - In questo caso l'approccio all'analisi degli investimenti richiede la selezione di un set minimale di attività che tenga conto almeno della verifica dell'allineamento con il business e l'analisi costi benefici.

# Val IT

- I principi alla base della metodologia Val IT sono i seguenti:
  - Gli investimenti connessi all'IT sono gestiti come un **portafoglio di investimenti**
  - Gli investimenti connessi all'IT includono tutte le attività richieste per **perseguire il valore per il business**
  - Gli investimenti connessi all'IT sono gestiti per tutto il loro **ciclo di vita economico**
  - Ci sono **differenti categorie** di investimenti che dovranno essere valutate e gestite in maniera diversa
  - Sono definite **metriche** chiave
  - Sono coinvolti tutti gli **attori** a cui sono assegnati obiettivi misurabili
  - Il processo è continuamente **monitorato, valutato e migliorato**

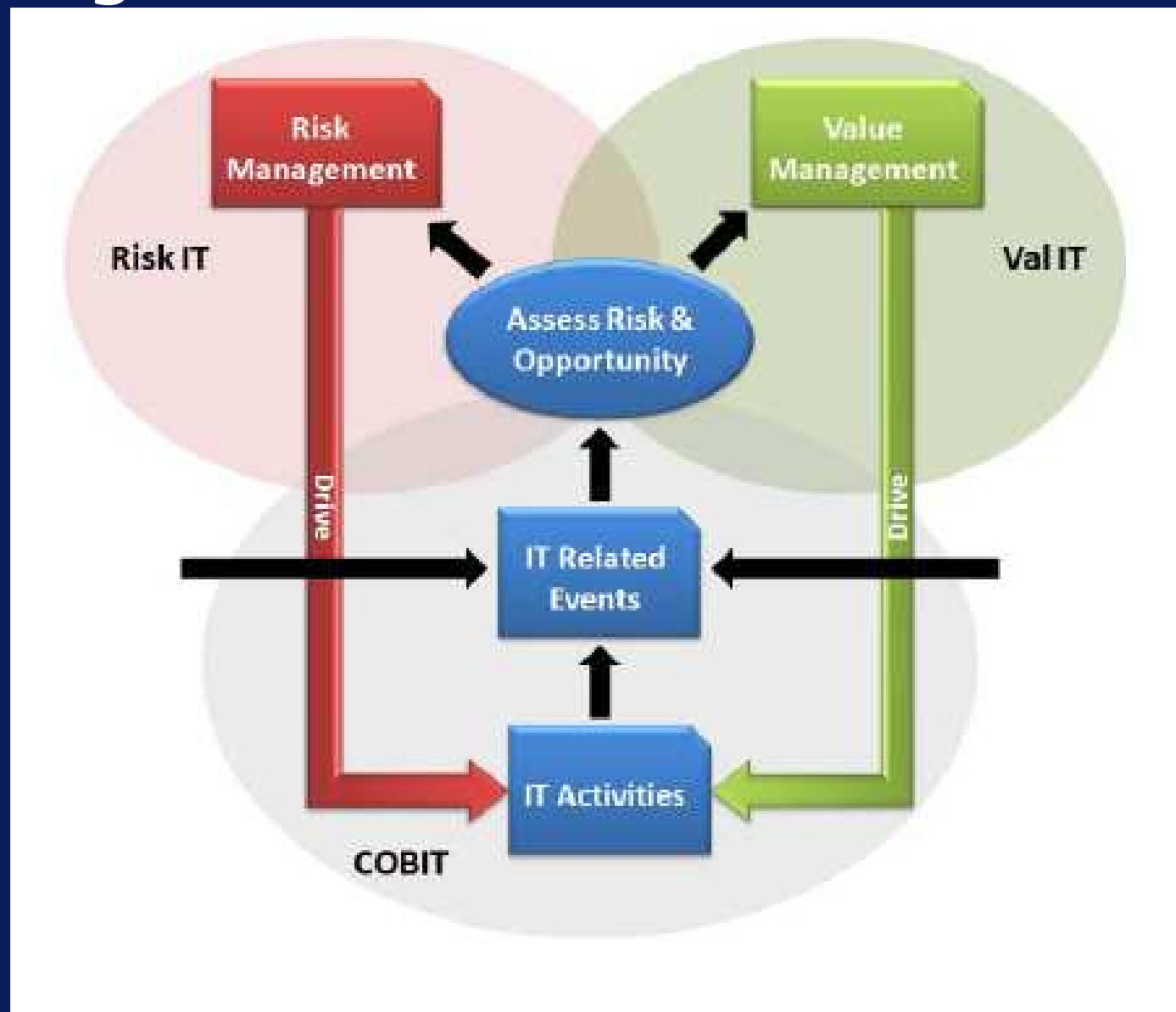
# VAL IT

- I principi della metodologia *Val IT* sono applicati ai seguenti processi:
  - *Value Governance (VG)*
    - *Framework di governo, monitoraggio e controllo*
    - *Linee strategiche per gli investimenti*
    - *Caratteristiche del portafoglio di investimenti*
  - *Portfolio Management (PM)*
    - *Soglie di investimento*
    - *Criteri di valutazione, prioritizzazione e selezione/rifiuto di nuovi investimenti*
    - *Gestione del portafoglio globale*
    - *Monitoraggio e reporting sulle performance del portafoglio*
  - *Investment Management (IM)*
    - *Identificazione dei business requirement*
    - *Sviluppo e analisi di alternative*
    - *Definizione e documentazione del progetto mediante **Business Case**, inclusi i benefici arrecati*
    - *Chiare "accountability" e "ownership" del progetto*
    - ***Gestione del programma/progetto***
    - *Monitoraggio e reporting delle performance e dei **benefici***

# Val IT

- L'applicazione dell'approccio, proposto dall'IT Governance Institute, genera i seguenti benefici:
  - Migliore comprensione e trasparenza dei costi, rischi e benefici
  - Migliore probabilità di selezionare gli investimenti con potenziale di elevato ritorno
  - Migliore probabilità di successo dell'investimento
  - Riduzione dei costi
  - Riduzione del rischio di fallimento dell'investimento

