COBIT introduzione

(Control Objectives for Information and Related Technology).

Antonello Giuliani
CISA
Antonello.giuliani@capgemini.com

Obiettivo per il 2005

Seguire un percorso sulla metodologie COBIT, come spirito del capitolo e come obiettivo degli Auditor, per il 2005.

Come implementare, praticamente , la metodologia COBIT nelle sue estensioni e ambiti di applicabilità:

Il Governo dell'IT e i suoi obiettivi di controllo,

l'applicabilità da parte degli Auditor della metodologia,

L'applicabilità della metodologia con le pratiche di Sicurezza,

La Presentazione

La presentazione è di carattere generale e introduttivo al COBIT, gli argomenti trattati verranno approfonditi nelle prossime sessioni del COBIT

COBIT

Agenda:

- Introduzione al COBIT:
  - Cos'è il COBIT,
  - La missione del COBIT,
  - Organizzazione del COBIT,
- Il COBIT :
  - Introduzione al governo dell'IT "IT Governance",
  - Introduzione ai controlli dell' IT "IT Control Framerwork"
  - Introduzione COBIT Linee guida del Management
  - Introduzione COBIT Linee guida di Audit

Generalità

Le Aziende debbono assicurare che il proprio patrimonio informativo, come tutti i beni dell'azienda, soddisfi i requisiti di :

- **Qualità**
- **Affidabilità**
- **Sicurezza,**

il management deve ottimizzare le risorse disponibili come :

- **Dati,**
- **Sistemi Applicativi,**
- **La Tecnologia,**
- **Personale,**

Per perseguire gli obiettivi aziendali il management deve :

- **Conoscere i propri sistemi,**
- **Decidere il grado di sicurezza e di controllo,**

Introduzione al COBIT : cos'è il COBIT

Il COBIT (Control Objectives for Information and related Technology), è un framerwork sviluppato da ISACA, e da IT Governance Istitute con la collaborazione degli sponsor, per dare un aiuto alle organizzazioni nel gestire i rischi dell'IT e assicurare, inoltre , che i processi IT siano coerenti con gli obiettivi di Business dell'azienda.

Per molte aziende, le informazioni e la tecnologia che utilizzano per gestirle rappresenta il patrimonio dell'azienda e la vita della stessa, la continua crescita della dipendenza delle aziende alle informazioni e ai relativi sistemi che le gestiscono porta ad avere :

- Aumento delle vulnerabilità,
- Aumento del volume degli investimenti,
- Continua trasformazione delle organizzazioni e di conseguenza, necessità di ridurre i Costi,

Introduzione al COBIT : la missione del COBIT

La missione del COBIT è quella di pubblicare promuovere e autorizzare le prassi , generalmente accettate, rendendo pubblico un set di obiettivi di controllo accettati a livello internazionale per il controllo e governo l'IT, il COBIT non'è solo progettato per gli Utenti e gli Auditor ma principalmente per il Management , il COBIT vuole essere una guida per i manager ed i responsabili dei processi aziendali al governo dell'IT. Al fine di fornire le corrette informazioni di cui una azienda ha bisogno, sempre considerando gli obiettivi di Business.

La visione del COBIT è essere un modello per il governo dell'IT.

Introduzione al COBIT : Obiettivo e Ambito del COBIT

L'obiettivo e ambito del COBIT è:

Standard e Good Practice generalmente accettati per il controllo delle informazioni e dell'IT,

Framework per il controllo dell'IT,

Orientato principalmente al Management dell'IT nonché agli Utenti e agli Auditor,

Basato sul Standard, Practice e metodologie : OECD, ISACA, ITSEC, TCSEC, ISO900, TickIT, Common Criteria, COSO, IFAC, AICPA, GAO, ISO 17799,

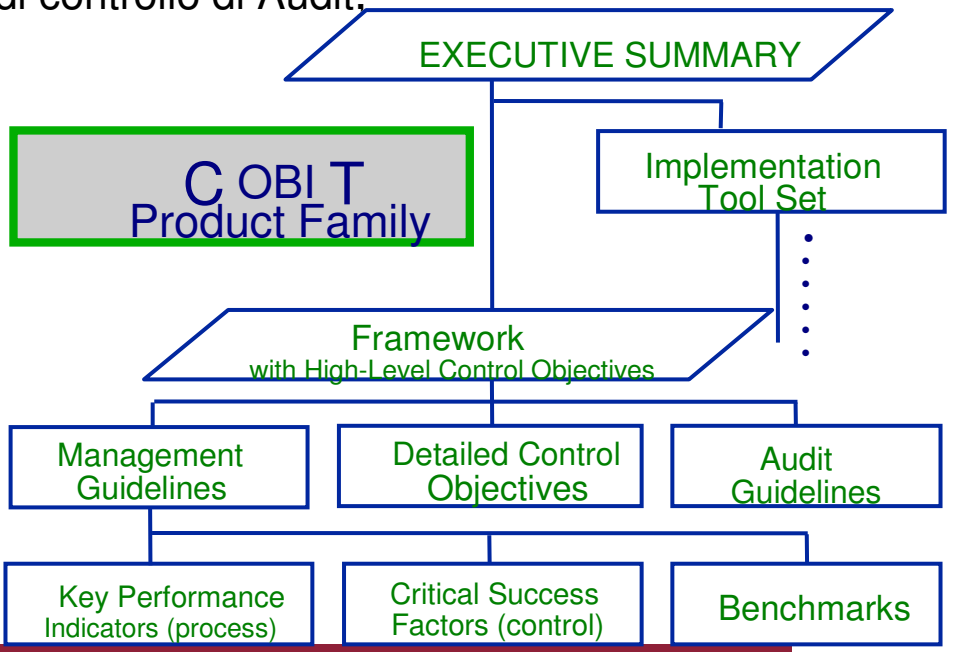
Introduzione al COBIT : Organizzazione del COBIT

Executive Summary: descrizione generale della metodologia,

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

Contol Objectives: descrizione dei controlli minimi da adottare, Obiettivi di controllo di dettaglio,

Audit Guidelines: descrizione degli obiettivi di controllo di Audit.

