

# Università di Venezia

## Corso di Laurea in Informatica

“Laboratorio di Informatica Applicata – Introduzione all’IT Governance”

Lezione 5

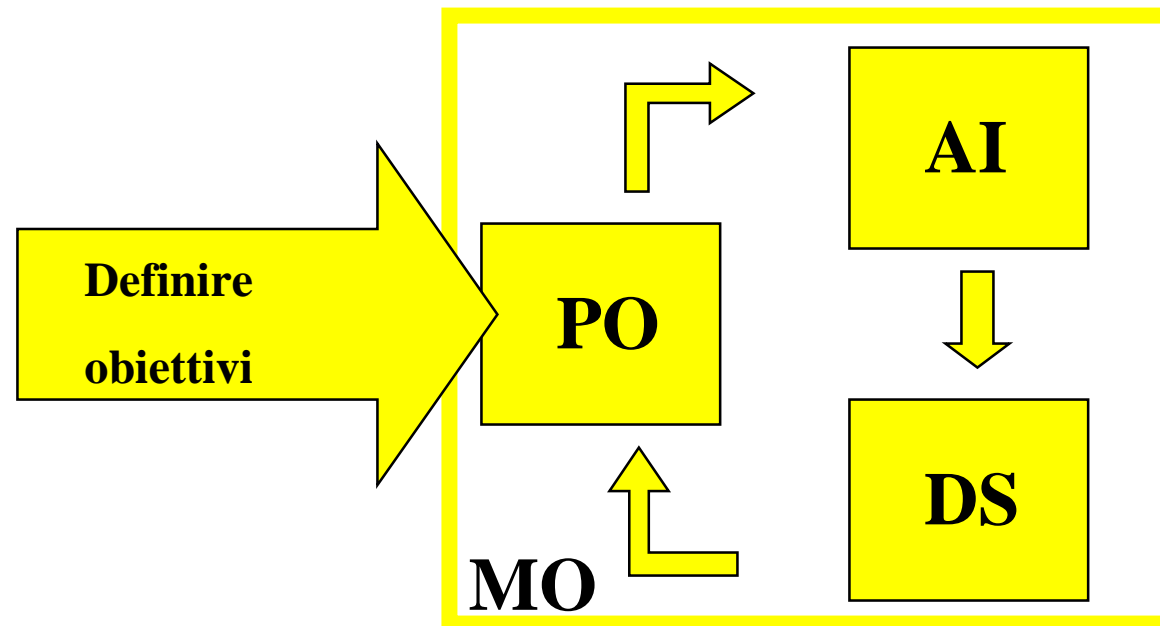


Marco Fusaro – KPMG S.p.A.

# CobiT

## CobiT:

- strumento per la comprensione di una organizzazione IT
- linee guida per il management (“best practice”)

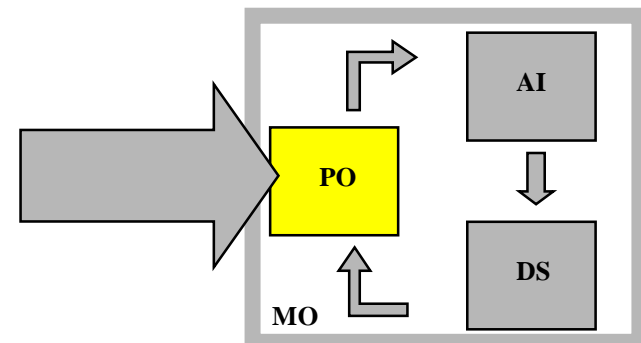


# Processi

## Processi del dominio PO (Planning & Organization)

Sono processi i cui obiettivi sono sintetizzabili nei seguenti punti:

- Definizione degli indirizzi strategici dell'IT
- Definizione dell'assetto organizzativo dell'IT
- Comunicazione della strategia alla struttura IT
- ...