# Val IT e gli altri



# Esempio di applicazione di COBIT Quickstart



# COBIT Quickstart

**Domanda:** considerata la vastità del COBIT, posso adottare un approccio semplificato o graduale?

**ITGI – ISACA rispondono a tale istanza con COBIT Quickstart® utile per:**

- soddisfare le esigenze di organizzazioni medio / piccole
- accelerare l'introduzione dei concetti chiave del COBIT, attraverso un percorso adattato alle esigenze e razionalmente semplificato.



# COBIT Quickstart

Lo scenario in cui si applica **COBIT Quickstart** ® è caratterizzato da:

- Infrastruttura IT non complessa
- Ridotto rischio di disallineamento Business vs. IT
- Outsourcing delle funzioni IT più rilevanti
- L'organizzazione prevalentemente commerciale e poco propensa alla costruzione in house
- Scarse competenze IT
- Tolleranza al rischio relativamente alta
- Particolare attenzione ai costi
- Strutture gerarchiche semplificate (catene di comando corte)

# COBIT Quickstart – esempio di applicazione

## Scenario:

- Azienda di servizi
- Area IT costituita da circa 20 risorse
- Obiettivo dell'intervento: verificare il livello di adeguatezza del sistema di controllo IT operante su uno specifico ambito
- Ambito di intervento:
  - tecnologia, cioè le porzioni dell'infrastruttura informatica interessate dal Sistema Applicativo
  - tipologie di flussi di dati gestiti dall'applicativo
  - processi di gestione dei sistemi operativi e dei database
  - procedure di amministrazione della sicurezza

# COBIT Quickstart – esempio di applicazione

## Attività progettuali svolte:

- Individuazione del perimetro di intervento dei controlli IT pertinenti il Sistema Applicativo
- Analisi del contesto operativo in cui è collocato il Sistema Applicativo
- Tracciamento dei flussi transazionali e informativi che attraversano il Sistema, l'identificazione delle interfacce applicative con altri sistemi aziendali.
- Rilevazione del disegno e successivo test dei controlli IT pertinenti il Sistema Applicativo.
  - Tale attività ha avuto lo scopo di verificare l'**esistenza** e valutare l'**operatività** dei controlli IT attraverso lo svolgimento di **interviste** al personale chiave dei Sistemi Informativi della Società coinvolti nell'esercizio dei relativi controlli, l'**acquisizione di documentazione**, l'esecuzione di attività di **gap analysis** rispetto al target di controllo definito, l'esecuzione di **test sui controlli** in modalità **walkthrough**.