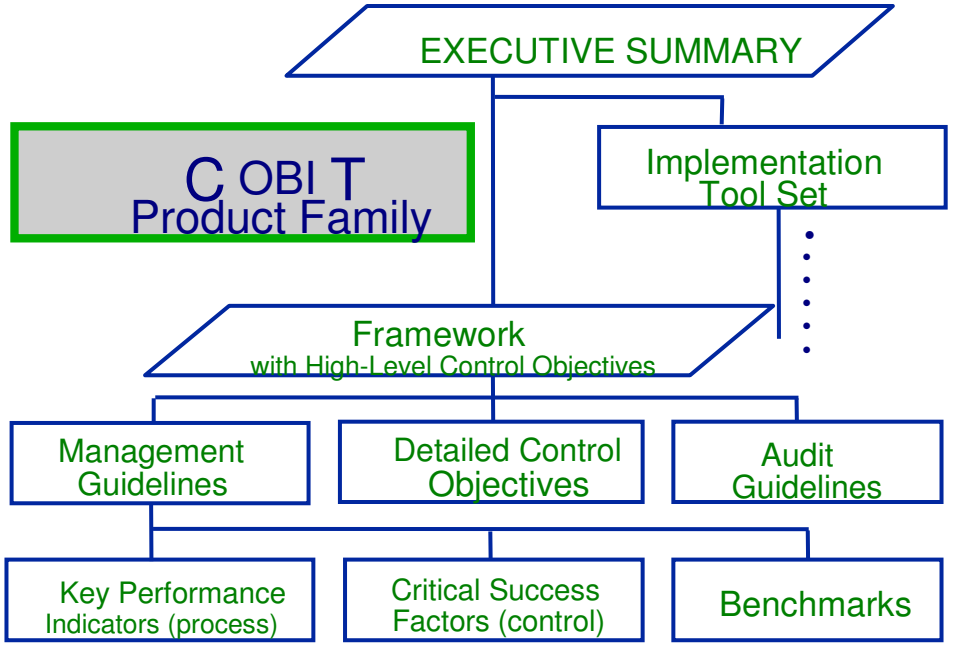


Introduzione al COBIT : Organizzazione del COBIT

Implementation Tool Set: come si utilizza la metodologia COBIT,

Management Guide: descrizione degli obiettivi di controllo per il Management

Cobit Security Baseline



IL COBIT : Il governo dell'IT "IT Governance"

Definizione del Governo dell'IT per il COBIT.

Una struttura di relazioni e di processi per dirigere e controllare l'azienda al fine di raggiungere gli scopi della stessa apportando valore e bilanciando Rischi e Benefici dell'IT e dei suoi processi.

COBIT è un quadro di riferimento generale rivolto ai responsabili IT.

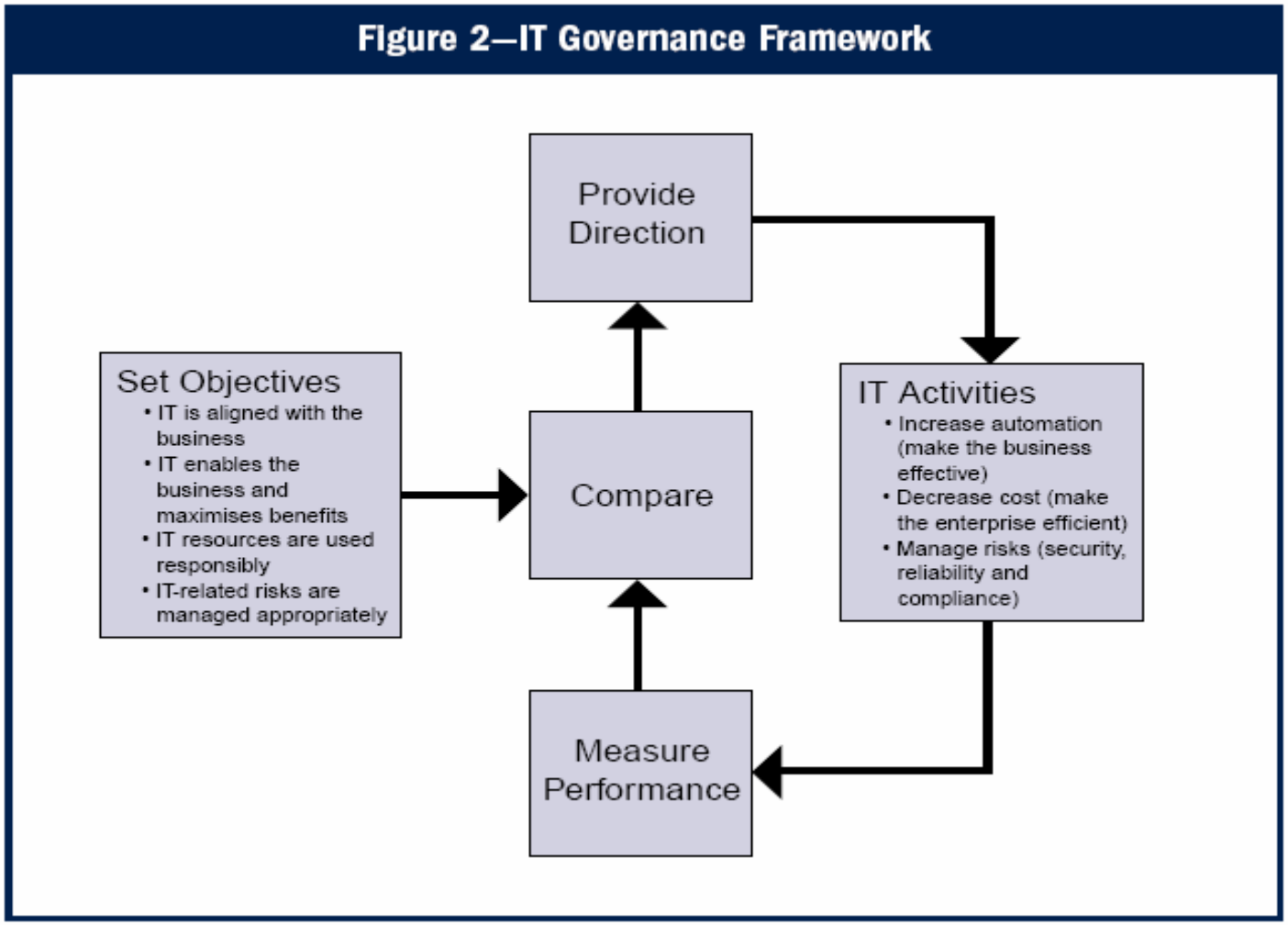
IL COBIT : Il governo dell'IT "IT Governance"

L'IT e strategico per il Business, aumentano le dipendenze con le informazioni e i sistemi, oggi la competitività passa per l'IT,

IT coinvolge grandi investimenti e grandi rischi, la tecnologia evolve in continuazione e cambia le organizzazioni e le pratiche di Business, creando nuove opportunità riducendo i costi, la Tecnologia molto velocemente diventa inadeguata,

Nella gestione e Governo dell'IT è necessario l'utilizzo di una Metodologia un "Framerwork" che governi l'IT per raggiungere gli obbiettivi di Business, il COBIT è la metodologia adeguata.

IL COBIT : Il governo dell'IT "IT Governance"



IL COBIT : Il governo dell'IT "IT Governance".

- Responsabilità del Management dell'IT:
  - Salvaguardare gli Asset,
  - Valutare gli Asset e le informazioni dell'IT
  - Gestire e mitigare il Rischio.

Il Management necessita del COBIT per:

- Valutare gli investimenti sull'IT,
- Bilanciare i Rischi e i controlli sugli investimenti,
- Eseguire dei Benchmark sull'IT esistente e futuro.

IL COBIT: Definizioni

Controllo: politiche, procedure, prassi, le strutture organizzative che forniscono garanzia degli obbiettivi aziendali, (Rif. COSO),

Obiettivo di controllo nell'IT: declaratoria del risultato atteso o dell'obiettivo atteso, l'implementazione di una procedura di controllo in una particolare attività IT.

