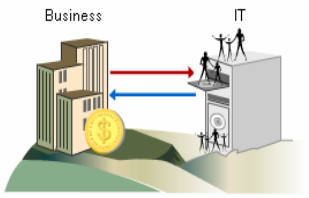
IT Governance & CobiT

Prof. Ing. Claudio Cilli
CISA, CIA, CISSP, CISM

Il bisogno dell'IT Governance



Strategic Alignment

Aligning IT with Business

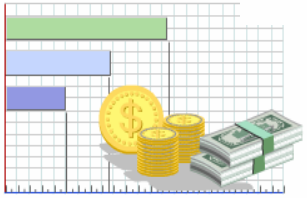
Poor Security Assurances

Security

Keeping IT Running

Handling External Relationship

Managing Complexity



Value/Cost

Regulatory Compliance

Le organizzazioni richiedono un approccio strutturato per gestire queste e le altre sfide.

Ciò assicurerà che ci sia allineamento tra gli obiettivi per l'IT, buone pratiche di controllo manageriale e efficace monitoraggio delle performance, per rimanere competitivi e evitare disguidi e spese inaspettati.

Il bisogno dell'IT Governance

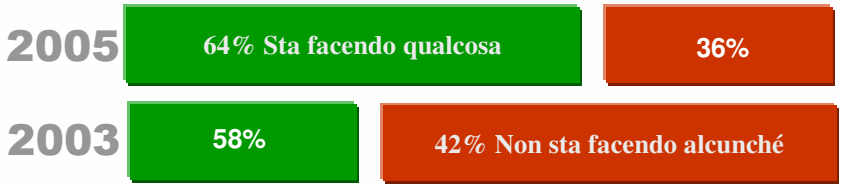
Enterprise governance consiste in un insieme di responsabilità e pratiche esercitate dall'alta direzione e dal management esecutivo con l'obiettivo di:

- Definire gli **indirizzi strategici**
- Assicurare che gli **obiettivi** siano raggiunti
- Accertare che i **rischi** siano gestiti in modo appropriato
- Verificare che le **risorse aziendali** siano impiegate responsabilmente

IT Governance, secondo la definizione dell'ITGI

IT governance è:

- La responsabilità dell'alta direzione e del management esecutivo
- Una **parte integrale** del governo dell'impresa, consistente in leadership, strutture organizzative e processi al fine di assicurare che l'**IT dell'impresa sostenga ed estenda le strategie e gli obiettivi dell'organizzazione**

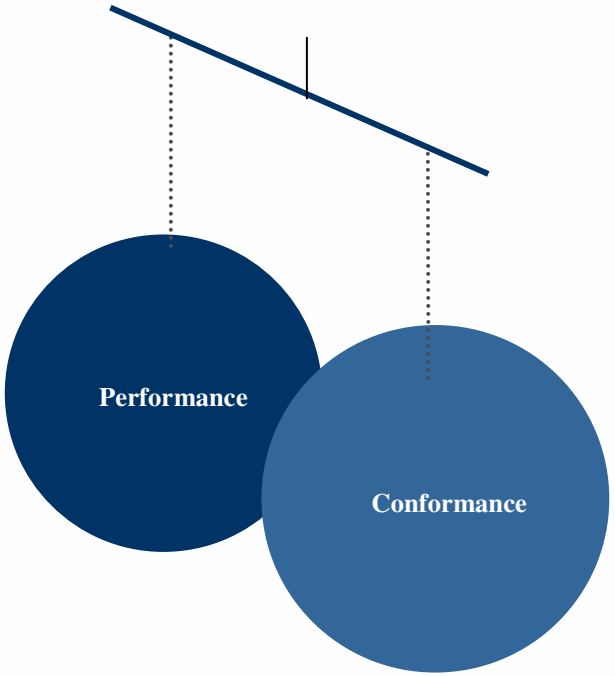


Source: Surveys by PwC for the IT Governance Institute Sep-Oct 2003 and Sep-Oct 2005

Il governo dell'impresa guida l'IT Governance

Governo d'impresa (enterprise governance) è:

- **Conformità**
  - Aderire alla legislazione, politiche interne, requisiti di audit, ecc.
- **Performance**
  - Migliorare la capacità di realizzare profitto, efficienza, efficacia, crescita, ecc.



Enterprise governance e IT governance richiedono un bilanciamento tra conformità e obiettivi di performance, secondo le direttive aziendali.

COBIT definisce un Framework per l'IT Governance

COBIT aiuta a superare i gap tra i rischi di business, le necessità di controllo e gli aspetti tecnici. Fornisce pratiche di controllo divise tra i vari domini e la struttura dei processi e presenta le attività organizzate in una struttura logica e gestibile

COBIT:

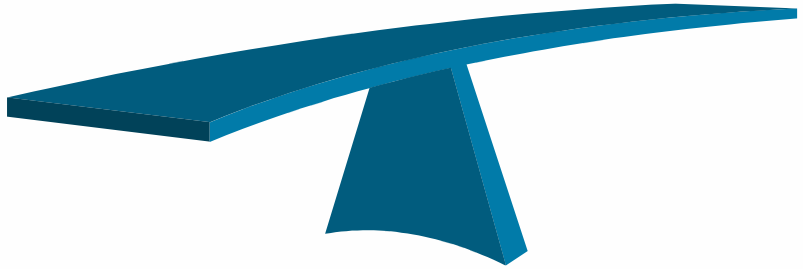
- Inizia dai requisiti di business
- E' orientato ai processi, organizzando le attività IT in un modello dei processi generalmente accettato
- Identifica le risorse IT principali su cui agire
- Definisce gli obiettivi di controllo manageriale da considerare
- Incorpora i principali standard internazionali
- E' diventato lo standard *de facto* per l'intero controllo dell'IT

Le risorse IT devono essere gestite da un insieme di processi raggruppati in modo naturale. COBIT fornisce un framework per raggiungere questo obiettivo

Come COBIT aiuta a implementare un'efficace IT Governance?

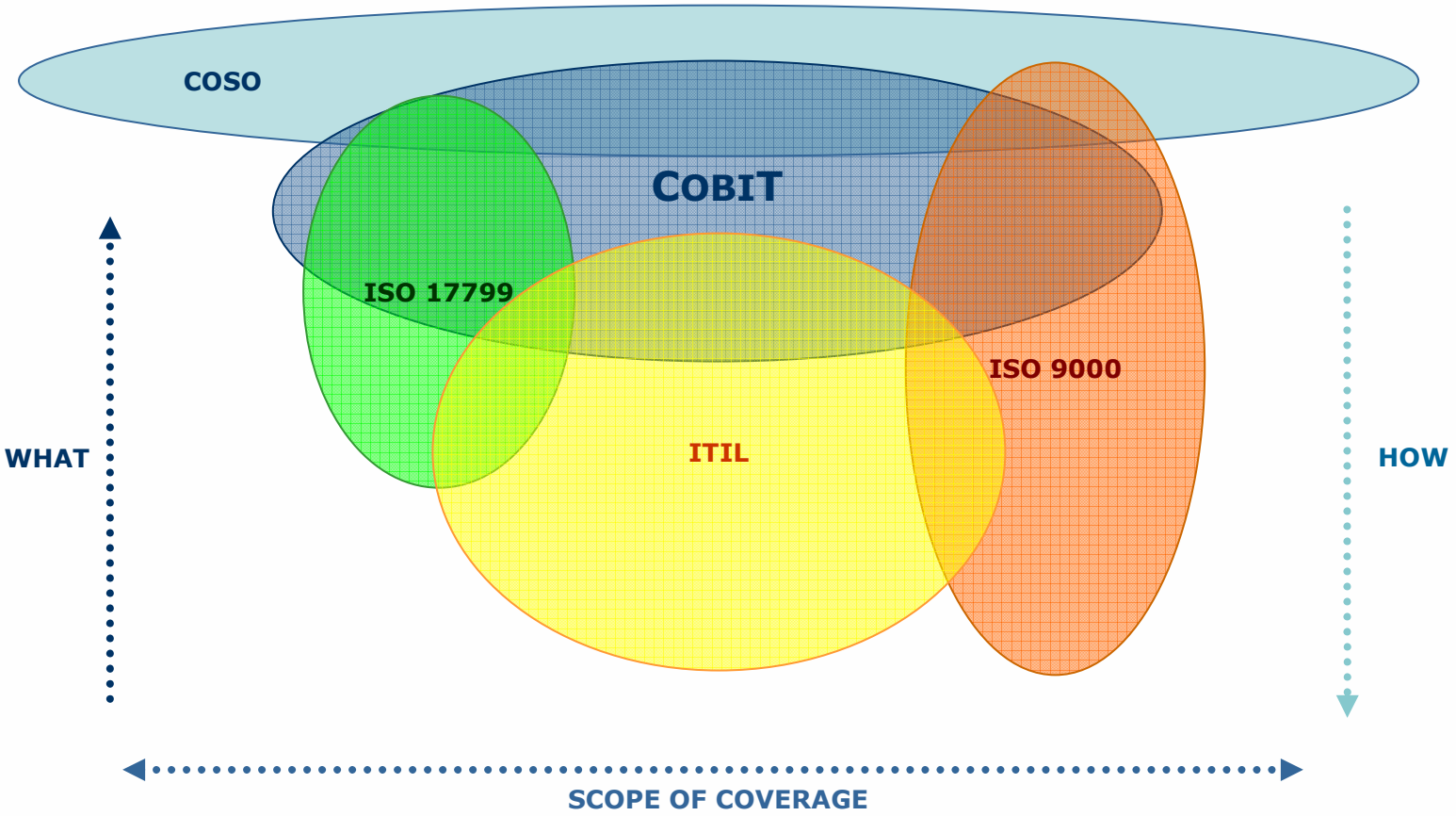
COBIT garantisce i seguenti vantaggi a uno sforzo di implementazione dell'IT governance:

- Abilita la mappatura degli obiettivi IT a quelli di business e *vice versa*
- Migliore allineamento, basato sul focus sul business
- Una visione di cosa fa l'IT che sia comprensibile alla direzione
- Chiara definizione di proprietà e responsabilità basata su un orientamento al processo
- Generale accettazione da parte di terze parti e organismi legislatori e regolatori
- Comprensione condivisa tra tutte le parti interessate, basata su un linguaggio comune
- Completo adeguamento ai requisiti COSO riguardo l'ambiente di controllo IT

