ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Dipartimento di Informatica
Facoltà di Scienze M.F.N.
Università di Roma "La Sapienza"

IL RUOLO DELL'IT GOVERNANCE E DEL COBIT NELL'ALLINEAMENTO DELL'IT AL BUSINESS

(a cura di **Enrico Ferretti - Protiviti - LA ISO 27001**)

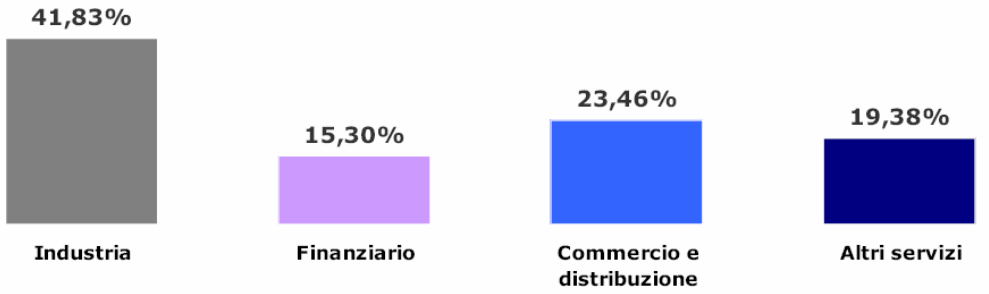
INDICE DELLA PRESENTAZIONE

- **L'IT Governance**
- Case study
- Riferimenti bibliografici e sitografici

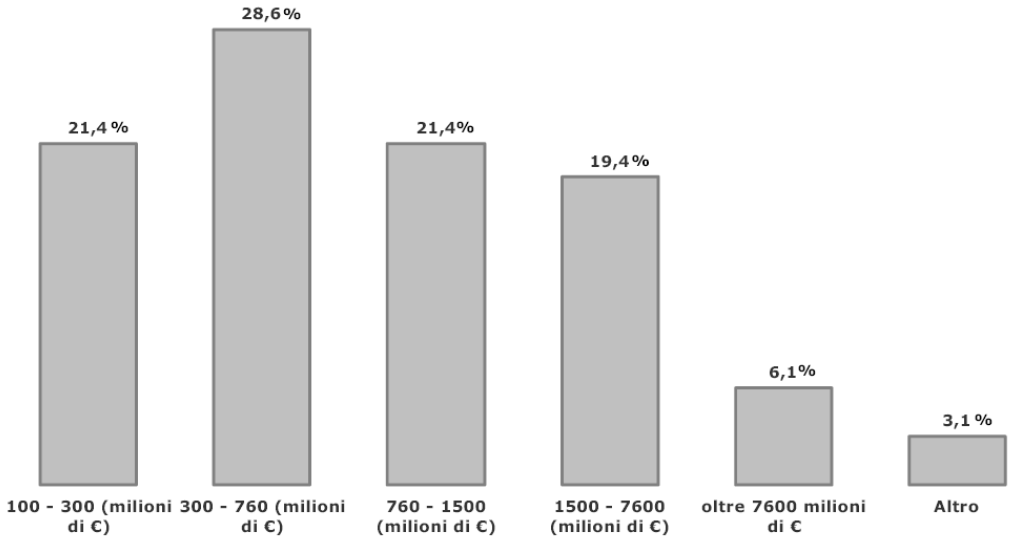
PROTIVITI RISK BAROMETER

Protiviti ha recentemente condotto una ricerca finalizzata a comprendere la percezione dell'esposizione al rischio e lo stato di implementazione dei processi di risk management di 100 primarie aziende italiane

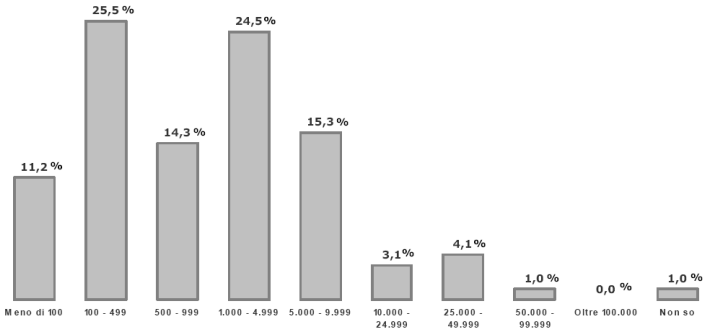
Settore di business di appartenenza delle società campione