# COBIT Quickstart – esempio di applicazione

Esempio di valutazione dei controlli:

Processo CobiT 4.1	Obiettivo di Controllo CobiT QS, 2nd Ed.	Attività di Controllo
AI7 - Installare e convalidare le soluzioni e le modifiche  Tutti i nuovi sistemi applicativi sono rilasciati in produzione solamente in seguito allo svolgimento di adeguate procedure di testing o conversione dati.	Testare i requisiti funzionali e operativi delle modifiche e dei nuovi sviluppi applicativi in un ambiente di test affidabile e rappresentativo dell'ambiente di produzione.  Eseguire test di integrazione nei casi in cui le modifiche e i nuovi sviluppi applicativi debbano essere integrati nell'ambiente esistente.	I test sono eseguiti utilizzando un insieme completo di dati di test che sia rappresentativo dei dati di produzione.  Tutte le attività di sviluppo, modifica e manutenzione di sistemi applicativi, di database, del software di sistema e di rete devono prevedere la definizione e la documentazione dei casi di test e dei risultati attesi, approvati dai business owner e dal management dello sviluppo applicativo.

# COBIT Quickstart – esempio di applicazione

## Esempio di valutazione dei controlli:

Test eseguito	Esito
<p>Non sono formalmente definite le modalità di pianificazione, di gestione e di documentazione delle procedure di testing adottate nel processo di sviluppo.</p> <p>La gestione del processo di testing applicativo segue una prassi consolidata secondo cui, al termine del processo di sviluppo applicativo, l'Area Applicazioni Credito predispone insieme all'Area Produzione – Operation l'ambiente di test, contenente la copia dei dati di produzione su cui convalidare le modifiche effettuate. La verifica della corrispondenza fra i due ambienti di test e produzione è effettuata attraverso script preconfigurati.</p>	L'attività di controllo – seppur svolta per prassi – opera efficacemente.
<p>La gestione del processo di testing applicativo segue una prassi consolidata che non definisce formalmente le modalità di pianificazione, di gestione e di documentazione delle procedure di testing adottate nel processo di sviluppo. La scheda di “<i>Richiesta Passaggio in Produzione</i>”, compilata dall'Area Applicazioni Credito e contenente i passi da seguire per eseguire correttamente la messa in produzione della modifica applicativa collaudata in precedenza, offre la possibilità di allegare un “<i>Verbale di collaudo</i>”, ma questo non sempre viene prodotto.</p>	L'attività di controllo è inefficace.

# Deloitte.

Il nome Deloitte si riferisce a una o più di una delle seguenti entità: Deloitte Touche Tohmatsu (una Verein svizzera), le sue member firm e le relative entità controllate e/o licenziatricie. Ciascuna member firm e ciascuna entità controllata e/o licenziataria è una entità giuridica separata e indipendente che opera sotto i nomi "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," o altri nomi derivati. I servizi sono forniti dalle member firm, dalle rispettive entità controllate o da entità licenziatricie e non dalla Verein Deloitte Touche Tohmatsu. Né Deloitte Touche Tohmatsu, in relazione alla sua natura di Verein (associazione) di diritto svizzero, né ciascuna delle member firm e/o delle entità controllate e/o licenziatricie può essere ritenuta in alcun modo responsabile per atti od omissioni posti in essere da altre entità.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firm, and their respective subsidiaries and affiliates. As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte", "Deloitte & Touche", "Deloitte Touche Tohmatsu", or other related names. Services are provided by the member firms or their subsidiaries or affiliates and not by the Deloitte Touche Tohmatsu Verein.

Member of  
**Deloitte Touche Tohmatsu**