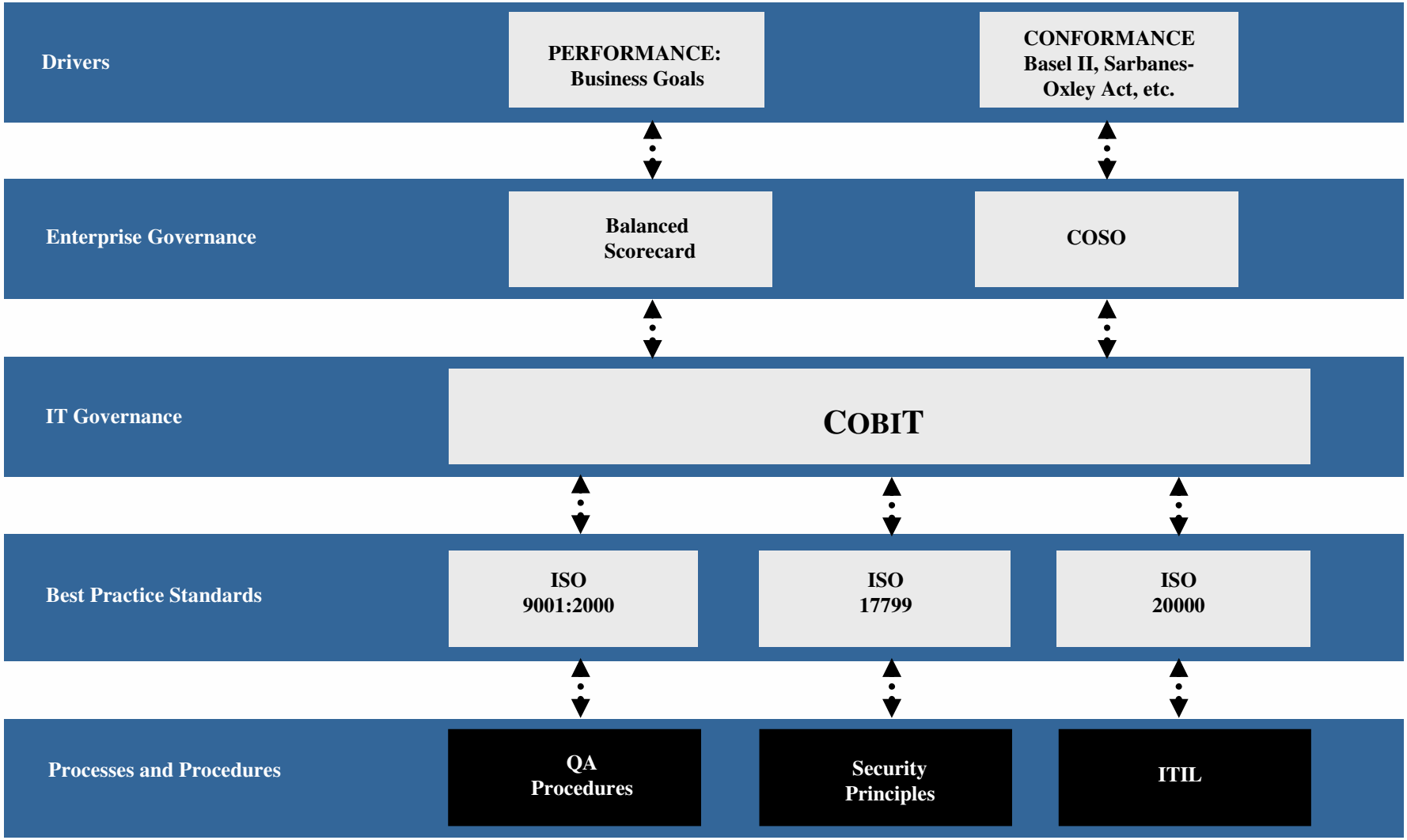


COBIT e gli altri IT Management Framework

Le organizzazioni considerano e utilizzano una varietà di modelli IT, standard e best practice. Questi devono essere compresi in modo da considerare come possano essere usati insieme, con COBIT che agisce da consolidatore ("ombrello").

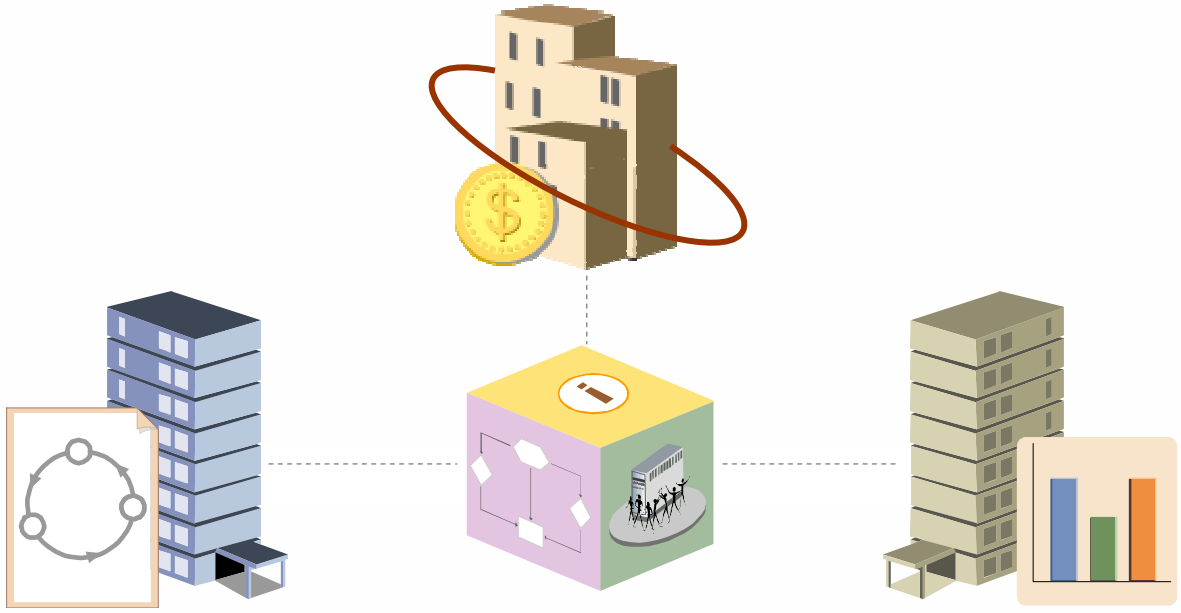


Dove si colloca COBIT?



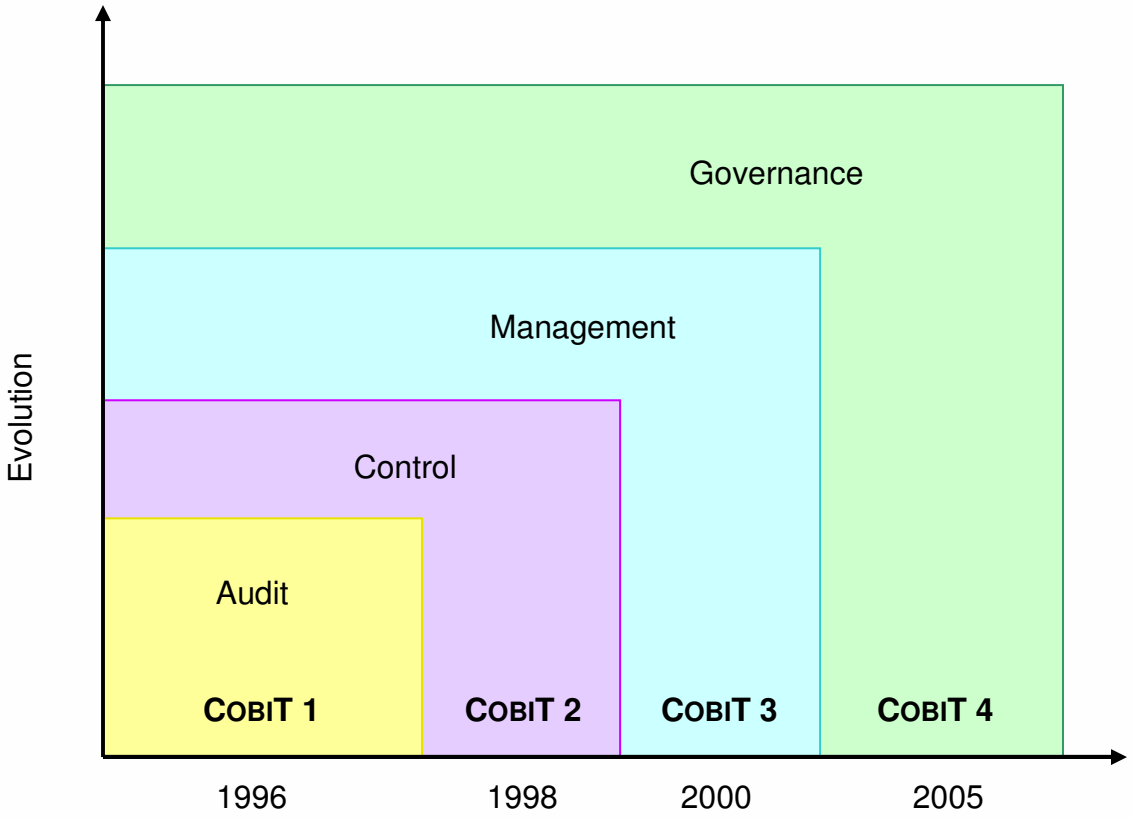
COBIT Framework

- Il framework COBIT è stato creato con le seguenti caratteristiche:
  - "Business-focused"
  - "Process-oriented"
  - "Controls-based"
  - "Measurement-driven"
- L'acronimo COBIT sta per *Control Objectives for Information and related Technology*.



Caratteristiche del Framework COBIT

COBIT: Un Framework per il Controllo IT



Per gli ultimi aggiornamenti su COBIT, vedere *www.isaca.org/cobit*

COBIT: Valore e Limitazioni

COBIT:

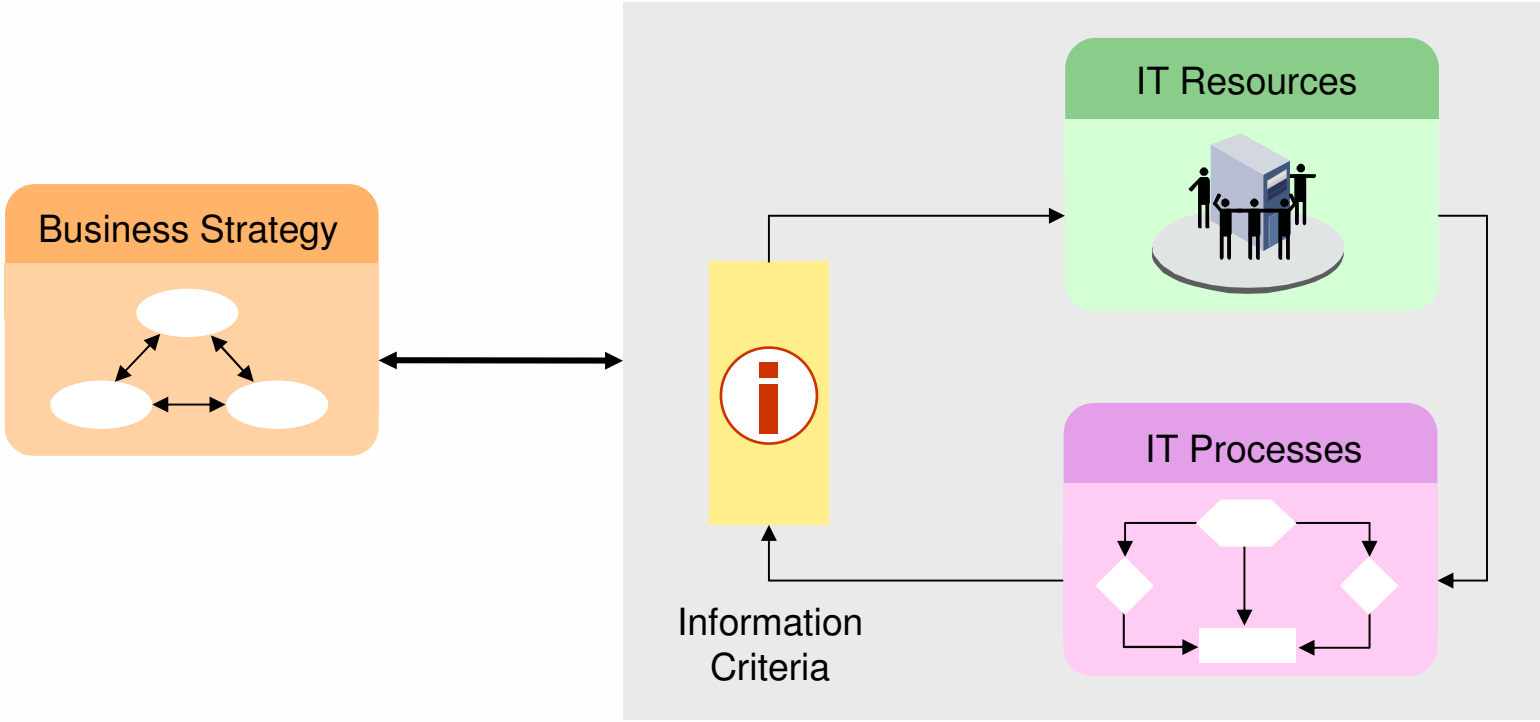
- E' stato intenzionalmente accettato come "good practice"
- E' management-oriented
- E' supportato da tool automatizzati e training
- E' scaricabile gratuitamente dal sito Isaca
- Consente la condivisione delle conoscenze degli esperti che hanno contribuito alla sua realizzazione
- Si evolve e si aggiorna continuamente
- E' mantenuto da un'organizzazione internazionale di chiara fama
- Mappato al 100% al COSO
- Mappato strettamente a tutti i principali standard correlati
- E' da intendersi come riferimento, non come metodologia omnicomprensiva

Le imprese hanno ancora bisogno di analizzare i requisiti di controllo e personalizzare COBIT basandosi sui loro:

- Elementi abilitatori del valore
- Profilo di rischio
- Infrastruttura IT, organizzazione e portafoglio progetti

COBIT: Componenti

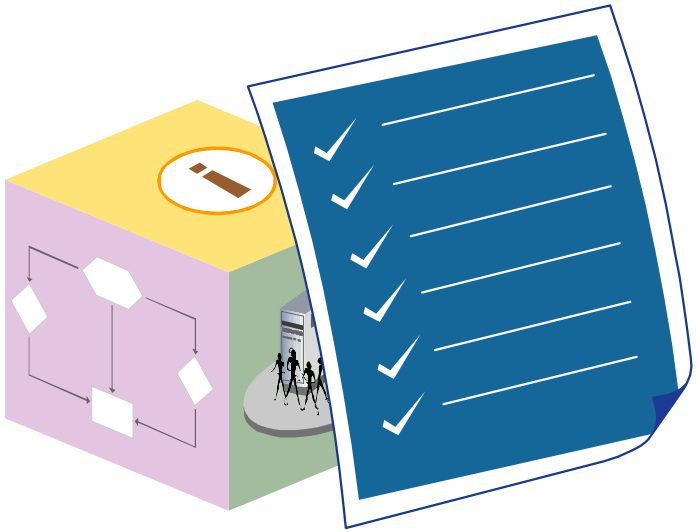
Un'organizzazione dipende da dati e informazioni affidabili e tempestivi. I componenti di COBIT forniscono un framework completo per erogare valore mentre si gestiscono il rischio e i controlli



COBIT: Vantaggi

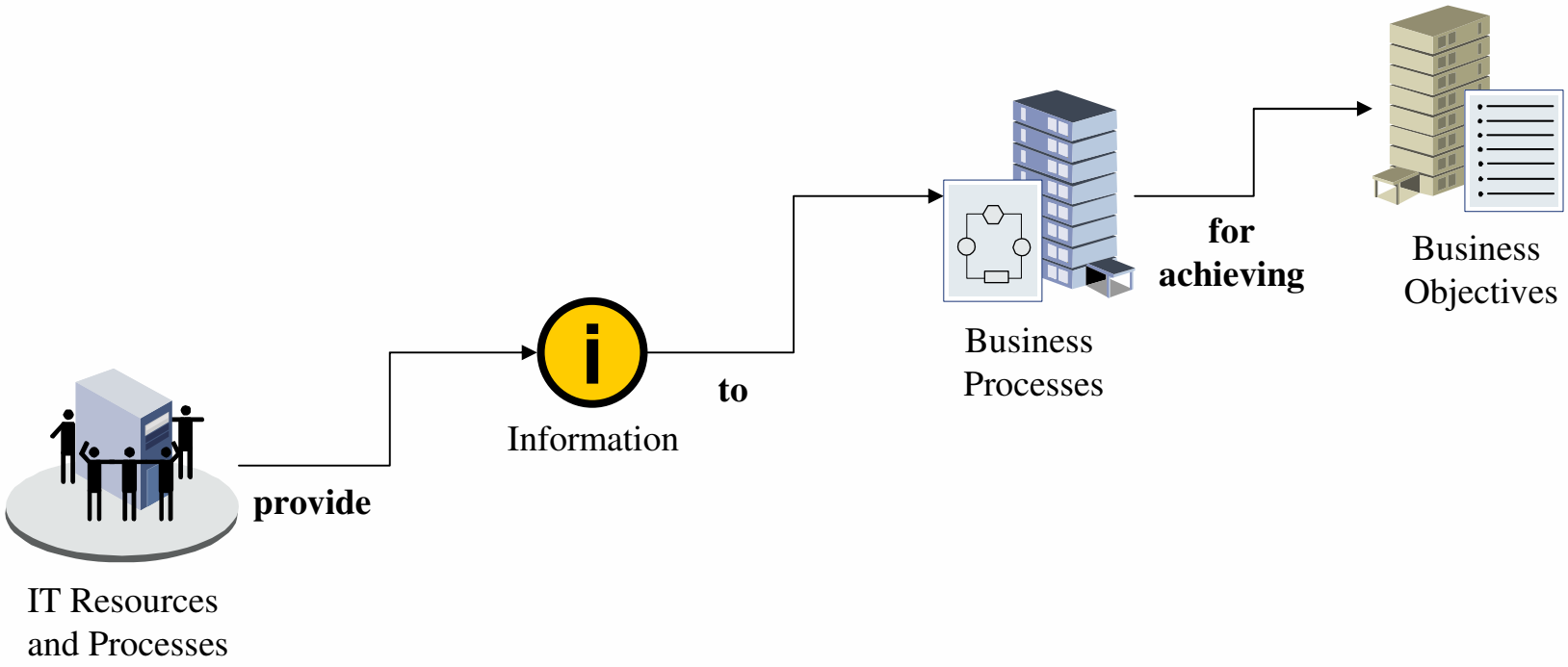
Alcuni vantaggi derivanti dall'adozione di COBIT sono:

- COBIT è allineato con gli altri standard e le good practice e dovrebbe essere utilizzato insieme ad esse
- Il framework di COBIT e le best practice che lo supportano determinano un ambiente IT correttamente gestito e flessibile
- COBIT fornisce un ambiente di controllo che risponde ai requisiti di business ed è al servizio del management e delle funzioni di audit relativamente alle rispettive responsabilità di controllo
- COBIT è corredato di strumenti che aiutano a gestire le attività IT



COBIT: Premessa

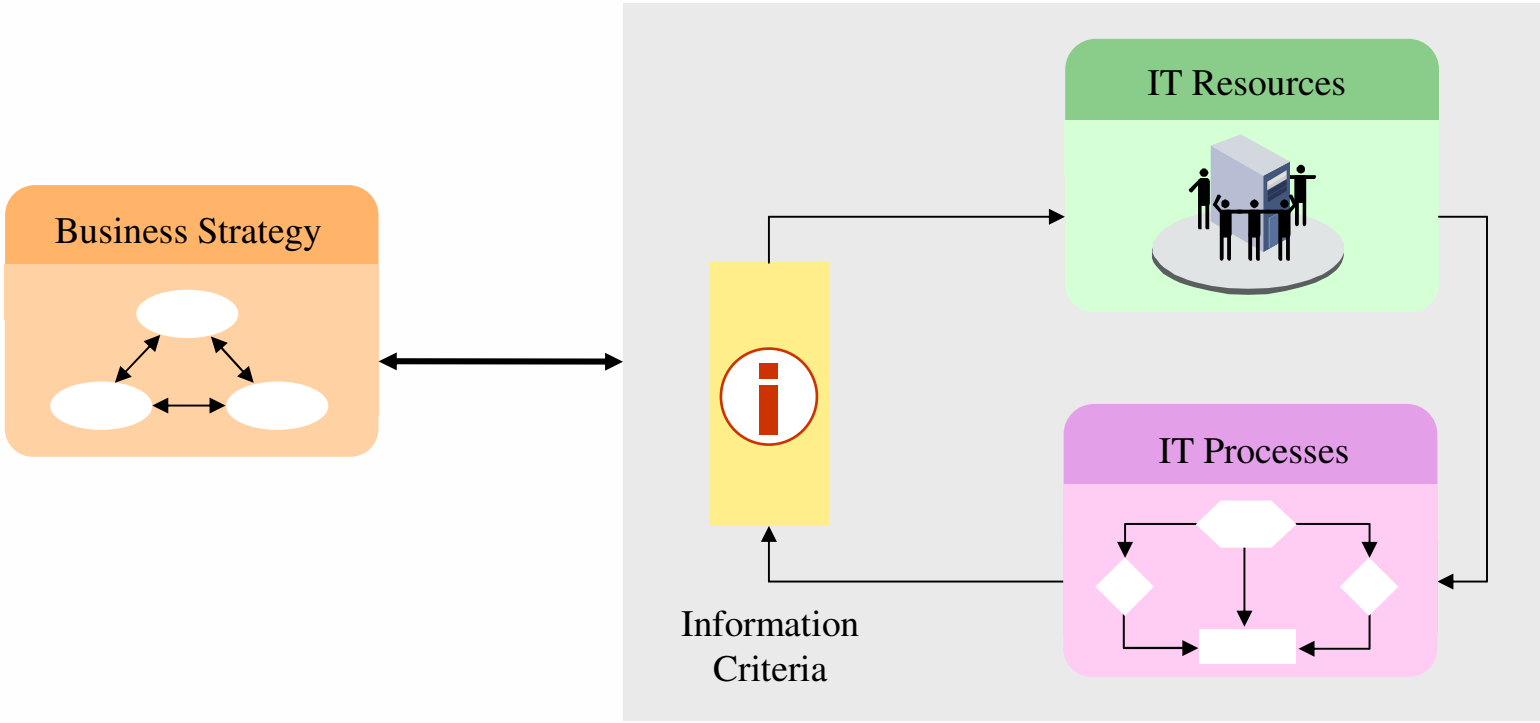
- Il framework COBIT è basato sulla premessa che l'IT ha bisogno di fornire le informazioni di cui l'organizzazione ha bisogno per conseguire i suoi obiettivi



- Il framework COBIT aiuta ad allineare l'IT al business concentrandosi sui requisiti delle informazioni di business e organizzando in tal senso le risorse IT. COBIT fornisce il framework e le linee guida per implementare l'IT governance.