Fatturato/giro d'affari delle società campione



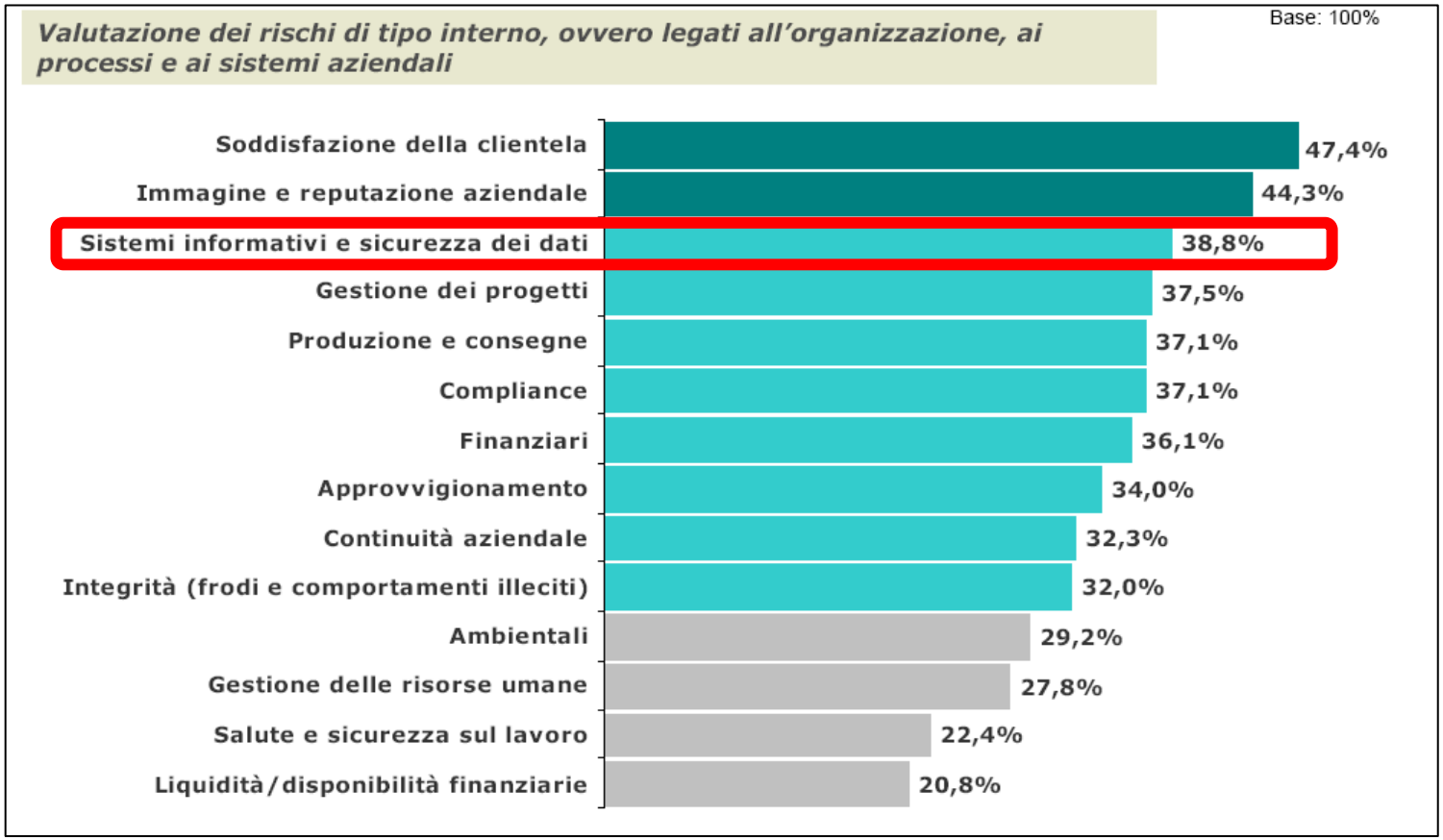
Numero di dipendenti delle società campione



Risk Barometer – Protiviti (Italia)