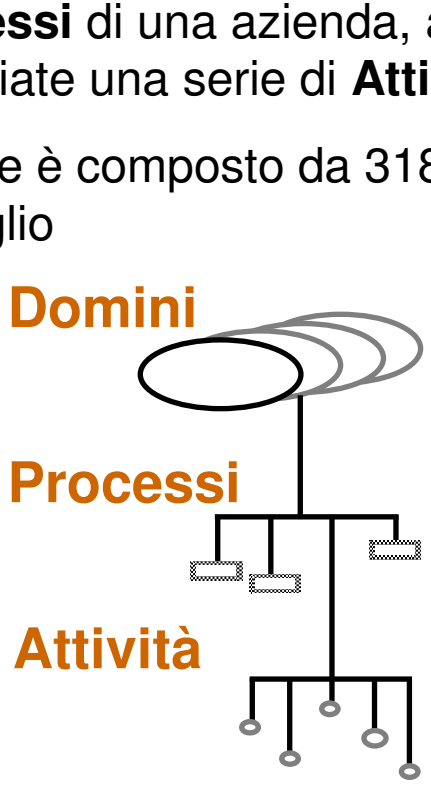
Governo dell'IT: una struttura di relazioni e di processi per dirigere e controllare l'azienda al fine di raggiungere gli scopi della stessa apportando valore e benefici all'IT e ai suoi processi.

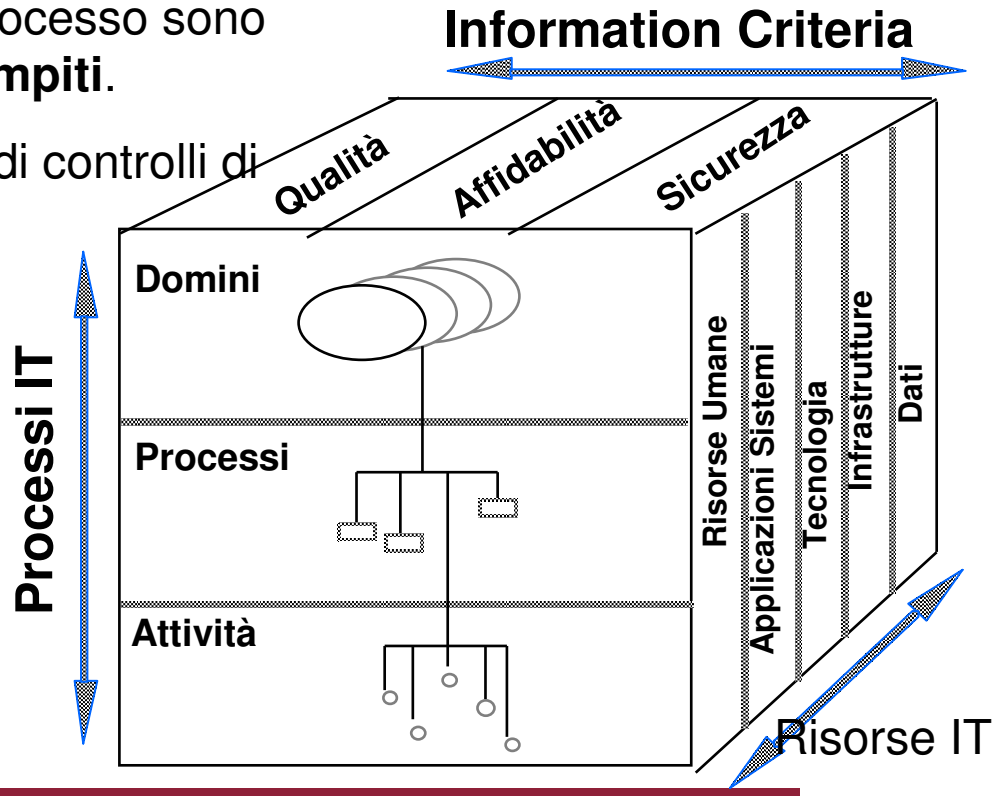
IL COBIT: il Framerwork

Principi della metodologia: il COBIT consiste di:

34 Obiettivi di Controllo di alto livello, di una loro classificazione composta da 4 **Domini**, da 34 Obiettivi di controllo che normalmente sono visti come di **Processi** di una azienda, ad ogni processo sono associate una serie di **Attività e Compiti**.

•Inoltre è composto da 318 obiettivi di controlli di dettaglio





IL COBIT: il Framerwork

Principi della metodologia: I domini del COBIT consistono di:

Pianificazione & Organizzazione: Questo Dominio copre la Strategia e la Tattica, riguarda come l'IT può meglio identificare il modo con cui contribuire al raggiungimento degli obbiettivi aziendali, realizzare una visione strategica con la pianificazione da parte del management, che deve comunicare e gestire,

•**Acquisizione e Realizzazione**: per poter realizzare una strategia è necessario individuare delle soluzioni, da **Sviluppare** o **Acquisire**, **gestione delle modifiche** e loro **manutenzione,**

•**Erogazione e Assistenza:** Erogazione Servizi Richiesti, operazioni tradizionali " Sistemistiche", alla Sicurezza e continuità del servizio, elaborazione di dati, e controlli delle applicazioni,

•**Monitoraggio**: Tutti i processi devono essere valutati nel tempo, sotto l'aspetto qualità e conformità ai requisiti di controllo, il management deve eseguire la supervisione dei processi di controllo, compresa la valutazione indipendente fornita dall'Audit sia interno che Esterno,

IL COBIT: il Framerwork

Principi della metodologia: Definizioni assunte dal COBIT.

- Efficacia: Le informazioni debbono essere rilevanti e pertinentiai processi aziendali,
- Efficienza: Riguarda l'uso ottimale delle risorse, (Prodittività e economicità),
- Riservatezza: La protezione delle informazioni da accessi non autorizzati,
- Integrità: Riguarda la Accurattezza e Completezza delle informazioni,
- Disponibilità: L'informazione deve essere disponibile quando richiesto dai processi aziendali,
- Conformità: Rispetto di leggi e regolamenti, accordi contrattuali, cui è soggetta l'azienda,
- Affidabilità: Riguarda la fornitura di appropriate informazioni alla Direzione, per far fronte alle proprie responsabilità e a obblighi di bilancio,