# Processi

---

## Processi del dominio PO (Planning & Organization):

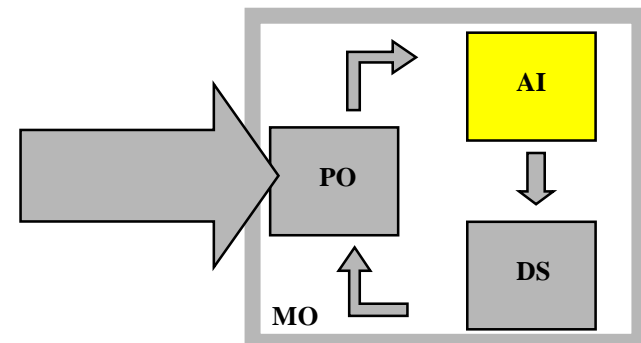
- **PO1 - Definizione del piano strategico per l'IT**
- **PO2 - Definizione dell'architettura informativa**
- **PO3 - Definizione dell'indirizzo tecnologico**
- **PO4 - Definizione dell'organizzazione IT e delle sue relazioni**
- **PO5 - Gestione degli investimenti IT**
- **PO6 - Comunicazione degli indirizzi e degli obiettivi del management**
- **PO7 - Gestione delle risorse umane**
- **PO8 - Conformità a leggi e norme**
- **PO9 - Valutazione dei rischi**
- **PO10 - Gestione dei progetti**
- **PO11 - Gestione della qualità**

# Processi

## Processi del dominio AI (Acquisition & Implementation)

Sono processi i cui obiettivi sono sintetizzabili nei seguenti punti:

- Identificazione delle soluzioni IT da sviluppare o acquistare per il soddisfacimento delle necessità aziendali
- Gestione del cambiamento dei sistemi



# Processi

---

## Processi del dominio AI (Acquisition & Implementation):

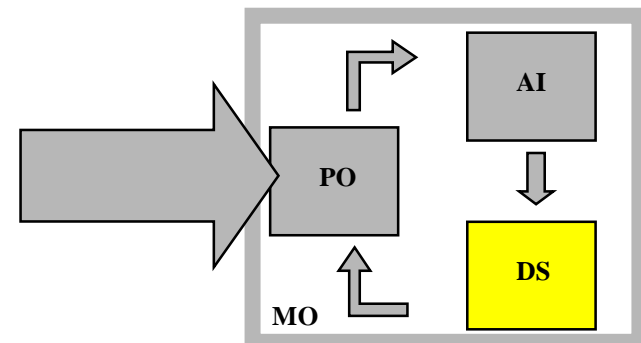
- **AI1 - Identificazione delle soluzioni**
- **AI2 - Acquisizione e manutenzione del software applicativo**
- **AI3 - Acquisizione e manutenzione dell'architettura tecnologica**
- **AI4 - Sviluppo e manutenzione delle procedure IT**
- **AI5 - Installazione e validazione dei sistemi**
- **AI6 - Gestione del cambiamento**

# Processi

## Processi del dominio DS (Delivery & Support):

Sono processi i cui obiettivi sono sintetizzabili nei seguenti punti:

- Gestione degli aspetti operativi dell'erogazione dei servizi
- Gestione degli aspetti relativi alla sicurezza dei sistemi