RISULTATI – IL RUOLO DELL'IT

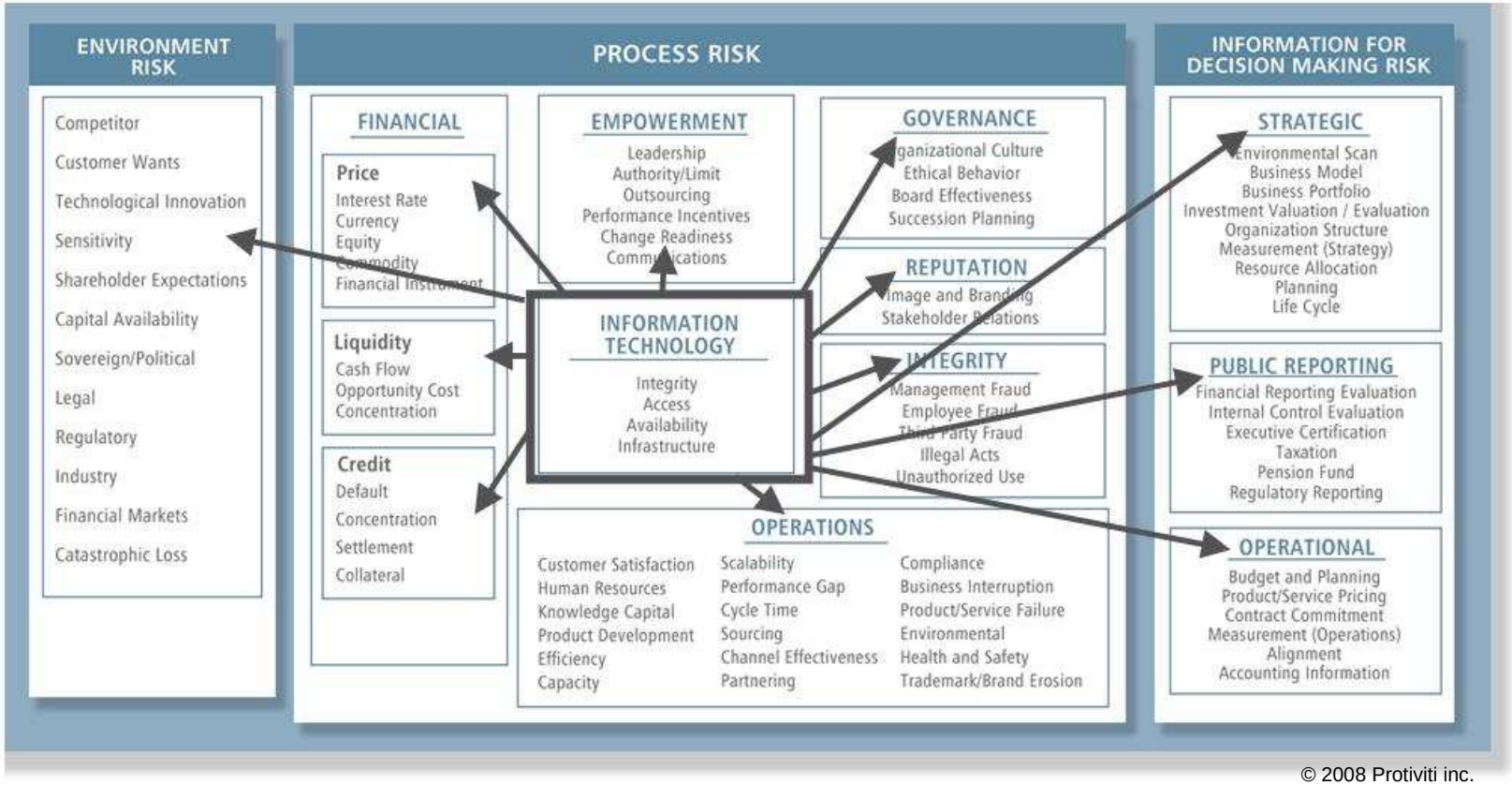
Relativamente alla valutazione dei rischi di tipo interno, ovvero legati all'organizzazione, ai processi e ai sistemi aziendali, la ricerca ha prodotto i seguenti risultati



Risk Barometer – Protiviti (Italia)

IT RISK MANAGEMENT

A causa della pervasività dei sistemi informativi in tutti i processi aziendali, i rischi di natura IT influenzano tutte le altre tipologie di rischio



Information Technology Risk is not just an IT issue!

I processi aziendali sono sempre più dipendenti dai Sistemi Informativi!

I rischi ai quali è soggetta la Funzione IT possono comportare serie conseguenze per il business della società e dare luogo ad interruzioni delle attività "core" nel breve, medio e lungo periodo, alle quali l'Organizzazione potrebbe non riuscire a far fronte

Risulta quindi importante identificare e prioritizzare i rischi in capo all'azienda e, nello specifico, alla Funzione IT

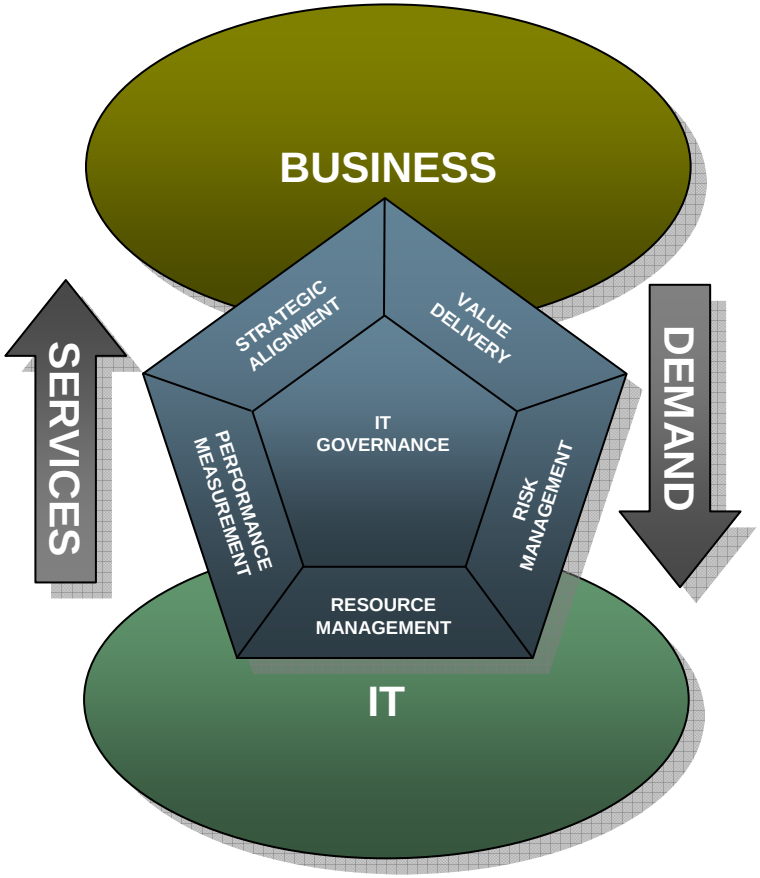
Examples of recent IT related mishaps:

- *2.3 million customer records were stolen containing credit card and other personal information.*
- *45.6 million credit and debit card numbers were stolen from a computer system.*
- *A routine programming change led to the interruption of service to 10 million customers.*
- *A bank halted PIN-based transactions in three countries associated with data compromised at a third party.*
- *Backup tapes, containing information on 470,000 clients, were lost in-transit.*
- *A database fault left 400,000 without pay.*

L'IT GOVERNANCE

Un **modello di IT Governance** consente di definire in maniera univoca e valida a livello aziendale le modalità di gestione dell'IT, in termini di struttura organizzativa, processi e procedure, strumenti, assicurando un approccio omogeneo e strutturato

- **Allineamento strategico**, finalizzato ad assicurare la rispondenza tra i piani aziendali ed i piani IT ed allineare l'operatività dell'IT a quella aziendale
- **Erogazione del valore**, finalizzata ad assicurare che l'IT produca i benefici attesi rispetto agli obiettivi strategici
- **Gestione delle risorse**, finalizzata a valutare gli investimenti ed a gestire nella maniera più appropriata le risorse IT
- **Gestione del rischio**, finalizzata alla consapevolezza dei rischi da parte dell'alta direzione aziendale, mediante una chiara visione della propensione al rischio dell'impresa, la conoscenza dei requisiti di conformità, e l'inserimento di responsabili dell'IT risk management all'interno dell'organizzazione
- **Misurazione della performance**, finalizzata a valutare e controllare l'attuazione della strategia, la conduzione dei progetti, l'utilizzo delle risorse, la performance dei processi e l'erogazione dei servizi