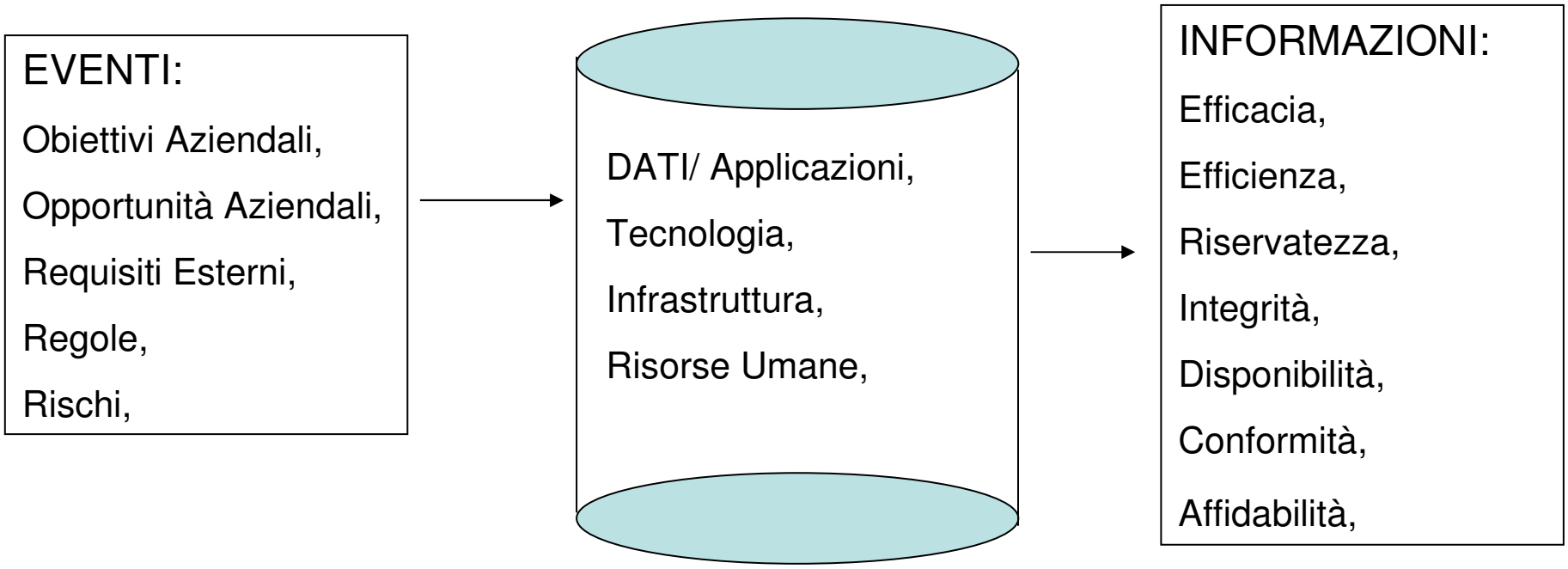
IL COBIT: il Framerwork

Principi della metodologia: le risorse individuate dal COBIT:

•**DATI**: Sono gli oggetti delle più ampia accezione strutturati e non, grafici, multimediali,
•**Applicazion**i: Sistemi comprensivi di procedure Manuali e Automatiche,
•**Tecnologia**: Hardware, Sistemi Operativi, database, management system, networking, multimedia,
•**Infrastrutture**: Risorse destinate ad ospitare e garantire il funzionamento dei sistemi informatici,
•**Risorse Umane**: Conoscenze, professionalità e produttività per pianificare organizzare, acquisire, erogare, gestire e governare il sistema informativo ed i servizi relativi.

IL COBIT: il Framerwork

Principi della metodologia: Relazione tra Risorse e Servizi per il COBIT:



IL COBIT: Obiettivi di Controllo DI ALTO LIVELLO

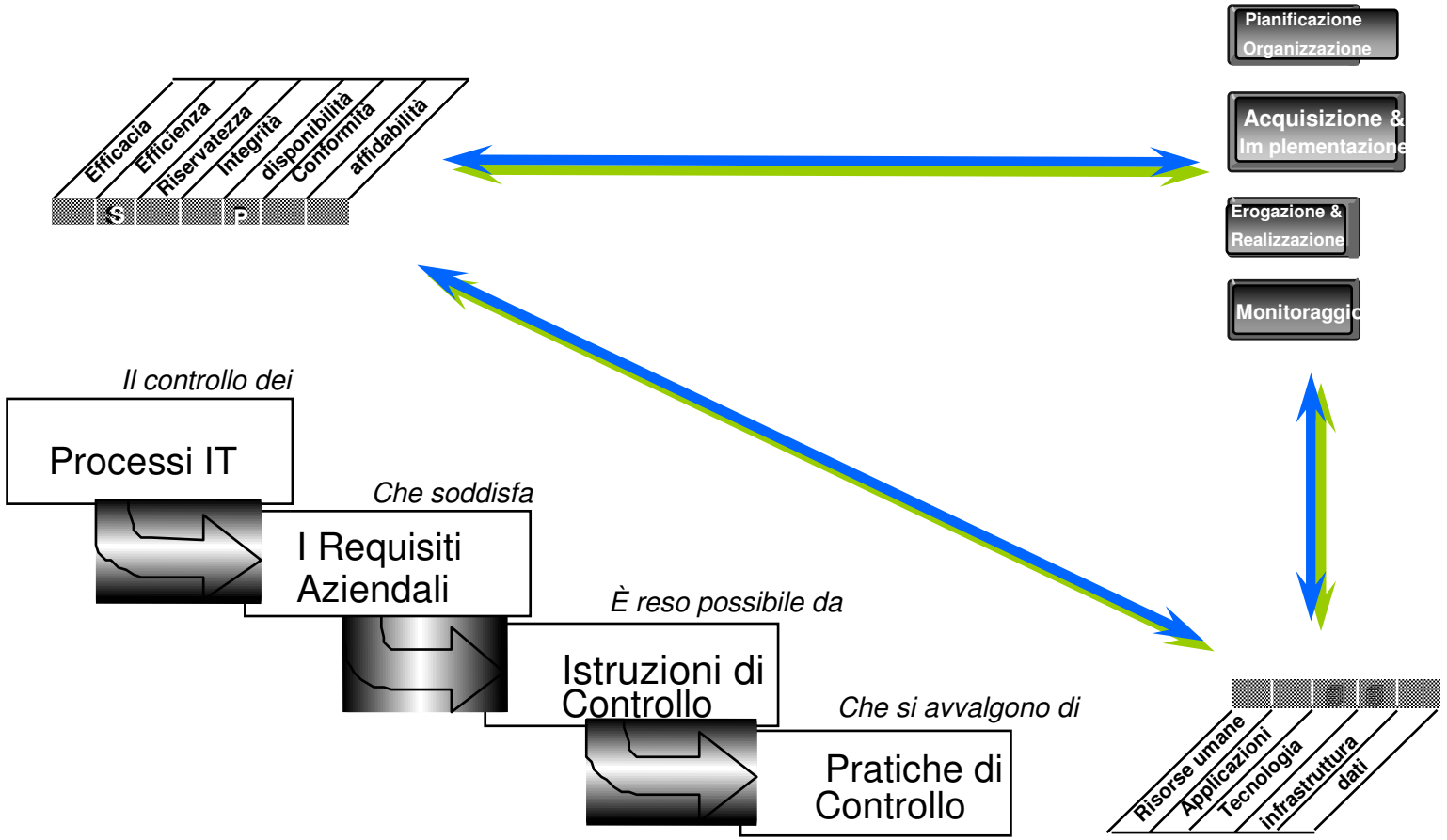
Aggiornamento al 21-1-2005 V 10			Criteri dell'Informazione								Risorse IT				
DOMINI	Cod.	Processi	Efficacia	Efficienza	Riservatezza	Integrità	Disponibilità	Conformità	Affidabilità		Risorse Umane	Applicazioni	Tecnologia	Infrastruttura	Dati
Pianificazione & Organizzazione															
	PO1	Definire il Piano Strategico per l'IT	P	S							V	V	V	V	V
	PO2	Definire l'Architettura dei DATI	P	S	S	S						S			S
	PO3	Valutare i Rischi	P	S									V	V	
	PO4	Definire l'Organizzazione e le relazioni IT	P	S							V				
	PO5	Gestire gli Investimenti in IT	P	P					S		V	V	V	V	
	PO6	Comunicare obiettivi e indirizzi della Direzione	P								V				
	PO7	Gestire le Risorse Umane	P	P							V				
	PO8	Assicurare la conformità ai requisiti Esterni	P					P	S		V	V			
	PO9	Valutare i Rischi	S	S	P	P	P	S	S		V	V	V	V	V
	PO10	Gestire i Progetti	P	P							V	V	V	V	
	PO11	Gestire La Qualità	P	P		P		S			V	V	V	V	
Acquisizione & Realizzazione															
	AI1	Identificare soluzioni automatizzate	P	S								V	V	V	
	AI2	Acquistare il software applicativo	P	P		S		S	S			V			
	AI3	Acquistare e mantenere l'infrastruttura tecnologica	P	P		S							V		
	AI4	Sviluppare e Mantenere le Applicazioni	P	P		S		S	S		V	V	V	V	
	AI5	Installare e Certificare i Sistemi	P	P		S	S				V	V	V	V	V
	AI6	Gestire le Modifiche	P	P		P	P		S		V	V	V	V	V