COBIT: Principio

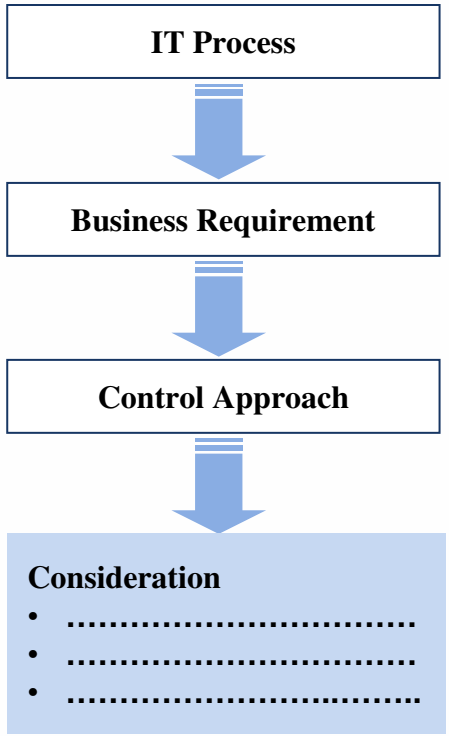
Il principio del framework COBIT è legare le aspettative del management dall'IT con le responsabilità della gestione IT. L'obiettivo è quello di facilitare l'IT governance per produrre valore gestendo nel contempo i rischi IT

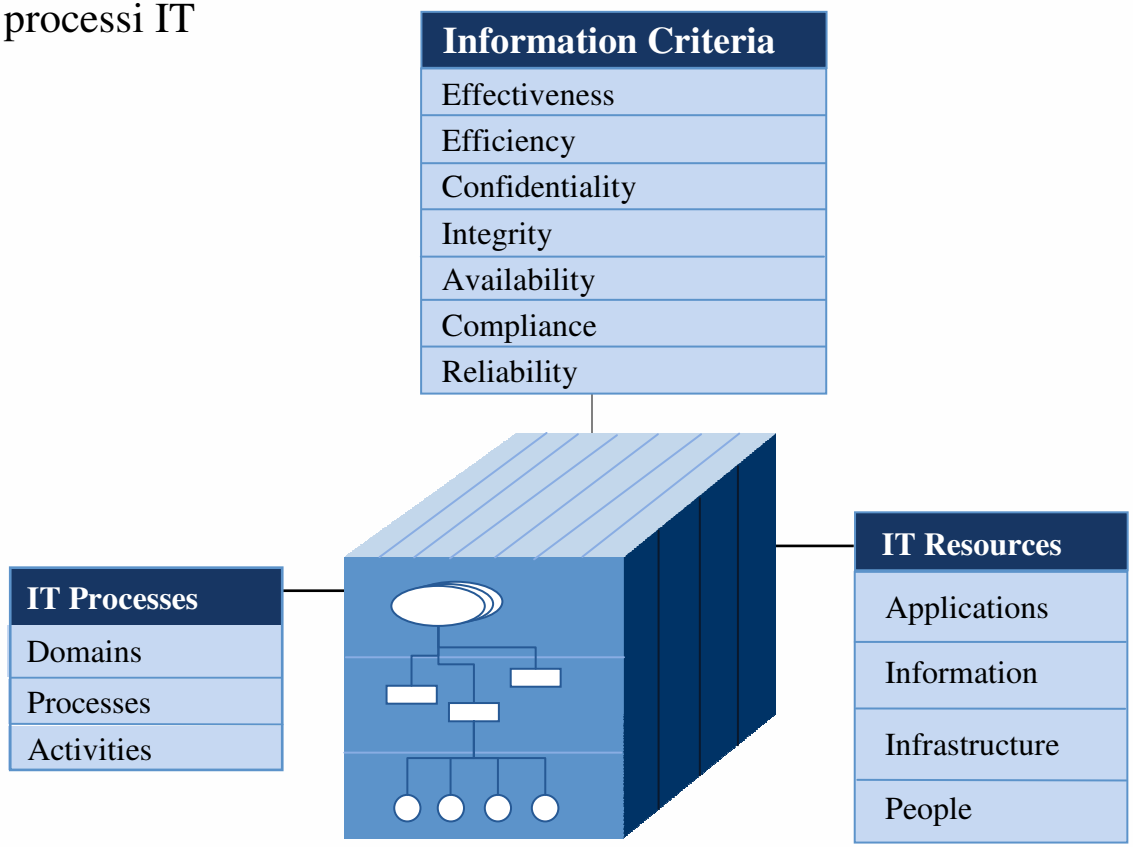


COBIT Framework

In quanto framework per il controllo e la governance dell'IT, COBIT si concentra su due aree principali:

- Fornire le informazioni richieste per supportare gli obiettivi di business e i requisiti
- Trattare le informazioni come risultato dell'applicazione combinata delle risorse legate all'IT che devono essere gestite dai processi IT

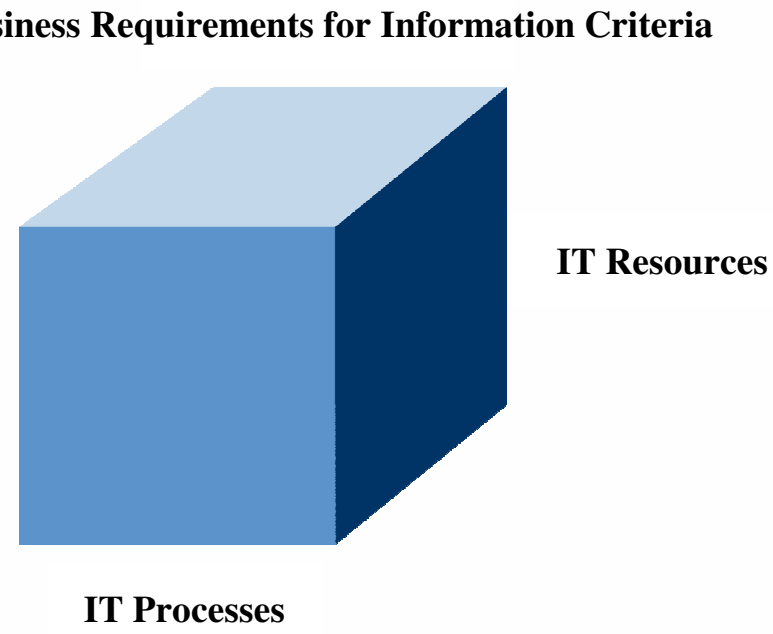




COBIT Cube

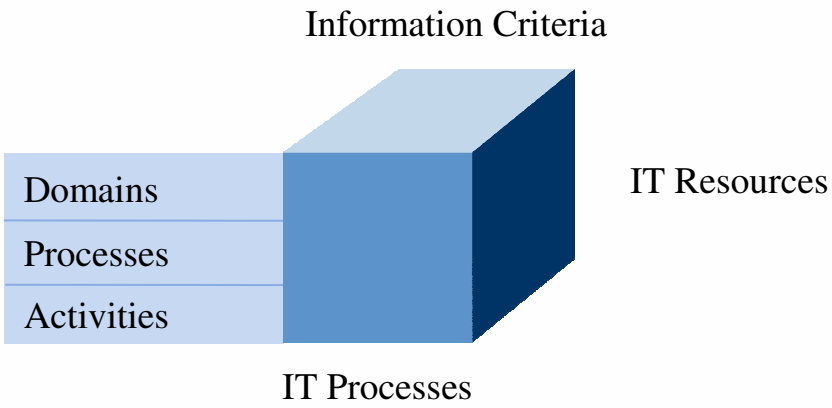
Il COBIT framework descrive come i processi IT erogano le informazioni di cui il business ha bisogno per raggiungere i propri obiettivi

Per controllare questo processo, COBIT fornisce tre elementi chiave, ognuno dei quali costituisce una dimensione COBIT cube.



COBIT Cube: Processi IT

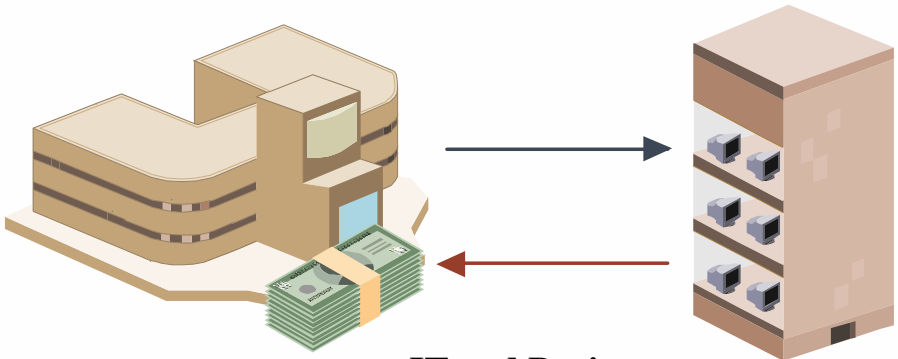
- COBIT descrive il ciclo di vita dell'IT mediante quattro **domini**:
  - Pianificazione & Organizzazione (Plan & Organise)
  - Acquisizione & Implementazione (Acquire & Implement)
  - Erogazione & Supporto (Deliver & Support)
  - Monitoraggio & Valutazione (Monitor & Evaluate)
- **Processi:** sono serie di attività con punti di controllo naturali. Vi sono 34 processi distribuiti fra i quattro domini. Questi processi specificano cosa il business richiede per raggiungere i propri obiettivi. L'erogazione dell'informazione è controllata tramite i 34 processi IT
- **Attività:** sono azioni necessarie a conseguire risultati misurabili. Inoltre, le attività hanno un ciclo di vita e comprendono diversi task discreti



COBIT Cube: Domini IT

Plan and Organise (PO)

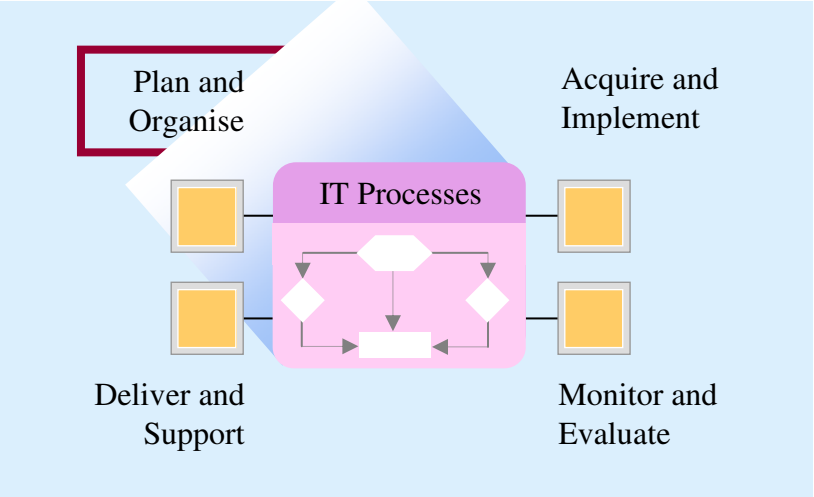
- Obiettivi:
  - Formulare strategia e tattica
  - Identificare come l'IT può meglio contribuire al raggiungimento degli obiettivi di business
  - Pianificare, comunicare e gestire la realizzazione della visione strategica
  - Implementare l'infrastruttura organizzativa e tecnologica
- Scopo:
  - L'IT e il business sono allineati strategicamente?
  - L'impresta sta facendo l'uso migliore delle proprie risorse?
  - Gli obiettivi IT sono compresi da tutti nell'organizzazione?
  - I rischi IT sono compresi e gestiti?
  - La qualità dei sistemi IT è appropriata per i bisogni del business?