LA PERCEZIONE DEL MERCATO

Figure 13—Importance of IT, by Sector

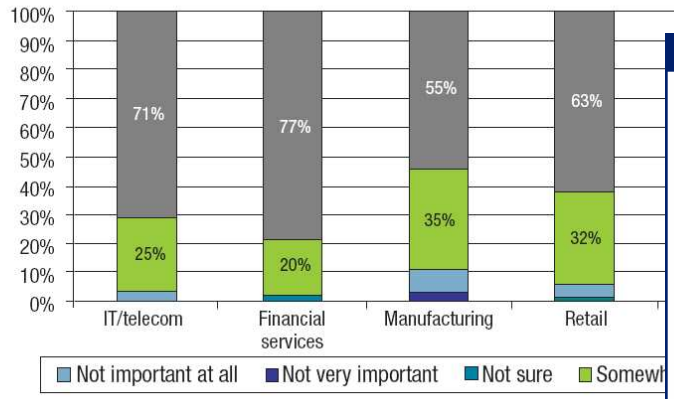


Figure 29—IT-related Problems in Last 12 Months

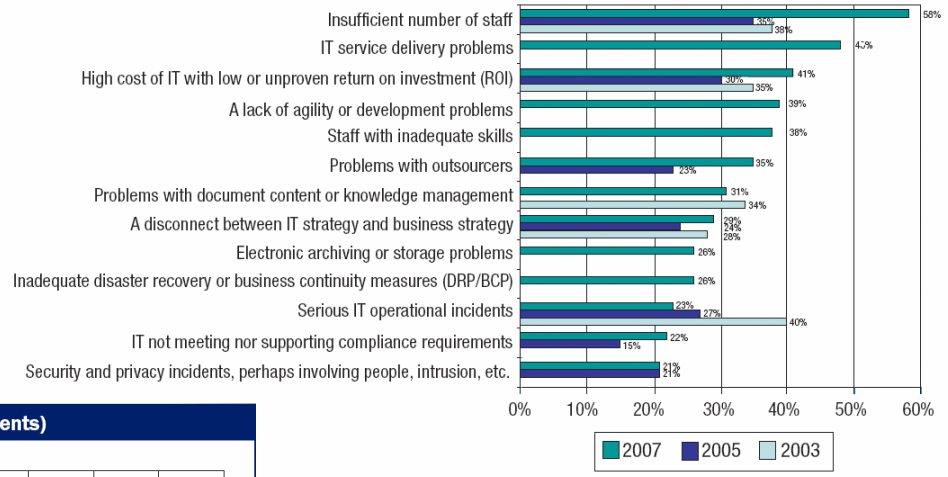
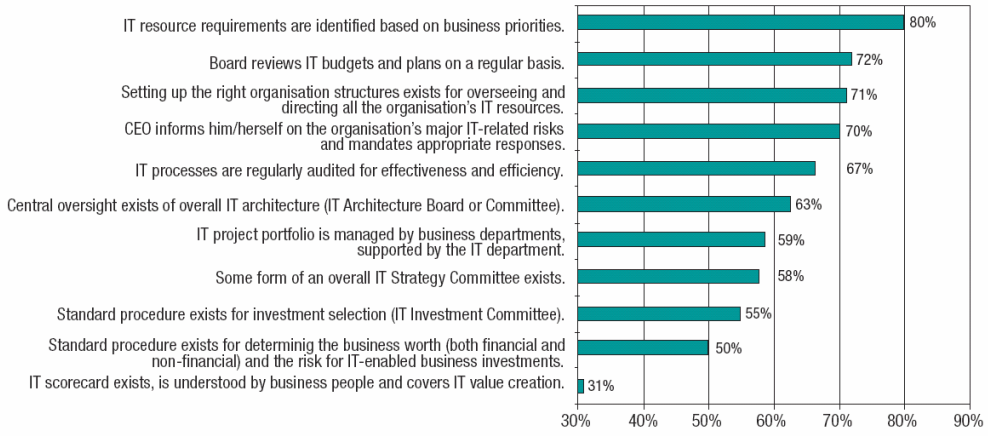
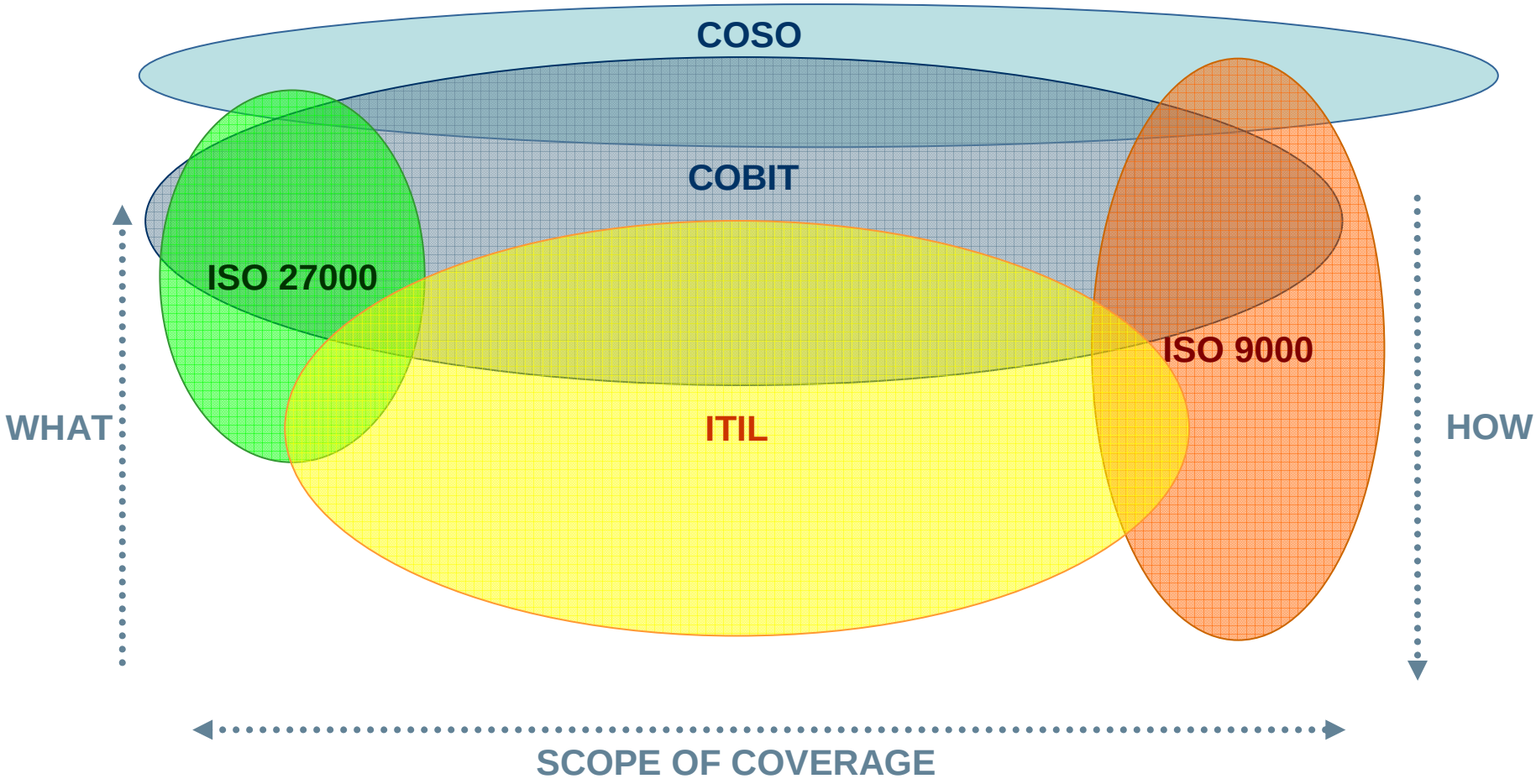


Figure 33—Current IT Governance Practices (749 Respondents)