IL COBIT: Obiettivi di Controllo DI ALTO LIVELLO

Aggiornamento al 21-1-2005 V 10			Criteri dell'Informazione								Risorse IT				
DOMINI	Cod.	Processi	Efficacia	Efficienza	Riservatezza	Integrità	Disponibilità	Conformità	Affidabilità		Risorse Umane	Applicazioni	Tecnologia	Infrastruttura	Dati
Erogazione & Assistenza															
	DS1	Definire e gestire i livelli di Servizio	P	P	S	S	S	S	S		V	V	V	V	V
	DS2	Gestire e Servizi di Terze Parti	P	P	S	S	S	S	S		V	V	V	V	V
	DS3	Gestire le prestazioni e la Capacità produttiva	P	P			S					V	V	V	
	DS4	Assicurare la continuità dei Servizi	P	S			P				V	V	V	V	V
	DS5	Garantire la sicurezza dei sistemi			P	P	S	S	S		V	V	V	V	V
	DS6	Identificare e attribuire i costi		P					P		V	V	V	V	V
	DS7	Formare e addestrare gli utenti	P	S							V				
	DS8	Assistere e dare consulenza agli utenti	P	P							V	V			
	DS9	Gestire la Configurazione	P				S		S			V	V	V	
	DS10	Gestire i problemi e gli incidenti	P	P			S				V	V	V	V	V
	DS11	Gestire i Dati				P			P						V
	DS12	Gestire le Infrastrutture				P	P							V	
	DS13	Gestire L'Esercizio	P	P		S	S				V	V		V	V
Monitoraggio															
	M1	Monitorare i Processi	P	P	S	S	S	S	S		V	V	V	V	V
	M2	Valutare l'adeguatezza del Controllo Interno	P	P	S	S	S	P	S		V	V	V	V	V
	M3	Ottenere certificazioni indipendenti	P	P	S	S	S	P	S		V	V	V	V	V
	M4	Condurre indagini di Audit indipendenti	P	P	S	S	S	P	S		V	V	V	V	V

IL COBIT

Aiuto alla navigazione



IL COBIT: Obiettivi di Controllo DI ALTO LIVELLO

PO1 Planning & Organisation
Define a Strategic Information Technology Plan

COBIT

HIGH-LEVEL CONTROL OBJECTIVE

Control over the IT process of

defining a strategic IT plan

that satisfies the business requirement

to strike an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment

is enabled by

a strategic planning process undertaken at regular intervals giving rise to long-term plans; the long-term plans should periodically be translated into operational plans setting clear and concrete short-term goals

and takes into consideration

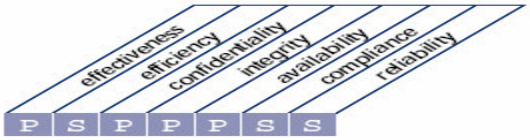
- enterprise business strategy
- definition of how IT supports the business objectives
- inventory of technological solutions and current infrastructure
- monitoring the technology markets
- timely feasibility studies and reality checks
- existing systems assessments
- enterprise position on risk, time-to-market, quality
- need for senior management buy-in, support and critical review

IL COBIT: Obiettivi di Controllo DI ALTO LIVELLO

PO9 Planning & Organisation
Assess Risks

COBIT

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

assessing risks

that satisfies the business requirement

of supporting management decisions through achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors

is enabled by

the organisation engaging itself in IT risk-identification and impact analysis, involving multi-disciplinary functions and taking cost-effective measures to mitigate risks

and takes into consideration

- risk management ownership and accountability
- different kinds of IT risks (technology, security, continuity, regulatory, etc.)
- defined and communicated risk tolerance profile
- root cause analyses and risk brainstorming sessions
- quantitative and/or qualitative risk measurement
- risk assessment methodology
- risk action plan
- timely reassessment

Linee Guida per il Management

introduzione

COBIT(Control Objectives for Information and Related Technology).

IL COBIT: Linee guida per il Management

Quadro di riferimento:

Il documento è rivolto al management dell'azieda ai Top Manager, costituito da :

•Modelli di Maturità,

•Fattori Critrici di Successo (CSF),

•Indicatori Chiave di Obiettivo (KGI),

•Indicatori chiave di Prestazione (KPI),

Tutto questo fornisce un quadro di riferimento per i responsabili per poter controllare e misurare l'IT

IL 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.

IL COBIT: Linee guida per il Management

Fattori Critici di Successo CSF: definiscono gli elementi o le azioni più importanti per i responsabili per controllare i processi IT, sia essi dall'esterno che dall'interno, devono essere costituite da Linee Guida orientate alla gestione del processo, devono indicare le azioni da eseguire "Procedure",

Le linee guida sono le attività che perseguono la strategia aziendale, la strategia Tecnica/Organizzativa, devono essere sintetiche con riferimento alla risorse.

Fattori Critici di Successo deve definire:

- Processi definiti e documentati,
- Politiche definite e documentate,
- Chiare competenze,
- Forte supporto "Impegno" dei dei responsabili,
- Idonea comunicazione,
- Coerenti pratiche di misurazione

IL COBIT: Linee guida per il Management

Indicatori Chiave di Obiettivo (KGI): definiscono le misure per indicare ai responsabili se un processo IT ha soddisfatto i requisiti aziendali, espressi in termini di criteri informatici:

- Disponibilità,
- Integrità e Riservatezza, (abbattimento dei rischi),
- Efficienza economica dei processi e delle operazioni,
- Conferma dei criteri di affidabilità, efficacia, e conformità,

Un indicatore Chiave di Obiettivo rappresenta l'obiettivo del processo, deve misurare cosa deve essere compiuto, deve essere misurabile per raggiungere l'obiettivo.