# Processi

---

## Processi del dominio DS (Delivery & Support):

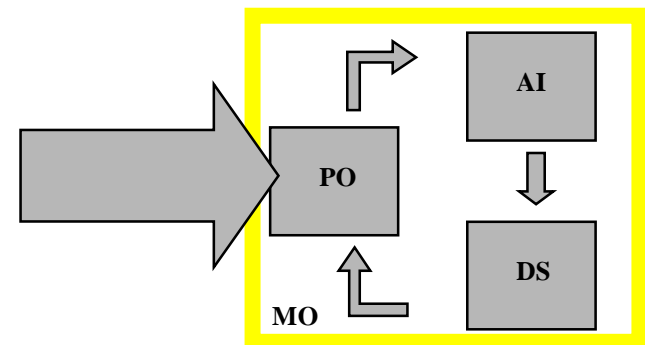
- **DS1 - Definizione dei livelli di servizio**
- **DS2 - Gestione dei servizi di terze parti**
- **DS3 - Gestione delle prestazioni e del dimensionamento**
- **DS4 - Gestione della continuità del servizio**
- **DS5 - Gestione della sicurezza dei sistemi**
- **DS6 - Identificazione e attribuzione dei costi**
- **DS7 - Formazione ed addestramento degli utenti**
- **DS8 - Assistenza e consulenza agli utenti**
- **DS9 - Gestione della configurazione**
- **DS10 - Gestione di anomalie ed incidenti**
- **DS11 - Gestione dei dati**
- **DS12 - Gestione delle infrastrutture**
- **DS13 - Attività operative e di sala macchine**

# Processi

## Processi del dominio MO (Monitoring)

Sono processi i cui obiettivi sono sintetizzabili nei seguenti punti:

- Valutazione periodica dei processi IT finalizzata alla verifica di conformità con gli obiettivi di controllo che l'azienda si è data



# Processi

---

## Processi del dominio MO (Monitoring):

- **M1 - Monitoraggio dei processi**
- **M2 - Valutazione dell'adeguatezza dei controlli interni**
- **M3 - Certificazione da terze parti**
- **M4 - Revisione indipendente dei controlli interni**

# Processi

ESEMPIO: DS4 – Assicurare la continuità del servizio

## Il controllo sul processo IT di

Assicurare la continuità del servizio

**Requisito aziendale**

## Che soddisfi il requisito aziendale

Di far sì che i servizi IT siano disponibili come richiesto e assicurino un minimo impatto aziendale in caso di grave evento distruttivo

## È reso possibile

Dal possesso di un piano di continuità operativo e testato dall'IT che sia in linea con il piano globale di continuità aziendale e con i suoi requisiti aziendali correlati