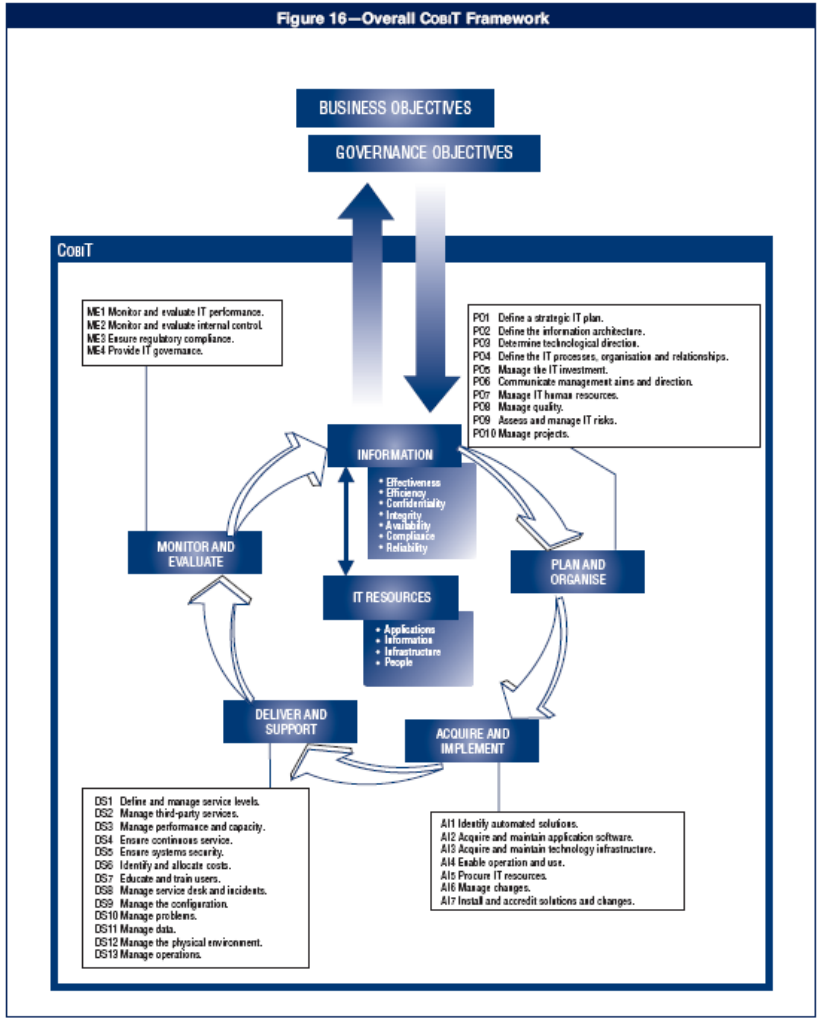


ITGI 2008

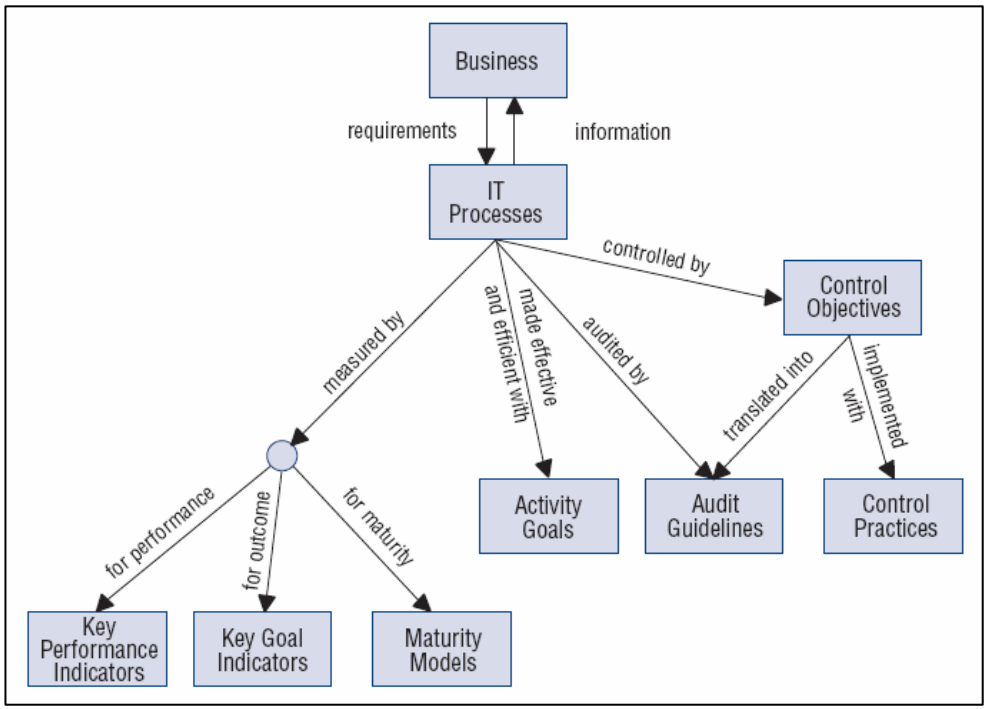
FRAMEWORK DI RIFERIMENTO



IL COBIT



- Fornisce gli strumenti per mettere in relazione il business e l'IT
- Fornisce un modello di misurazione per tracciare le performance dell'IT basato sul CMM
- Identifica le principali risorse IT
- Definisce gli obiettivi di controllo che il management dovrebbe utilizzare