IT and Business

COBIT Cube: Domini IT *(Cont.)*

Si consideri il modello dei processi di COBIT, che consiste di 34 processi IT definiti nell'ambito dei quattro domini IT



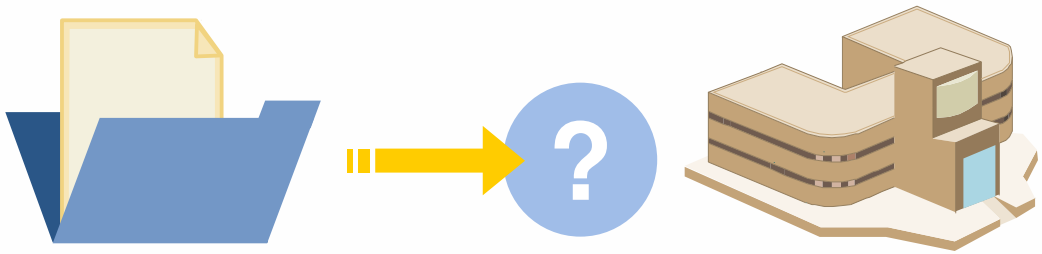
Plan and Organise

PO1 Define a strategic IT plan.
PO2 Define the information architecture.
PO3 Determine technological direction.
PO4 Define the IT processes, organisation and relationships.
PO5 Manage the IT investment.
PO6 Communicate management aims and direction.
PO7 Manage IT human resources.
PO8 Manage quality.
PO9 Assess and manage IT risks.
PO10 Manage projects.

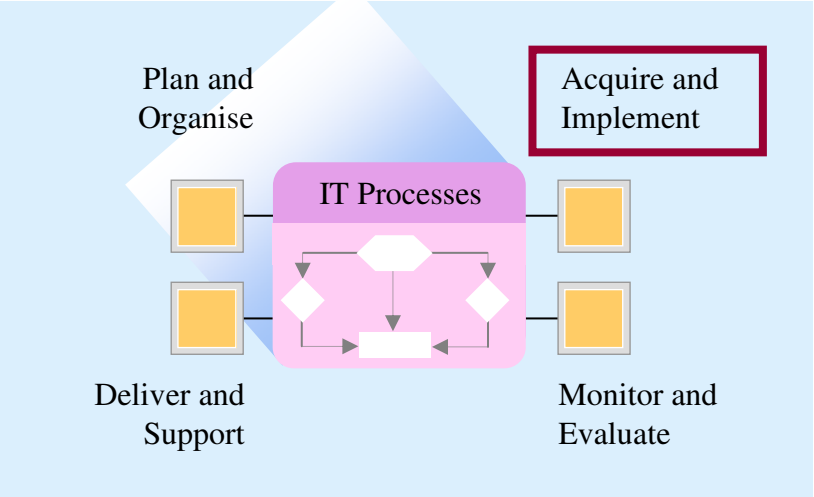
COBIT Cube: Domini IT *(Cont.)*

Acquire and Implement (AI)

- Obiettivi:
  - Identificare, sviluppare o acquisire, implementare, e integrare le soluzioni IT
  - Cambiamenti e manutenzione dei sistemi esistenti
- Scopo:
  - I nuovi progetti sono in grado di fornire soluzioni che soddisfino i requisiti del business?
  - I nuovi progetti sono in grado di essere completati nei tempi previsti e nei limiti del budget?
  - I nuovi sistemi opereranno adeguatamente quando implementati?
  - Le modifiche saranno apportate senza alterare le operazioni di business correnti?



COBIT Cube: Domini IT *(Cont.)*



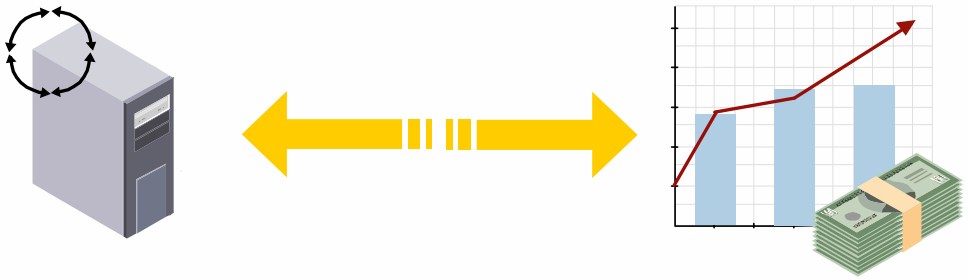
Acquire and Implement

AI1 Identify automated solutions.
AI2 Acquire and maintain application software.
AI3 Acquire and maintain technology infrastructure.
AI4 Enable operation and use.
AI5 Procure IT resources.
AI6 Manage changes.
AI7 Install and accredit solutions and changes.

COBIT Cube: Domini IT *(Cont.)*

Deliver and Support (DS)

- Obiettivi:
  - L'erogazione puntuale dei servizi che saranno richiesti, compresi quelli attuali
  - La gestione della sicurezza, continuità, strutture per dati e operazioni
  - Assistenza e supporto per gli utenti
- Scopo:
  - I servizi IT sono erogati in linea con le priorità del business?
  - I costi dell'IT sono ottimizzati?
  - Le persone sono in grado di utilizzare i sistemi IT con produttività e sicurezza?
  - Sono in vigore le corrette misure per la riservatezza, integrità e disponibilità?



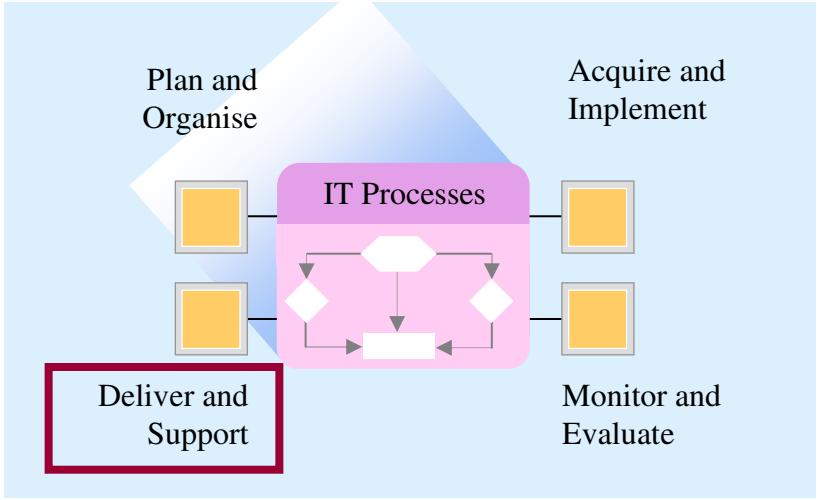
IT Services

Business Priorities

COBIT Cube: Domini IT *(Cont.)*

Deliver and Support

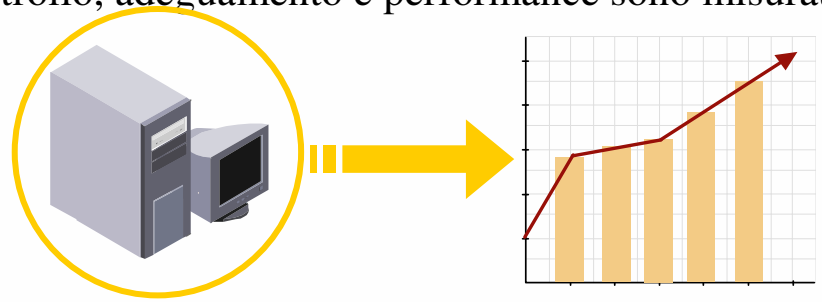
DS1 Define and manage service levels.
DS2 Manage third-party services.
DS3 Manage performance and capacity.
DS4 Ensure continuous service.
DS5 Ensure systems security.
DS6 Identify and allocate costs.
DS7 Educate and train users.
DS8 Manage service desk and incidents.
DS9 Manage the configuration.
DS10 Manage problems.
DS11 Manage data.
DS12 Manage the physical environment.
DS13 Manage operations.



COBIT Cube: Domini IT *(Cont.)*

Monitor and Evaluate (ME)

- Obiettivi:
  - Gestione delle performance
  - Monitoraggio dei controlli interni
  - Adeguamento a leggi e normative
  - Governance
- Scopo:
  - La performance dell'IT è misurata in modo da rilevare i problemi prima che sia troppo tardi?
  - Il management garantisce che i controlli interni siano efficaci ed efficienti?
  - La performance dell'IT può essere collegata agli obiettivi di business?
  - Rischio, controllo, adeguamento e performance sono misurati e inclusi in report?