**Istruzioni di alto livello**

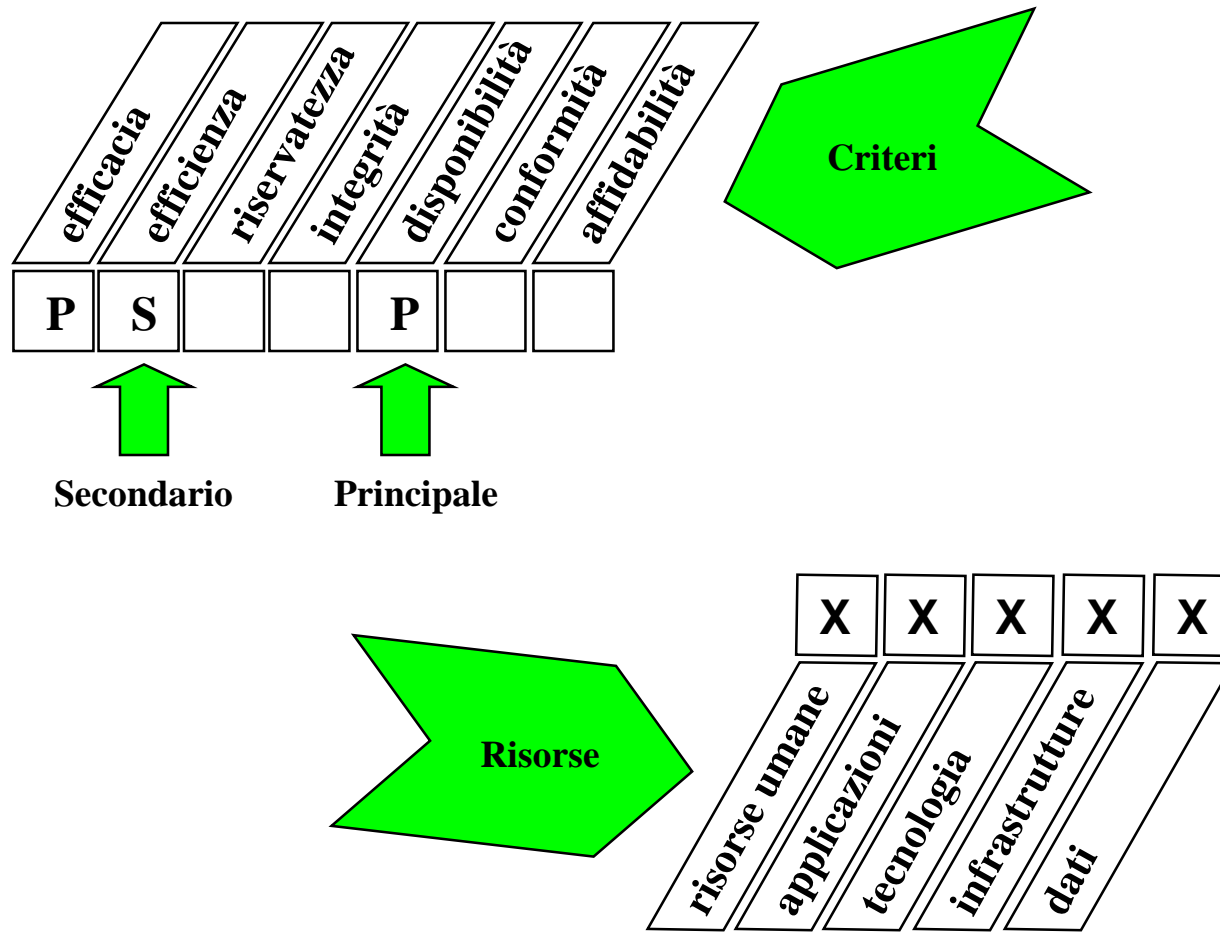
## E considera

- classificazione delle criticità
- procedure alternative
- salvataggio e ripristino
- attività di test e addestramento sistematiche e regolari
- processi di monitoraggio ed escalation
- responsabilità organizzative interne ed esterne
- ...

**Pratiche di controllo**

# Processi

ESEMPIO: DS4 – Assicurare la continuità del servizio



# CobiT

---

## Management Guidelines:

- Documento indirizzato in modo specifico a chi deve implementare un processo di governance dell'IT
- Contiene strumenti (di tipo organizzativo) finalizzati a:
  - ✓ mantenere i processi sotto controllo (CSF)
  - ✓ monitorare il raggiungimento degli obiettivi (KGI)
  - ✓ monitorare le attività all'interno dei processi (KPI)
  - ✓ effettuare scelte strategiche e misurare il livello di una organizzazione limitatamente ai processi IT (Maturity Models)

# CobiT

---

Elementi componenti delle Management Guidelines:

Come per i Control Objectives per ogni processo sono proposti:

- requisiti aziendali
- istruzioni di alto livello
- risorse gestite dal processo
- criteri per le informazioni

Inoltre:

- Le pratiche di controllo sono sostituite da KGI, CSF e KPI
- Maturity Model

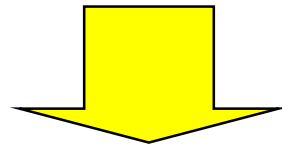
# CobiT

---

## Critical Success Factor (CSF):

- Forniscono l'indicazione su cosa fare per implementare i controlli a livello di processo
- Per fare in modo che gli obiettivi del processo siano raggiunti, sono “le cose più importanti da fare” dal punto di vista:

- ✓ strategico
- ✓ tecnico
- ✓ organizzativo
- ✓ procedurale



- Indicazioni esplicite su ciò che deve essere fatto

# CobiT

---

## Critical Success Factor (CSF):

ESEMPIO: DS4 – Assicurare la continuità del servizio

- Un gruppo di continuità è installato e testato regolarmente
- Rischi potenziali per la disponibilità sono individuati e affrontati in modo proattivo
- Componenti critici dell'infrastruttura sono identificati e continuamente monitorati
- Al fine di garantire la continuità del servizio:
  - sono svolte attività periodiche di capacity planning
  - acquisizione di componenti ad alta affidabilità
  - acquisizione di componenti ridondati
  - esistono piani di contingency testati
  - sono rimossi i single point of failure

# CobiT

---

- Sono intraprese azioni a seguito di “lezioni imparate” dai test e da incidenti reali
- E’ regolarmente svolta una attività di analisi dei requisiti di disponibilità
- SLA (service level agreements) sono utilizzati per accrescere la consapevolezza e la cooperazione di fornitori legati a necessità di continuità
- Il processo di escalation (trasferimento delle responsabilità di soluzione di un problema ad un livello gerarchico e di competenza superiore) è compreso in modo chiaro e basato su una classificazione dei possibili incidenti relativi alla disponibilità
- I costi aziendali per l’interruzione dei servizi sono, quando possibile, quantificati: devono fornire la motivazione per lo sviluppo di piano appropriati e la predisposizione di infrastrutture per la continuità

# CobiT

---

Alcuni commenti:

- i CSF non sono un concetto originale del CobiT!!!
- sono direttamente focalizzati sul processo IT → si applicano direttamente

# CobiT

---

## Key Performance Indicators:

- Sono indicatori che segnalano come il processo si sta evolvendo per raggiungere il requisito di business del processo

## Caratteristiche:

- Sono indicatori quantitativi (non qualitativi)
- Predicono la probabilità di successo o fallimento nel futuro per il processo
- Orientati al processo cui si riferiscono, ma focalizzati sull'IT
- ...

# CobiT

---

## Key Performance Indicators:

ESEMPIO: DS4 – Assicurare la continuità del servizio

- Numero di problemi per la continuità del servizio non risolti o non affrontati
- Tempo intercorso tra cambiamenti organizzativi e aggiornamento del piano di continuità
- Tempo per diagnosticare un incidente e decidere l'esecuzione del piano di continuità
- Tempo per normalizzare il livello del servizio dopo l'esecuzione del piano di continuità
- Frequenza del training
- Frequenza dei test
- ...

# CobiT

---

## Key Performance Indicators:

- Rispetto ad un KPI l'organizzazione deve:
  - ✓ definire l'oggetto della misurazione
  - ✓ impostare la metrica
  - ✓ definire lo strumento utilizzato per la misurazione
  
- Gli indicatori individuati come KPI devono essere raccolti in appositi report da proporre a coloro che hanno la responsabilità sul processo
  
- Non c'è relazione diretta tra CSF e KPI (alcuni CSF possono non essere misurabili in modo quantitativo)

# CobiT

---

## Key Goal Indicators:

- rappresentano l'obiettivo da raggiungere

## Caratteristiche:

- Indicatori quantitativi (quando possibile)
- Orientati all'IT, ma guidati dalle esigenze di business

## Nota

- il KPI dice quanto bene stiamo andando
- il KGI dice se abbiamo raggiunto l'obiettivo

# CobiT

---

## Key Goal Indicators:

ESEMPIO: DS4 – Assicurare la continuità del servizio

- Nessun incidente causa di imbarazzo
- Numero di processi di business critici che fanno affidamento sull'IT e che hanno adeguati piani di continuità
- Prove regolari e formali che i piani di continuità funzionino
- Riduzione dei tempi di downtime
- Numero di componenti critici dell'infrastruttura con monitoraggio automatico della disponibilità

# CobiT

---

## Key Goal Indicators:

➤ Similmente a quanto visto per i KPI, rispetto ad un KGI l'organizzazione deve:

- ✓ definire l'oggetto della misurazione
- ✓ impostare la metrica
- ✓ definire lo strumento utilizzato per la misurazione

## Nota:

I KPI e i KGI misurano oggetti diversi (collegati a livello logico all'interno del processo).