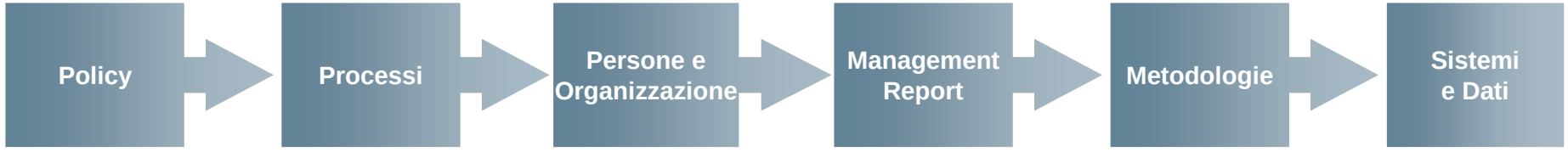
CAPABILITY MATURITY MODEL

Capability Maturity

Capability Level	Capability Description
Optimizing	**CONTINUOUS IMPROVEMENT** Continuously improving controls enterprise-wide
Managed	**QUANTITATIVE** Risks managed quantitatively enterprise-wide "Chain of accountability"
Defined	**QUALITATIVE/QUANTITATIVE** Policies, process and standards defined and institutionalized -- "Chain of certification"
Repeatable	**INTUITIVE** Process established and repeating; reliance on people continues -- Controls documentation lacking
Initial	**AD HOC/CHAOTIC** Control is not a priority -- Unstable environment leads to dependency on heroics

6 ELEMENTS OF INFRASTR.

Protiviti utilizza il proprio modello "Six Elements Infrastructure" per valutare in modo sistematico le componenti critiche della gestione dei sistemi informativi e le capability essenziali relative ad ognuna di esse



- Obiettivi d'implementazione
- Allineamento con il Business
- Policy IT
- Policy per il Rischio

- Project Management
- Processi IT
- Processi Operativi
- Erogazione di Servizi
- Supporto ai Servizi

- Project Steering Committee
- Sponsor di Progetto
- Process/Data Owner
- Technical Owner
- Job Role
- Segregation of Duty

- Report di Controllo sui processi IT
- Report su Integrità dei dati e su Errori
- Report su violazioni (es. limiti di sicurezza / rischio)
- Financial Reporting
- Management Reporting

- Controlli sui Progetti
- Application Design
- Application Deployment
- Profile/Security Approach
- Change Management

- Business Application
- Database
- Infrastruttura Tecnica
- Internet/Intranet
- Interfacce
- Master Data
- Transazioni

Rischi associati:

I processi non seguono le policy stabilite e/o non ottengono i risultati attesi

Non si dispone della conoscenza e/o esperienza necessaria ai processi

I report non forniscono informazioni utili per una gestione efficace

Le metodologie non analizzano adeguatamente i dati e le informazioni

Non sono disponibili informazioni per l'analisi e il reporting

SEI + CMM

	Business Policies	Business Processes	People and Organization	Management Reports	Methodologies	Systems and Data
Optimized	Aligned strategic plans, total strategic sourcing, defined and integrated policies & responsibilities	Integrated and effective procurement processes and continuous benchmarking	Ability to adapt to changing environments and customer demands, Outsourcing of non core competencies	Fully developed automated, consistent follow-up and planning	Aligned strategic methodologies that emphasize continuous improvement	Complete suite of systems across the supply chain for analysis
Managed	Initial execution of strategic sourcing and personnel aligned against plans	Effective utilization of formal risk management techniques	Consolidated and leveraged supply base in place; Trained commodity teams,	High quality procurement information, self assessment commonplace	Sophisticated, robust models and tools	Procurement data warehouse in place and utilized; P-cards and automation
Defined	Annual procurement plans, strategic sourcing for key commodities	Defined processes, Strategic partnerships in place	A/P centralized, training offered, and special purpose teams	Key suppliers tracked, standard benchmarks and internal audits	Well-developed models available for decision-making	Organization operates with contracts
Repeatable	Only occasional strategic focus on sourcing and informal polices	Occasional supply leverage; A few strategic partnerships	Some procurement professionals; Limited training	Key internal procurement information available with audits occurring	Simple models used inconsistently	Suite of fairly effective systems; Procedures manual
Initial	Procurement not addressed as a strategic opportunity, no direction or policies	Purchases not leveraged, No strategic partnerships	No leadership and lack of qualified staff	Critical information not available and no internal auditing	No models; Reliance on people	Disparate, inefficient, purchasing, A/P systems