Gli Indicatori Chiave di Obiettivo sono indicatori "a posteriori", poiché loro misurano solo dopo il fatto, danno indicazione che l'informatica e la tecnologia stanno o meno contribuendo alla strategia dell'impresa.

IL COBIT: Linee guida per il Management

Indicatori Chiave di Obiettivo (KGI), generici indicatori:

- Migliorata gestione delle prestazioni,
- Riduzione dei Rischi dell'IT,
- Aumento della produttività,
- Integrazione delle catene di fornitura,
- Processi Standardizzati,
- Spinta all'Erogazione dei Servizi(Vendite),
- Raggiungimento di nuovi clienti e soddisfazione dei preesistenti,
- Creazione di nuovi canali per l'Erogazione dei servizi,
- Disponibilità di larghezza di Banda, potenza elaborativa ed meccanismi di erogazione dell'IT,
- Rispetto dei Requisiti della clientela e del Badget
- Numero di clienti e costo per cliente Servizio,
- Aderenza agli Standard

IL COBIT: Linee guida per il Management

Indicatori Chiave di Prestazioni (KPI):

Gli Indicatori Chiave di Prestazione sono misure che indicano ai responsabili che il processo IT sta raggiungendo i suoi obiettivi aziendali, è un controllo “a priori”, è un controllo che misura le prestazioni dei fattori abilitanti dei processi IT, indica quanto bene il processo contribuisce al raggiungimento dello scopo.

Gli Indicatori Chiave di Prestazione spesso sono una misura per i Fattori Critici di Successo.

IL COBIT: Linee guida per il Management

Indicatori Chiave di Prestazioni (KPI) insieme di generici indicatori:

- Tempi ridotti di elaborazione,
- Accresciuta qualità e innovazione,
- Utilizzo delle risorse a larga banda e della potenza elaborativa,
- Disponibilità del servizio e tempi di risposta,
- Soddisfazione dei “Stakeholder” (statistiche e numero di reclami),
- Numero di addetti e addestrati nelle nuove tecnologie e competenze nel servizio della clientela,
- Aumentata convenienza economica dei processi,
- Produttività dello staff,
- Qualità di Errori e rifacimenti,
- Numero di rapporti di non conformità,

IL COBIT: Linee guida per il Management

PO1 Planning & Organisation
Define a Strategic Information Technology Plan

Control over the IT process **Define a Strategic IT Plan** with the business goal of *striking an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment*

ensures delivery of information to the business that addresses the required Information Criteria and is measured by Key Goal Indicators

is enabled by *a strategic planning process undertaken at regular intervals giving rise to long-term plans; the long-term plans should periodically be translated into operational plans setting clear and concrete short-term goals*

considers Critical Success Factors that leverage specific IT Resources and is measured by Key Performance Indicators

Information Criteria
P effectiveness
S efficiency
confidentiality
integrity
availability
compliance
reliability

(P) primary (S) secondary

IT Resources
✓ people
✓ applications
✓ technology
✓ facilities
✓ data

(✓) applicable to

Critical Success Factors

- The planning process provides for a prioritisation scheme for the business objectives and quantifies, where possible, the business requirements
- Management buy-in and support is enabled by a documented methodology for the IT strategy development, the support of validated data and a structured, transparent decision-making process
- The IT strategic plan clearly states a risk position, such as leading edge or road-tested, innovator or follower, and the required balance between time-to-market, cost of ownership and service quality
- All assumptions of the strategic plan have been challenged and tested
- The processes, services and functions needed for the outcome are defined, but are flexible and changeable, with a transparent change control process
- A reality check of the strategy by a third party has been conducted to increase objectivity and is repeated at appropriate times
- IT strategic planning is translated into roadmaps and migration strategies

Key Goal Indicators

- Percent of IT and business strategic plans that are aligned and cascaded into long- and short-range plans leading to individual responsibilities
- Percent of business units that have clear, understood and current IT capabilities
- Management survey determines clear link between responsibilities and the business and IT strategic goals
- Percent of business units using strategic technology covered in the IT strategic plan
- Percent of IT budget championed by business owners
- Acceptable and reasonable number of outstanding IT projects

Key Performance Indicators

- Currency of IT capabilities assessment (number of months since last update)
- Age of IT strategic plan (number of months since last update)
- Percent of participant satisfaction with the IT strategic planning process
- Time lag between change in the IT strategic plans and changes to operating plans
- Index of participants involved in strategic IT plan development, based on size of effort, ratio of involvement of business owners to IT staff and number of key participants
- Index of quality of the plan, including timelines of development effort, adherence to structured approach and completeness of plan

IL COBIT: Linee guida per il Management

PO9 Planning & Organisation
Assess Risks

Control over the IT process **Assess Risks** with the business goal of *supporting management decisions in achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors*

ensures delivery of information to the business that addresses the required Information Criteria and is measured by Key Goal Indicators

is enabled by *the organisation engaging itself in IT risk-identification and impact analysis, involving multi-disciplinary functions and taking cost-effective measures to mitigate risks*

considers Critical Success Factors that leverage specific IT Resources and is measured by Key Performance Indicators

Information Criteria	
P	effectiveness
S	efficiency
P	confidentiality
P	integrity
P	availability
S	compliance
S	reliability

(P) primary (S) secondary

IT Resources	
✓	people
✓	applications
✓	technology
✓	facilities
✓	data

(✓) applicable to

Key Goal Indicators

- Increased degree of awareness of the need for risk assessments
- Decreased number of incidents caused by risks identified after the fact
- Increased number of identified risks that have been sufficiently mitigated
- Increased number of IT processes that have formal documented risk assessments completed
- Appropriate percent or number of cost effective risk assessment measures

Critical Success Factors

- There are clearly defined roles and responsibilities for risk management ownership and management accountability
- A policy is established to define risk limits and risk tolerance
- The risk assessment is performed by matching vulnerabilities, threats and the value of data
- Structured risk information is maintained, fed by incident reporting
- Responsibilities and procedures for defining, agreeing on and funding risk management improvements exist
- Focus of the assessment is primarily on real threats and less on theoretical ones
- Brainstorming sessions and root cause analyses leading to risk identification and mitigation are routinely performed
- A reality check of the strategy is conducted by a third party to increase objectivity and is repeated at appropriate times

Key Performance Indicators

- Number of risk management meetings and workshops
- Number of risk management improvement projects
- Number of improvements to the risk assessment process
- Level of funding allocated to risk management projects
- Number and frequency of updates to published risk limits and policies
- Number and frequency of risk monitoring reports
- Number of personnel trained in risk management methodology

IL COBIT: Linee guida per il Management

Conclusioni:

Per avere sotto controllo la Tecnologia Informatica in modo che l'IT sia allineata all'azienda nel suo complesso e che sia un fattore abilitante è necessario seguire le Linee guida per il Management, il COBIT si esprime:

"**I CSF sono quanto di più importante si deve fare sulla base delle scelte effettuate nel modello di Maturità, monitorando contemporaneamente tramite i KPI la probabilità di raggiungimento degli abiettivi stabiliti dai KGI**"

Linee Guida per l'AUDIT introduzione

COBIT(Control Objectives for Information and Related Technology).