# CobiT

---

In definitiva:

➤ CSF

Devo farlo per avere il controllo

➤ KPI serve per monitorare progressivamente l'attività collegata al processo

➤ KGI segnala il raggiungimento o meno dell'obiettivo → deve essere deciso dall'organizzazione

# CobiT

---

Qualche altro esempio:

AI2 – Acquisizione e mantenimento di software applicativo

Requisito di business: fornire al business applicazioni che lo supportino in modo efficace

Istruzione di alto livello per il controllo: esistenza di una metodologia “robusta”

CSF:

- La metodologia di acquisizione e implementazione è fortemente sostenuta dal senior management
- ...
- C'è separazione delle funzioni tra attività di sviluppo e attività di test
- 

strategico

organizzativo

# CobiT

## KPI:

➤ Numero di richieste di modifica collegate a “bug”, di errori critici riscontrati e specifiche di nuove funzionalità

**Misuro l'efficacia collegata all'applicazione della metodologia**

➤ ...

➤ Numero di deviazioni dalle procedure standard, come applicazioni non documentate, progetti non approvati e riduzione delle attività di test a causa della necessità di rispettare i tempi di consegna

**Misuro il numero di eccezioni rispetto a quanto previsto dalla metodologia**

➤ ...

# CobiT

## KGI:

- Numero di applicazioni consegnate secondo le scadenze previste, ...
- Numero di applicazioni senza problemi di integrazione durante l'implementazione
- ...
- Numero di problemi rilevati in produzione (suddivisi per applicazione) che hanno causato degrado della qualità del servizio o periodi di sospensione del servizio
- ...



**KPI → misurano attività interne all'IT**

**KGI → misurano l'effetto sul business**

# CobiT

---

## ESERCIZIO:

Processo: frequentare l'università

- Obiettivo di alto livello?
- CSF ?
- KPI ?
- KGI ?

# CobiT

## ESERCIZIO:

Processo: frequentare l'università

➤ Obiettivo di alto livello?

- ✓ laurearsi in un tempo ragionevole e con un voto dignitoso

➤ CSF ?

- ✓ motivazione personale

“strategico”

- ✓ “genitori assillanti”

“strategico”

- ✓ frequenza costante delle lezioni

“organizzativo”

- ✓ studio giorno per giorno

- ✓ ...


“organizzativo”

# CobiT

---

## ➤ KPI ?

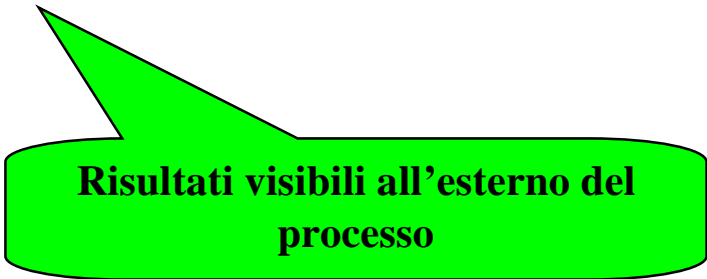
- ✓ votazione media
- ✓ rapporto numero esami superati / anni



**Come sto andando?**

## ➤ KGI ?

- ✓ voto di laurea obiettivo
- ✓ tempo di permanenza all'università obiettivo



**Risultati visibili all'esterno del  
processo**

# CobiT

---

## Maturity models:

- I Maturity Models costituiscono il tentativo di fornire alle organizzazioni uno strumento per misurare il livello dei processi
- Per ogni processo sono definiti 6 scenari cui è associata una scala di valori crescente:
  - ✓ 0 – processo non esistente
  - ✓ 1 – processo allo stadio iniziale
  - ✓ 2 – processo ripetibile
  - ✓ 3 – processo definito
  - ✓ 4 – processo gestito
  - ✓ 5 – processo ottimizzato