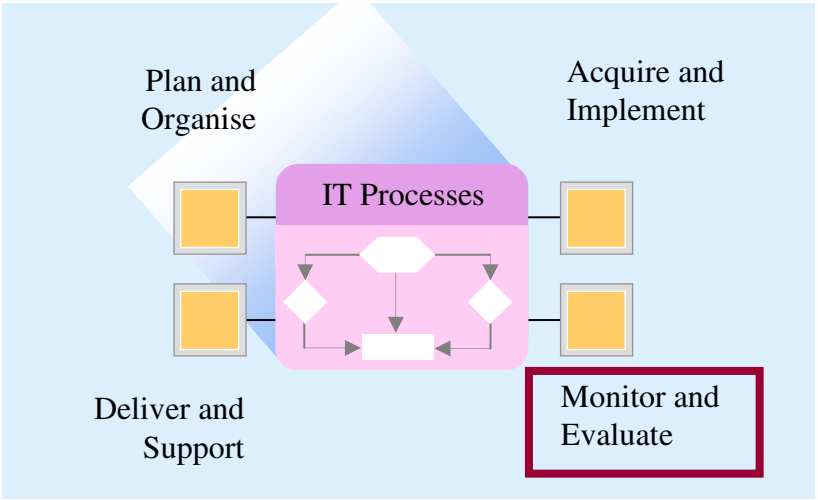


IT Performance

COBIT Cube: Domini IT *(Cont.)*

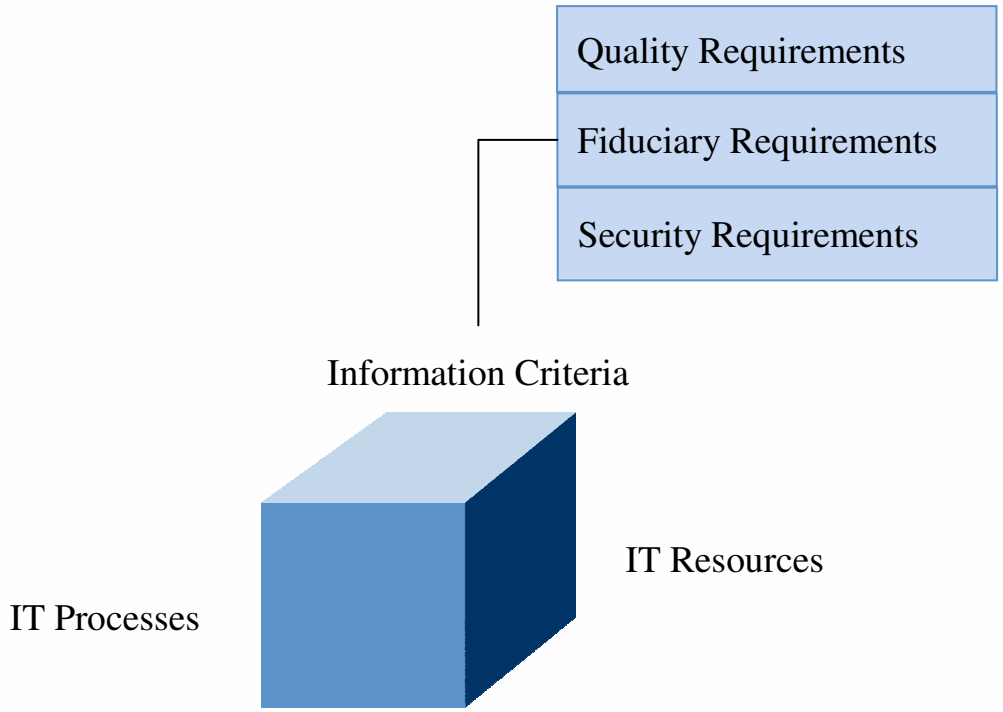
Monitor and Evaluate

ME1 Monitor and evaluate IT performance.
ME2 Monitor and evaluate internal control.
ME3 Ensure compliance with external requirements.
ME4 Provide IT governance.



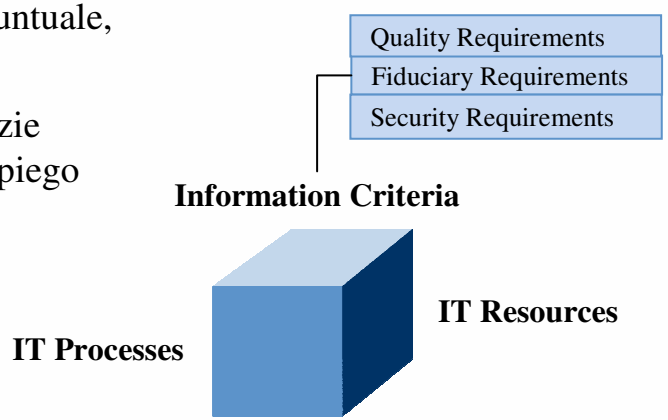
COBIT Cube: Information Criteria

- Per soddisfare gli obiettivi di business, le informazioni hanno bisogno di conformarsi a specifici criteri di controllo, che COBIT definisce requisiti di business per l'informazione
- In generale, gli information criteria sono basati sui seguenti requisiti:
  - Qualità
  - Fiducia
  - Sicurezza



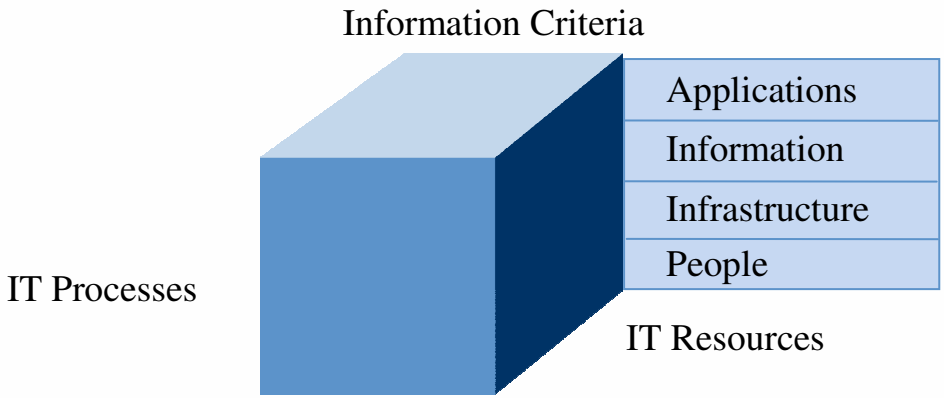
COBIT Cube: Information Criteria *(Cont.)*

Effectiveness	Efficacia - Le informazioni devono essere rilevanti e pertinenti ai processi di business, e devono essere erogate in modo puntuale, corretto, consistente ed utilizzabile
Efficiency	Efficienza - Le informazioni devono essere prodotte grazie all'utilizzo ottimale (il più produttivo ed economico) impiego delle risorse
Confidentiality	Riservatezza - Riguarda la protezione delle informazioni da divulgazione non autorizzata
Integrity	Integrità - Si riferisce all'accuratezza e completezza delle informazioni come anche alla loro validità in accordo ai valori del business ed alle aspettative
Availability	Disponibilità - Le informazioni devono essere disponibili quando richieste dai processi di business. Riguarda inoltre la salvaguardia delle risorse necessarie e delle capacità associate
Compliance	Adeguamento - Si riferisce all'adeguamento a leggi, normative e accordi contrattuali ai quali è assoggettato il processo di business, ad esempio i criteri di business imposti dall'esterno come anche le politiche interne
Reliability	Affidabilità - Riguarda la fornitura di appropriate informazioni che consentono al management di gestire l'entità ed esercitare le proprie responsabilità sulla fiducia e il governo



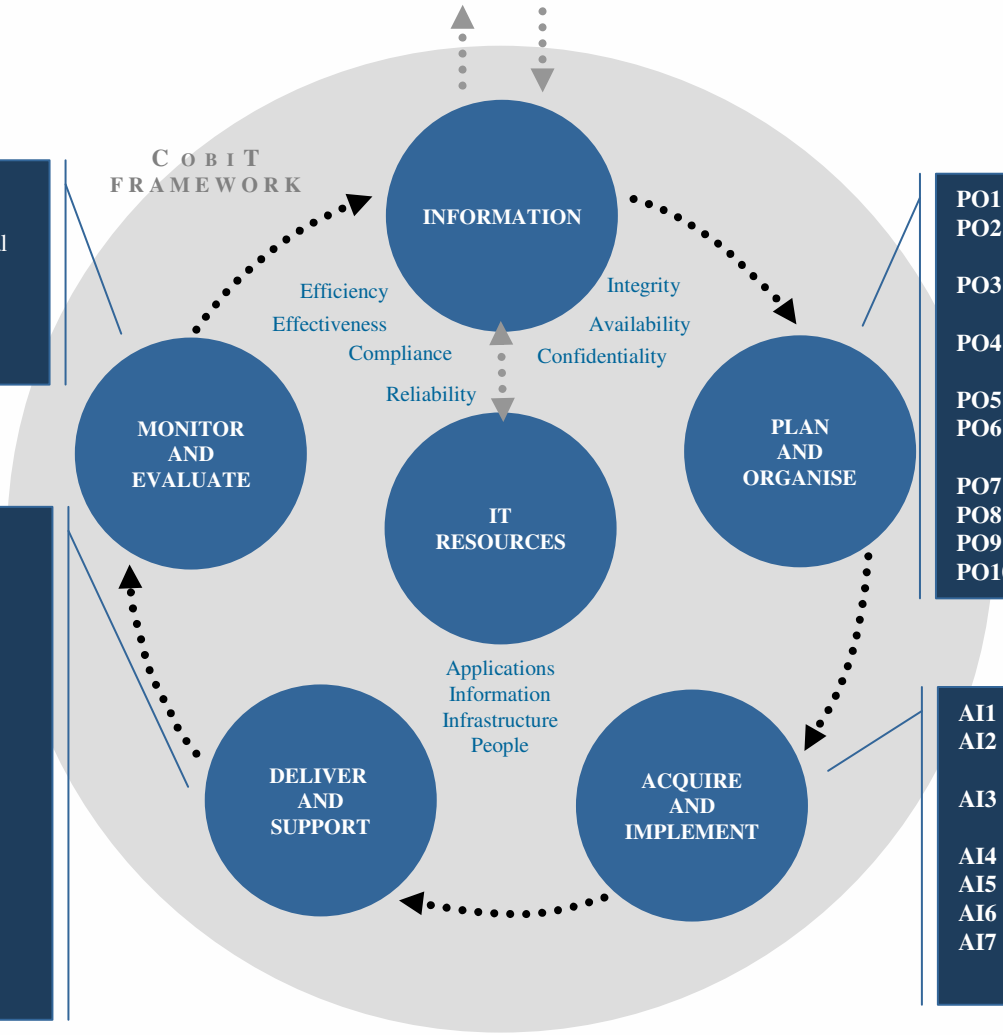
COBIT Cube: Risorse IT

- I processi IT gestiscono le risorse IT per generare, consegnare e conservare le informazioni di cui l'organizzazione ha bisogno per raggiungere i suoi obiettivi.
- Le risorse IT identificate in COBIT sono definite come:
  - **Applicazioni** sono sistemi automatizzati o procedure manuali che elaborano le informazioni.
  - **Informazione** è il dato ricevuto in ingresso, elaborato e prodotto dai sistemi informativi, in qualsiasi formato utilizzato dal business.
  - **Infrastrutture** comprendono le tecnologie e le strutture fisiche, come hardware, sistemi operativi e rete, che consentono l'elaborazione delle applicazioni.
  - **Persone** rappresentano il personale richiesto per pianificare, organizzare, acquisire, implementare, consegnare, supportare, monitorare e valutare i sistemi informativi e i servizi. Possono essere interne, totalmente esterne o a contratto temporaneo, come necessario.



COBIT Framework

OBIETTIVI DI BUSINESS E OBIETTIVI DI GOVERNANCE



ME1 Monitor and evaluate IT performance.
ME2 Monitor and evaluate internal control.
ME3 Ensure compliance with external requirements.
ME4 Provide IT governance.