IL COBIT: Linee guida per Audit

Negli ultimi anni è diventato evidente la necessità di un Framerwork per la sicurezza e per il controllo dell'IT, il successo dell'organizzazione dipende dalla comprensione dei rischi e dei vincoli all'interno dell'azienda per raggiungere un adeguato controllo.

La globale competizione delle aziende e le organizzazioni che sono in costante riorganizzazione, semplificazione, miglioramento della competenze, portano ad un "re-ingineering" dei processi aziendali, alla gestione in "outsourcing" , appiattimento delle organizzazioni per migliorare i costi, tutti questi cambiamenti influiscono sul governo del Business e dell'Azienda. Scaturisce la necessità del governo dell'IT e conseguentemente Audit nell'Information Tecnology.

IL COBIT: Linee guida per Audit

Le linee guida per l'AUDIT sono la semplice applicazione del Framerwork di COBIT.

Le Linee Guida del COBIT per l'Audit sono generiche e di alto livello, richiedono di fornire al management l'assicurazione che determinati obiettivi di controllo vengano raggiunti.

Le Linee guida di Audit forniscono una guida per preparare il piano di Audit, integrato con il Framerwork di dettaglio degli Obiettivi di Controllo.

Le linee guida abilitano l'Auditor nella revisione dei processi, aiutano il Management a capire dove i controlli sono sufficienti e viceversa, in quali processi sono necessari dei miglioramenti, può dare supporto al piano di sviluppo di una Azienda.

IL COBIT: Linee guida per Audit

Struttura generale dell'Audit definisce obiettivi di Audit:

- •Fornire al Management una ragionevole assicurazione che gli obiettivi di controllo sono raggiunti,
- •Indicare al Managemet azioni correttive,
- • Avere comprensione dei requisiti di Business in relazione ai Rischi e relative misure di controllo,
- •Valutare l'appropriato stato dei controlli,
- •Valutare la conformità dei test dello stato dei controlli se stanno lavorando correttamente,
- •Avere certezza che gli obiettivi di controllo lavorano come prescritto,

IL COBIT: Linee guida per Audit

Nel fornire aiuto al Management e necessario che:

- Definire un approccio a livelli orientato agli obiettivi di Business,
- che l'approccio sia del tipo "process driven",
- Concentrarsi sulle risorse che sono necessarie al Management,
- concentrasi sui criteri che sono necessari al Management,

IL COBIT: Linee guida per Audit

L'Applicazione delle linee guida di Audit:

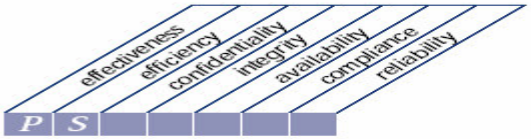
- Level 1 "Approccio generali di AUdit":
  - Utilizzo del Cobit Framerwork " di alto livello"
  - Utilizzo delle linee guida di Audit di alto livello
- Level 2 " Process Audit guidelines
  - Linee guida di Audit in dettaglio
- Livello 3 " Punti di attenzione e dettaglio degli obiettivi di controllo"
  - Dettagliare le tecniche di controllo utilizzate,
  - Specificre le piattaforme utilizzate,
  - Specificare gli standard industriali,
  - Specificare i criteri adottati.

IL COBIT: Linee guida per Audit

PO1 Planning & Organisation
Define a Strategic Information Technology Plan

COBIT

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

defining a strategic IT plan

that satisfies the business requirement

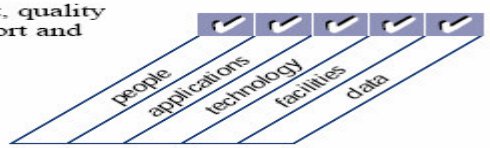
to strike an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment

is enabled by

a strategic planning process undertaken at regular intervals giving rise to long-term plans; the long-term plans should periodically be translated into operational plans setting clear and concrete short-term goals

and takes into consideration

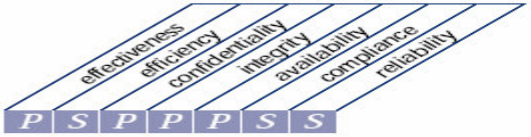
- enterprise business strategy
- definition of how IT supports the business objectives
- inventory of technological solutions and current infrastructure
- monitoring the technology markets
- timely feasibility studies and reality checks
- existing systems assessments
- enterprise position on risk, time-to-market, quality
- need for senior management buy-in, support and critical review



IL COBIT: Linee guida per Audit

PO9 **Planning & Organisation**
Assess Risks
COBIT

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

assessing risks

that satisfies the business requirement

of supporting management decisions through achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors

is enabled by

the organisation engaging itself in IT risk-identification and impact analysis, involving multi-disciplinary functions and taking cost-effective measures to mitigate risks

and takes into consideration

- risk management ownership and accountability
- different kinds of IT risks (technology, security, continuity, regulatory, etc.)
- defined and communicated risk tolerance profile
- root cause analyses and risk brainstorming sessions
- quantitative and/or qualitative risk measurement
- risk assessment methodology
- risk action plan
- timely reassessment

COBIT Implementazione

COBIT(Control Objectives for Information and Related Technology).

COBIT Implementazione

Il COBIT è orientato al business, è utilizzato dal management dell'IT, nella gestione dei rischi.

Il COBIT contiene anche un *Implementation Tool Set che fornisce delle indicazioni operative per le organizzazioni*

COBIT Implementazione

Come Introduci il Cobit nella tua Organizzazione.

Introduzione:

Il COBIT fornisce delle pratiche generalmente accettate, per:

•**Il Management** , gestendo i rischi generalmente accettati, controllare gli investimenti di un ambiente IT.

•Aiuta **l'Utente** ad avere maggiore sicurezza e controllo sull'IT.
•Aiuta **l'Auditor** a sostenere le opinioni del management sui controlli interni dell'IT ad essere proattivo e consigliare le azioni sul Business.
Alcune aree funzionali e organizzazioni possono ottenere benefici dall'utilizzo del COBIT, i Manager possono trarre beneficio nel prender decicisioni sugli investimenti IT.
Con il COBIT gli utenti possono otenere assicurazione sui processi per gestire l'IT, il COBIT da possibilità all'Auditor di fornire I criteri per le revisioni dei processi per migliorare Efficenza e Efficacia.