# CobiT

---

- **0 – processo non esistente**
  - ✓ non c'è o l'organizzazione non ha percepito il problema
- **1 – processo allo stadio iniziale**
  - ✓ approccio disorganizzato, soluzioni ad hoc
- **2 – processo ripetibile**
  - ✓ persone diverse seguono procedure simili per attività simili
- **3 – processo definito**
  - ✓ procedure standardizzate e documentate
  - ✓ è lasciato agli individui il compito di seguirle
- **4 – processo gestito**
  - ✓ è effettuato un monitoraggio sulle procedure
  - ✓ sono in atto processi per gestire il miglioramento
- **5 – processo ottimizzato**
  - ✓ processo a livello di best practice
  - ✓ in atto procedure per il benchmarking

# CobiT

---

## Struttura degli scenari

Gli scenari possono coprire, secondo i processi, i seguenti aspetti:

- grado di comprensione e consapevolezza dei rischi relativi al processo
- modalità di training e comunicazione
- approccio alla gestione del processo
- uso di strumenti tecnologici e automatizzati a supporto della gestione dei processi
- compatibilità tra le attività e policy interne, normative, regolamenti, ...
- expertise coinvolta nei processi

# CobiT

---

## Esempio

AI2 – Acquisire e mantenere software applicativo

Scenario 2 – Ripetibile ma intuitivo

Si rilevano processi simili per l'acquisizione e il mantenimento delle applicazioni, ma sono basati sull'esperienza del personale IT, non su un processo documentato.

La percentuale di successo con le applicazioni dipende in modo sostanziale da skill interni e dal livello di esperienza dell'IT.

La manutenzione è di solito problematica ed è resa più difficile nel caso di perdita di competenze interne.

**Approccio alla gestione del  
processo**

# CobiT

---

## Esempio

AI2 – Acquisire e mantenere software applicativo

Scenario 4 – Gestito e misurabile

Si rileva una metodologia formale, chiara, ben compresa per l'acquisizione e il mantenimento dei sistemi; tale metodologia include un processo formale per la definizione dei requisiti progettuali, un processo per il test ...

E' in atto un meccanismo formale di approvazione dei vari passi previsti dalla metodologia e di autorizzazione delle eccezioni.

...

**Approccio alla gestione del  
processo**

# CobiT

---

Come si possono usare?

- Gli scenari proposti costituiscono la metrica con la quale individuare il “punteggio” da attribuire ad una organizzazione
- Occorre quindi analizzare lo stato dell’organizzazione rispetto al processo e individuare lo scenario più vicino alla realtà aziendale.
- Può non essere immediato (e in generale non lo è) attribuire il “punteggio” perché lo stato di un processo può essere la combinazione di elementi corrispondenti a punteggi diversi
  - ✓ i vari elementi dello scenario sono disaggregati e valutati singolarmente
  - ✓ attraverso un meccanismo di ponderazione si valuta qual è lo scenario che comprende più elementi applicabili allo stato del processo

# CobiT

---

A cosa servono i punteggi acquisiti?

- Confronto della situazione aziendale con la best practice rappresentata dallo scenario 5 → capisco quanto lontano sono dall'ottimo
- Confronto tra competitor → potrei realizzare una indagine tra possibili fornitori e valutarli in modo oggettivo (nell'ipotesi che, oltre al prodotto fornito, sia di vitale importanza per il servizio la qualità dell'organizzazione che fornisce il prodotto stesso)

# Metodologia ITRMB KPMG

---

## Alcune considerazioni sul “benchmarking”

- La ricerca del confronto con le altre organizzazioni è considerata è considerata una pratica “sana” per il miglioramento
- KPMG ha sviluppato una metodologia ed un servizio che permette alle organizzazioni di confrontarsi con organizzazioni simili
- La metodologia ITRMB e il benchmarking

# Materiale per consultazione

---

- I manuali del CobiT

<http://www.isaca.org>