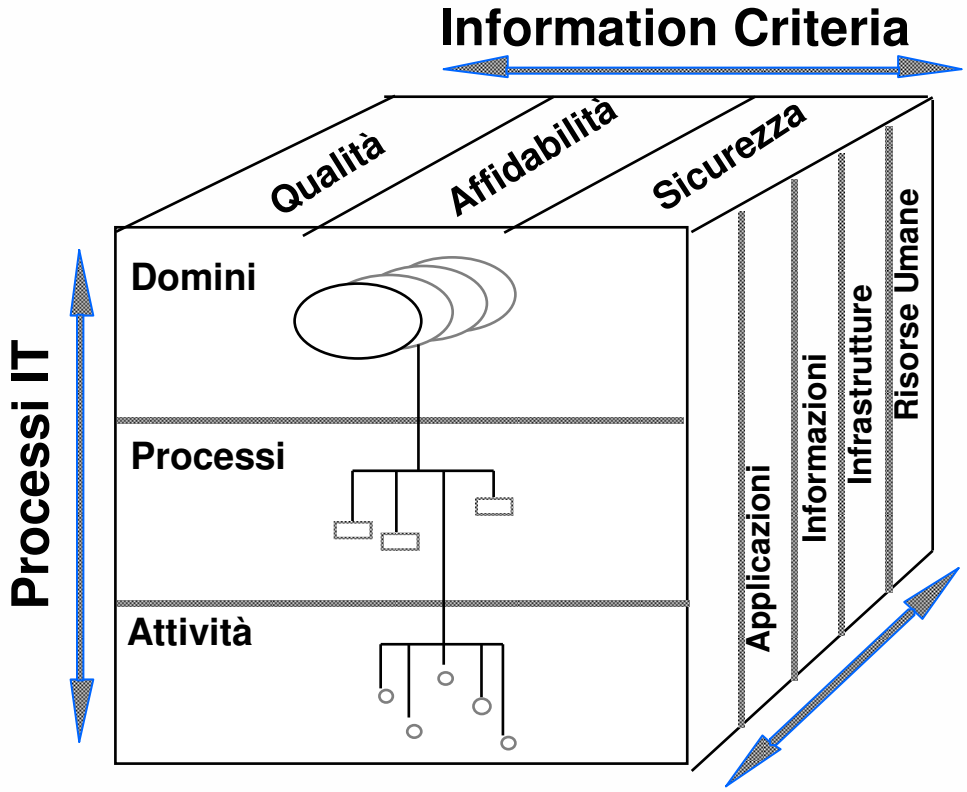
PO1 Define a strategic IT plan.
PO2 Define the information architecture.
PO3 Determine technological direction.
PO4 Define the IT processes, organisation and relationships.
PO5 Manage the IT investment.
PO6 Communicate management aims and direction.
PO7 Manage IT human resources.
PO8 Manage quality.
PO9 Assess and manage IT risks.
PO10 Manage projects.

DS1 Define and manage service levels.
DS2 Manage third-party services.
DS3 Manage performance and capacity.
DS4 Ensure continuous service.
DS5 Ensure systems security.
DS6 Identify and allocate costs.
DS7 Educate and train users.
DS8 Manage service desk and incidents.
DS9 Manage the configuration.
DS10 Manage problems.
DS11 Manage data.
DS12 Manage the physical environment.
DS13 Manage operations.

AI1 Identify automated solutions.
AI2 Acquire and maintain application software.
AI3 Acquire and maintain technology infrastructure.
AI4 Enable operation and use.
AI5 Procure IT resources.
AI6 Manage changes.
AI7 Install and accredit solutions and changes.

COBIT Cube

Le risorse IT sono gestite dai processi IT per raggiungere gli obiettivi IT che rispondono ai requisiti di business. Questo è il principio base del COBIT framework, illustrato dal "COBIT Cube"



Introduzione a CObIT: la famiglia di prodotti

Executive Summary: descrizione generale della metodologia

Framework: descrizione del metodo con la descrizione degli obiettivi di controllo di alto livello

Control Objectives: descrizione dei controlli minimi da adottare, obiettivi di controllo di dettaglio

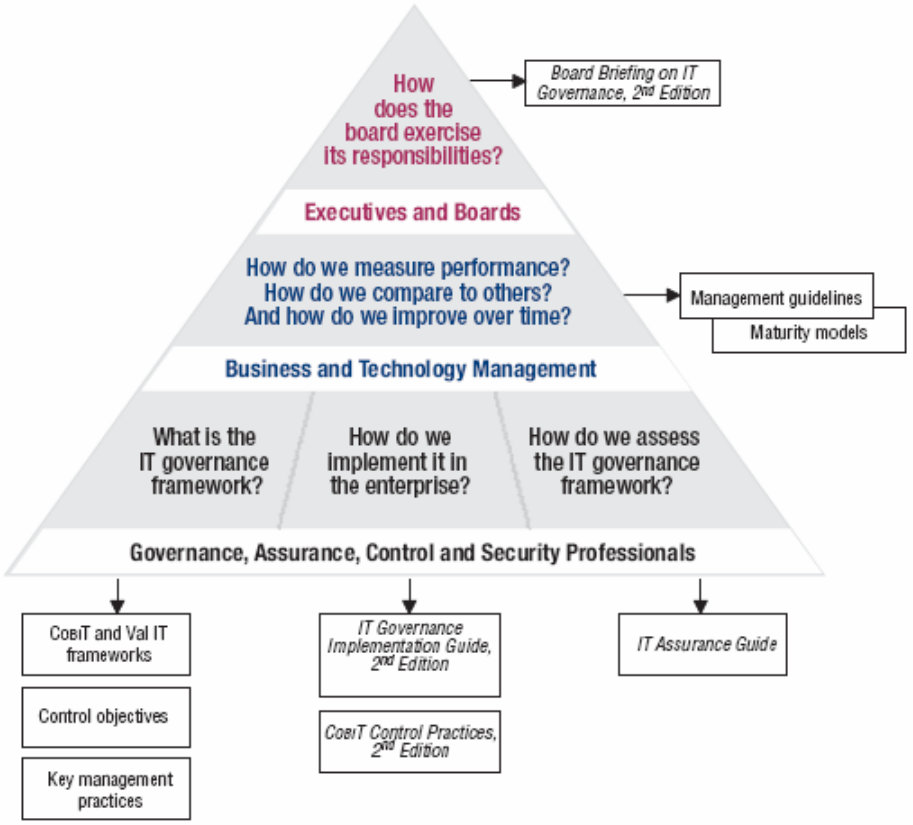
Audit Guidelines: descrizione degli obiettivi di controllo di Audit

Implementation Tool Set: come si utilizza la metodologia CObIT

Management Guide: descrizione degli obiettivi di controllo per il Management

CObIT Security Baseline: elementi per la sicurezza dei sistemi

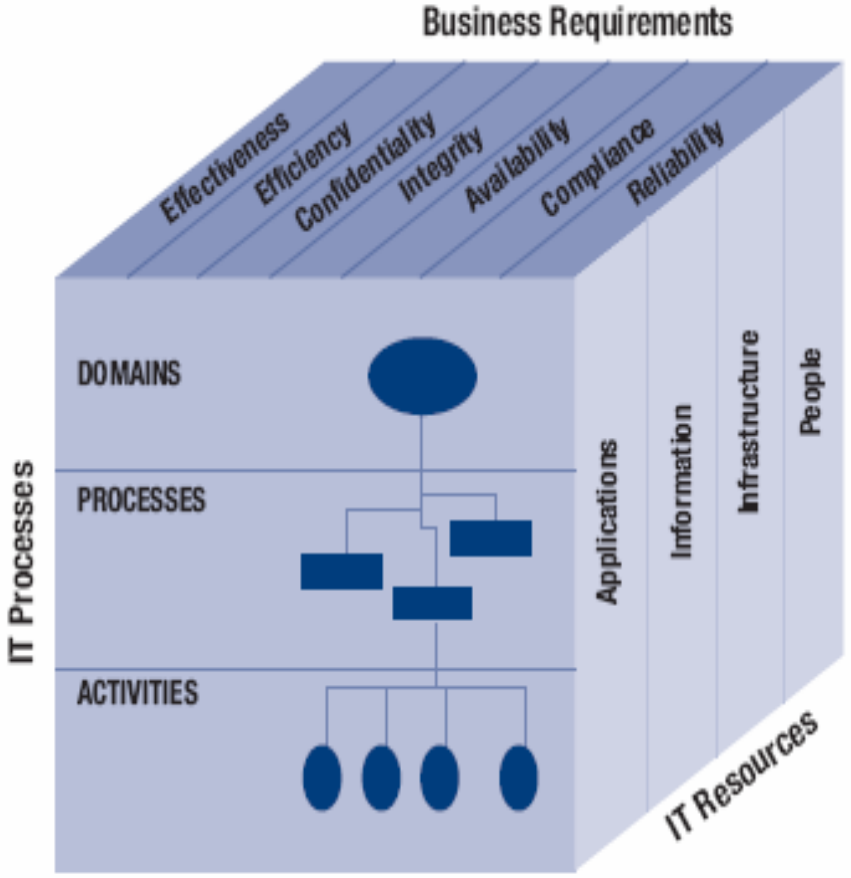
Figure 3—CobiT Content Diagram



This CobiT-based product diagram presents the generally applicable products and their primary audience. There are also derived products for specific purposes (*IT Control Objectives for Sarbanes-Oxley, 2nd Edition*), for domains such as security (CobiT *Security Baseline* and *Information Security Governance: Guidance for Boards of Directors and Executive Management*), or for specific enterprises (CobiT *Quickstart* for small and medium-sized enterprises or for large enterprises wishing to ramp up to a more extensive IT governance implementation).

CObIT: Framerwork

- Promuove la focalizzazione sui processi e la loro proprietà
- Suddivide l'IT in 34 processi facenti capo a 4 macro-aree e fornisce per ciascuno un alto livello di controllo degli obiettivi
- Considera fiducia, qualità e sicurezza bisogni dell'azienda, fornendo 7 criteri informativi che possono essere usati per definire genericamente cosa richiede il business all'IT
- E'supportato da un set di oltre 200 dettagliati obiettivi di controllo



CObIT: Framework

Principi della metodologia: Relazione tra Risorse e Servizi per CObIT:

Le Risorse rese disponibili —e costruite da — IT

Come l' IT è organizzato per rispondere ai requisiti

A quali criteri deve rispondere l'organizzazione delle risorse IT

- Applicazioni
- Informazione
- Infrastrutture
- Persone

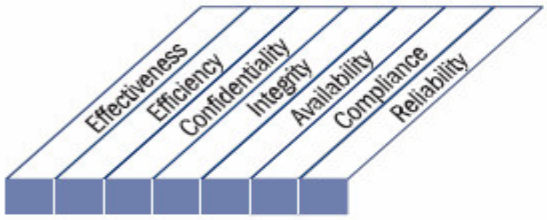
- Pianificazione e Organizzazione
- Acquisizione e Organizzazione
- Erogazione e Supporto
- Monitoraggio e Valutazione

- Efficacia
- Efficienza
- Riservatezza
- Integrità
- Disponibilità
- Adeguamento
- Affidabilità