COBIT Implementazione

EXHIBIT 1

WHEN YOU ARE...	COBIT COULD SERVE THE FOLLOWING OBJECTIVES FOR YOU...	SOME SPECIFIC APPROACHES WHICH COULD PROVE TO BE USEFUL TO YOU...
Executive manager	Accept and promote COBIT's IT governance model for all entities within the enterprise.	Use COBIT to complement existing internal control frameworks (e.g., COSO) for IT specific matters. Use COBIT to self-assess the organisation against generally accepted international standards and take actions to improve their IT operations, as warranted. Use the COBIT process model to establish a common language between business and IT as well as to allocate clear responsibilities.
Business manager	Use COBIT to establish a common entity-wide control model so as to manage and monitor IT's contribution to the business.	Use the COBIT control objectives as code of good practice for dealing with IT at large within the business function. Use the COBIT control objectives to determine the different aspects which need to be covered by the Service Level Agreement (SLA) agreed upon with the IT function (whether internally or outsourced).
IT manager	Use the COBIT process model and detailed control objectives so as to structure the IT services function into manageable and controllable processes focussing on the business contribution. The latter is the domain of quality, security and effectiveness.	Use the COBIT control model to establish SLAs and to communicate with business functions. Use the COBIT control model as the basis for process-related performance measures. Use the COBIT control model as the basis for IT-related policies and norms. Use COBIT as the baseline model to establish the appropriate level of generally accepted control objectives as well as for external certifications (e.g., SysTrust™ and SAS 70).

COBIT Implementazione

How To Introduce CobiT Into Your Organisation, *continued*

Exhibit 1, *continued*

When you are…	CobiT could serve the following objectives for you…	Some specific approaches which could prove to be useful to you…
Project Manager	As general framework for minimal project and quality assurance standards.	Use CobiT to help ensure that project plans incorporate generally accepted phases in IT planning, acquisition and development, service delivery, and project management and assessment.
Developer	As minimal guidance for controls to be applied within development processes as well as for internal control to be integrated in information systems being built.	Use CobiT to ensure that all applicable IT control objectives in the development project have been addressed.
Operations	As general framework for minimal controls to be integrated into service delivery and support processes, placing clear focus on client objectives.	Use CobiT to ensure that operational policies and procedures are sufficiently comprehensive.
User	As minimal guidance for internal control to be integrated within information systems, being fully operational or under development.	Use CobiT to guide service level agreements.
Information security officer	As harmonising framework providing a way to integrate information security with other business related IT objectives.	Use CobiT to structure the information security program, policies, and procedures.
Auditor	As basis for determining the IT audit universe and as IT control reference.	Use CobiT as criteria for review and examination and for framing IT-related audits.

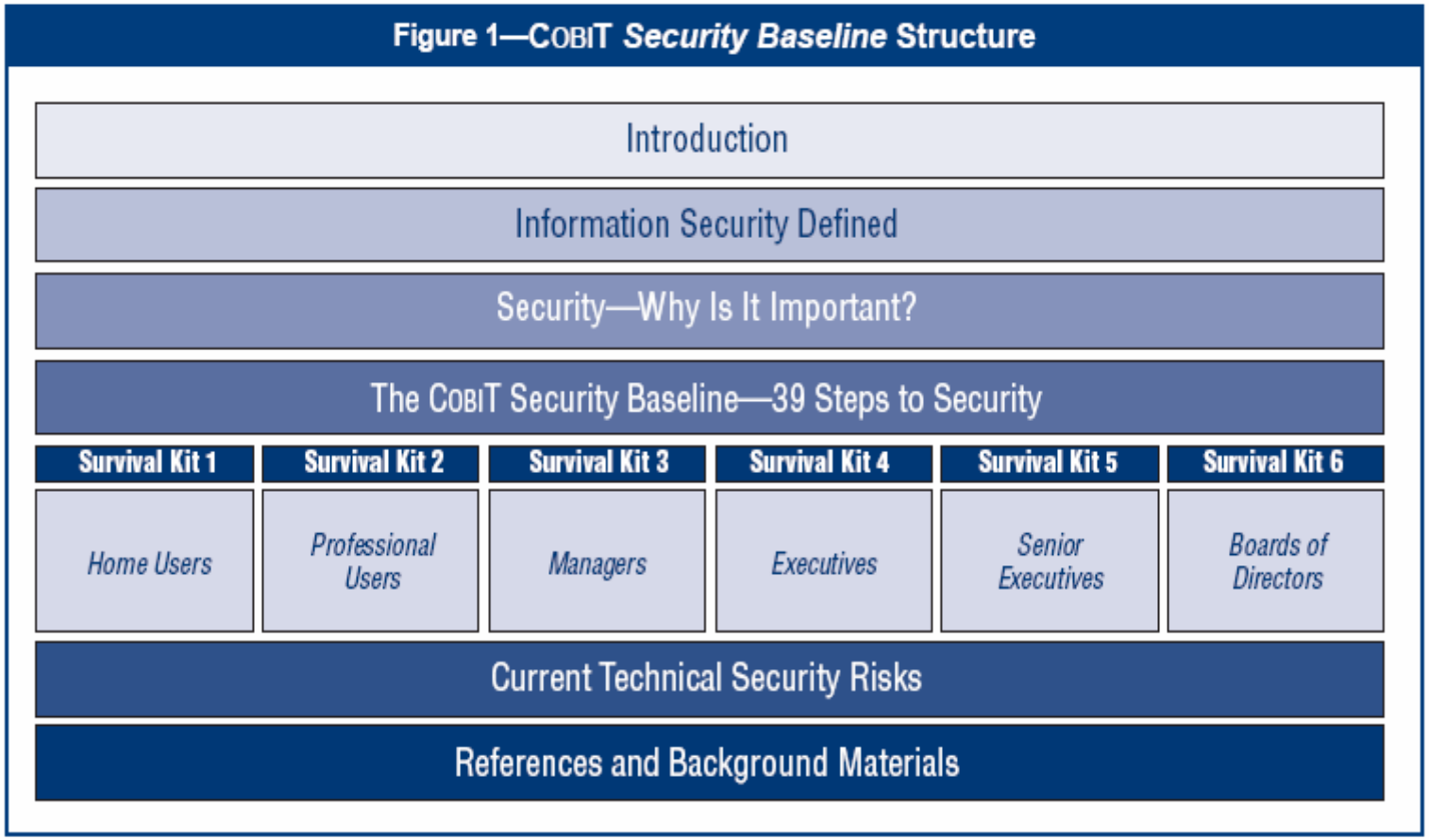
COBIT Security Baseline

COBIT(Control Objectives for Information and Related Technology).

COBIT Security Baseline

Questa Guida è basata sul *Control Objectives for Information and related Technology* (COBIT), la guida è un comprensivo set di risorse per comprendere le necessità dell'organizzazione e il governo dell'IT e della gestione dei RIschi.
Questa guida si concentra sui specifici rischi della Sicurezza IT in modo semplice per implementarla per le piccole, medie e grandi aziende.

COBIT Security Baseline



COBIT

Agenda per i prossimi incontri:

Creare dei gruppi per trattare e approfondire Il COBIT :

- COBIT controlli dell' IT "IT Control Framerwork" di alto livello e applicabilità,
- COBIT dettaglio degli Obiettivi di Controllo e applicabilità,
- COBIT Linee guida del Management e applicabilità,
- COBIT Linee guida di Audit e applicabilità,
- COBIT Implementazione "Implementation e Tool Set" e applicabilità,

COBIT introduzione

(Control Objectives for Information and Related Technology).

Termine della presentazione

Antonello Giuliani
CISA
Antonello.giuliani@capgemini.com