IL CObIT: Obiettivi di Controllo DI ALTO LIVELLO

Sigla	Processo	Information Criteria							IT Resources			
		effectiveness	efficiency	confidentiality	integrity	availability	compliance	reliability	applications	informations	infrastructure	people
PC	Generic Control requirements											
PO1	Define an IT strategic Plan	P	S						X	X	X	X
PO2	Define the information architecture	S	P	S	P				X	X		
PO3	Determine Technological Direction	P	P						X		X	
PO4	Define the IT processes, organization and relationships	P	P									X
PO5	Manage the IT Investment	P	P					S	X		X	X
PO6	Communicate Management Aims and Direction	P					S			X		X
PO7	Manage IT Human Resources	P	P									X
PO8	Manage Quality	P	P		S			S	X	X	X	X
PO9	Assess and manage IT Risks	S	S	P	P	P	S	S	X	X	X	X
PO10	Manage Projects	P	P						X		X	X

IL COBIT **Aiuto alla navigazione**



Control over the IT process of

process name

that satisfies the business requirement for IT of

summary of most important IT goals

by focusing on

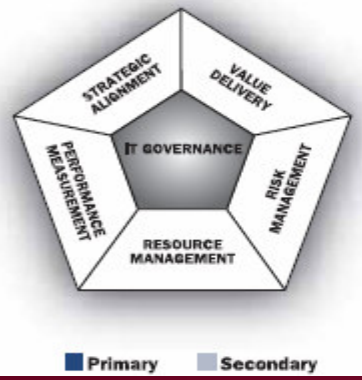
summary of most important process goals

is achieved by

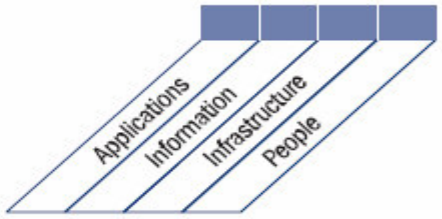
activity goals

and is measured by

key metrics



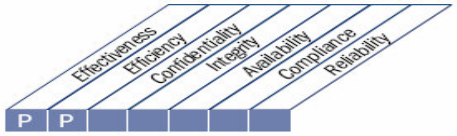
Primary Secondary



IL CObIT: Obiettivi di Controllo DI ALTO LIVELLO

P03 Determine Technological Direction

The information services function determines the technology direction to support the business. This requires the creation of a technological infrastructure plan and an architecture board that sets and manages clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms. The plan is regularly updated and encompasses aspects such as systems architecture, technological direction, acquisition plans, standards, migration strategies and contingency. This enables timely responses to changes in the competitive environment, economies of scale for information systems staffing and investments, as well as improved interoperability of platforms and applications.



Control over the IT process of

Determine technological direction

that satisfies the business requirement for IT of

having stable, cost-effective, integrated and standard application systems, resources and capabilities that meet current and future business requirements

by focusing on

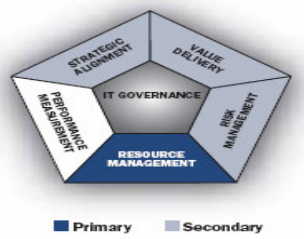
defining and implementing a technology infrastructure plan, architecture and standards that recognise and leverage technology opportunities

is achieved by

- Establishing a forum to guide architecture and verify compliance
- Establishing the technology infrastructure plan balanced against cost, risk and requirements
- Defining the technology infrastructure standards based on information architecture requirements

and is measured by

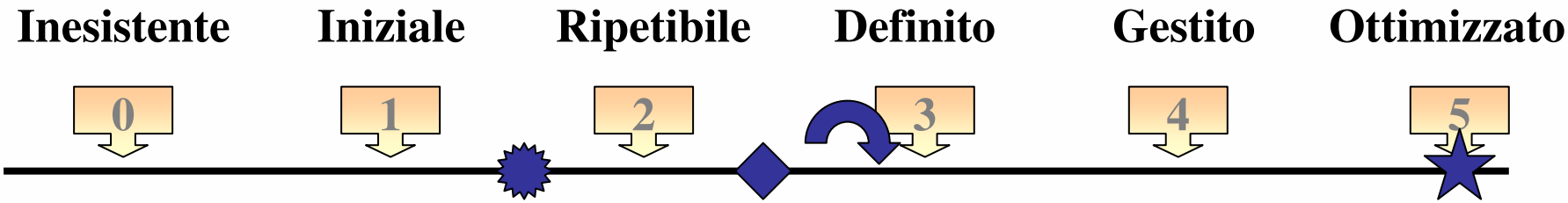
- Number and type of deviations from the technology infrastructure plan
- Frequency of the technology infrastructure plan review/update
- Number of technology platforms by function across the enterprise



CObIT: Linee guida per il Management

Modello di Maturità:

Il controllo dei processi IT si basa sullo sviluppo di un metodo a punteggi con il quale l'azienda può valutare il livello del processo e/o dell'azienda, è derivato dal modello SEI Software Engineering Institute.

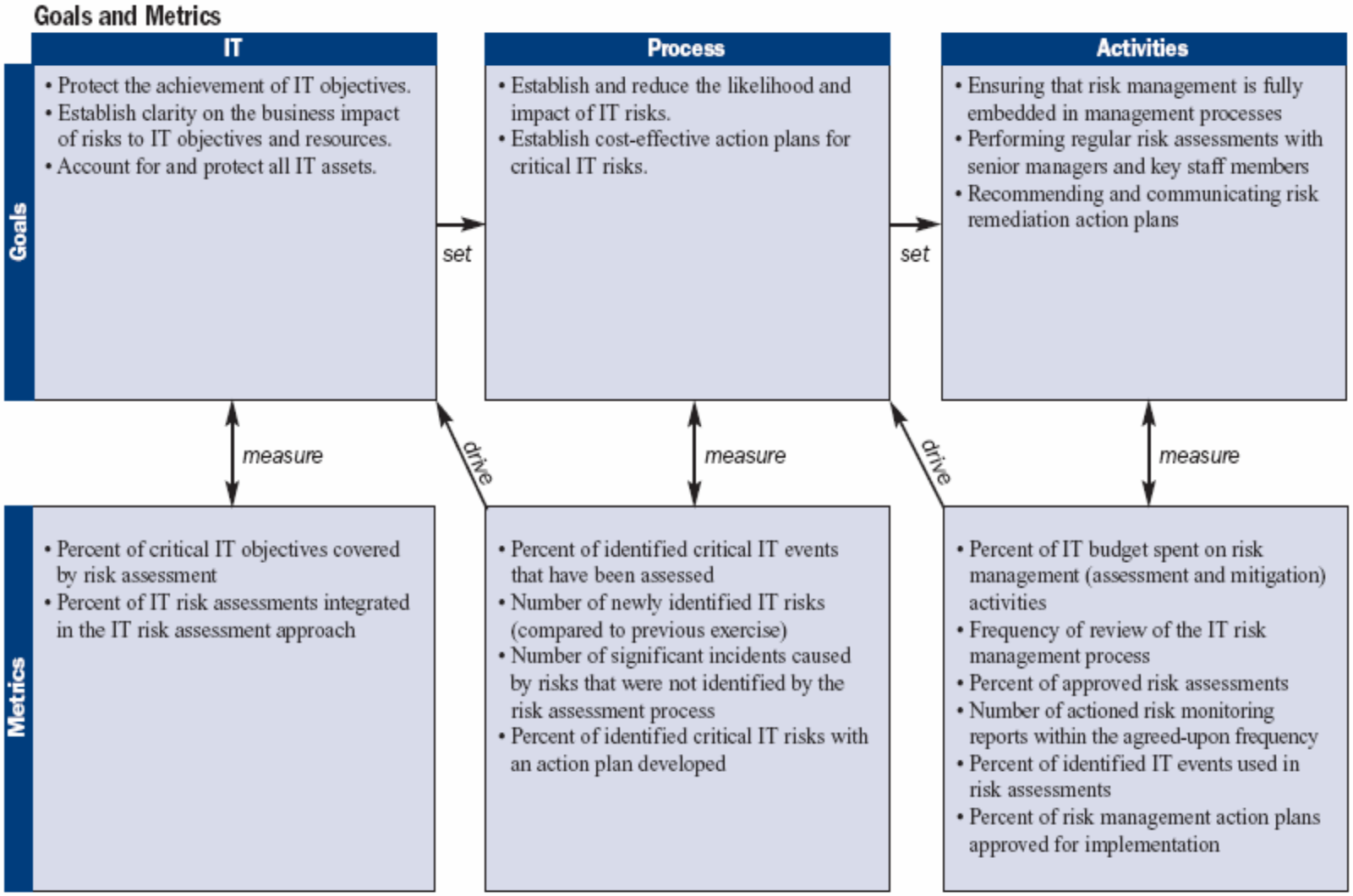


Legend for Symbols Used

- **Enterprise current status**
- **International standard guidelines**
- **Industry best practice**
- **Enterprise strategy**

0. Inesistente – nessun processo riconoscibile – questione non nota
1. Iniziale – questione nota, nessun approccio riconoscibile – approccio caso per caso
2. Ripetibile – attività svolte di norma allo stesso modo anche da persone diverse
3. Definito – processo documentato e comunicato
4. Gestito – elementi di misurazione e contromisure in caso di scostamenti o inefficacia
5. Ottimizzato – applicazione delle migliori pratiche di interventi di ottimizzazione

COBIT: Linee guida per il Management



COBIT Implementazione

Figure 15—COBIT's Audiences

When you are...	→ COBIT can serve the following objectives for you...	→ Some specific approaches for the use of COBIT that may prove useful to you...
Board and executive	→ Mandate and promote COBIT's IT governance model for all entities within the enterprise	→ To complement existing internal control frameworks (e.g., COSO) for IT-specific matters → To establish a common language and clear responsibilities amongst business, IT and audit → To self-assess against the generally accepted COBIT standards and take actions as warranted to improve IT
Business management	→ Establish a common enterprisewide control model to manage and monitor IT's contribution to the business	→ As a code of good practices for dealing with IT in the business function → As a code of good practices for addressing application controls in business processes → To determine the different aspects that need to be covered by the service level agreement (SLA) agreed upon with the IT function (whether internally or outsourced)
IT management	→ Structure the IT services function into manageable and controllable processes focusing on the business contribution → Assess and improve IT processes to enhance delivery to the business	→ As the baseline model to establish the appropriate level of generally accepted control objectives as well as for external certifications (e.g., ISO 17799, ISO 20000, SysTrust™ and SAS 70) → As the basis for the process-related performance measures → As the basis for IT-related policies and norms → To help avoid or mitigate risk → To establish SLAs and communicate with business functions
IT audit	→ Serve as the basis for determining the IT audit universe and as the IT control reference	→ As criteria for review and examination and for scoping IT-related audits → As the starting point for developing an audit programme → To help link business drivers to the audit process → To provide assurance and control over IT → To provide assurance and control over the IT performance management system
Risk and compliance	→ Serve as the basis for advising on IT compliance and timely risk mitigation	→ As criteria for the risk/compliance assessment and for framing IT-related assessments → To ensure that IT complies with policy, laws and regulations → To ensure that new risks are identified in a timely manner

COBIT Security Baseline

Figure 1—*COBIT Security Baseline* Structure