INDICE DELLA PRESENTAZIONE

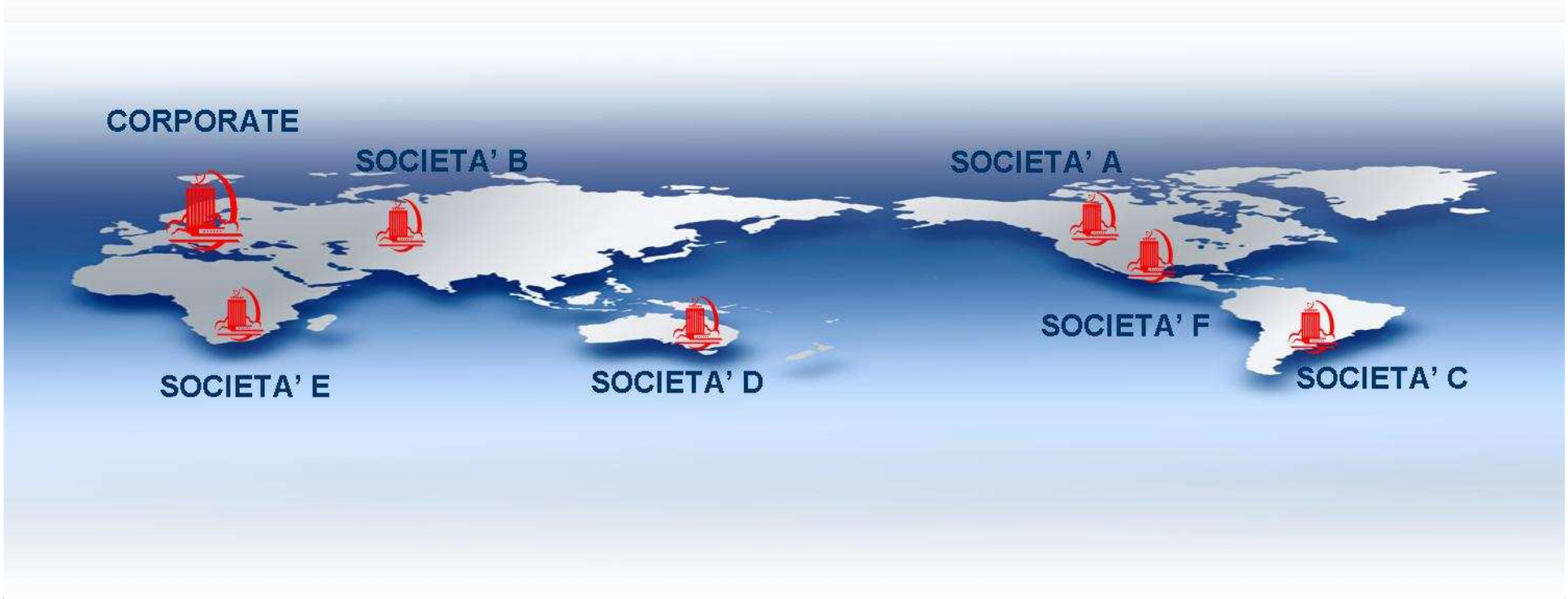
- L'IT Governance
- **Case study**
- Riferimenti bibliografici e sitografici

IL CASO XYZ

La Società XYZ è un primario Gruppo Internazionale, con un fatturato di oltre 1 Miliardo di Euro

La struttura societaria è così composta:

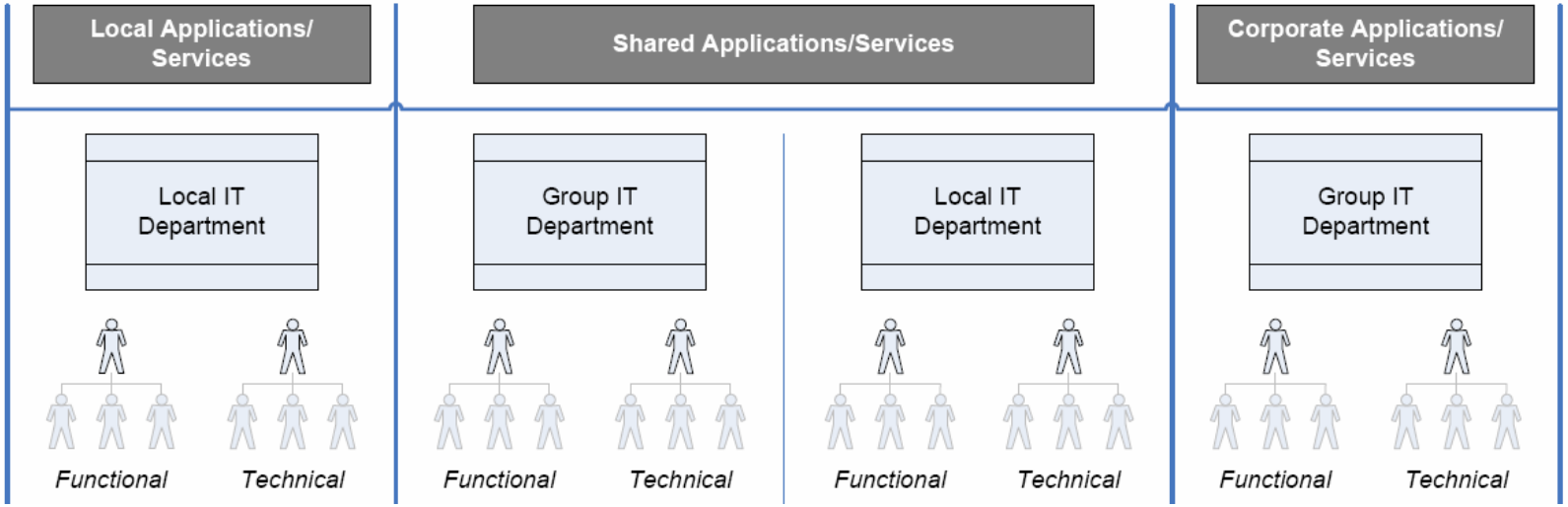
- Corporate, con sede in Italia, quotata alla Borsa Italiana da circa 2 anni
- 6 Società Operative con sedi dislocate nei 5 continenti



LA REALTA' IT

La realtà IT che caratterizza il Gruppo XYZ può essere sintetizzata dai seguenti elementi, che costituiscono i fulcri del Modello di IT Governance che regola le attività IT:

- una struttura IT di Gruppo e strutture IT locali all'interno delle singole società operative
- sistemi suddivisibili in 3 categorie:
  - Sistemi condivisi fra la Corporate e le Società Operative (es. SAP condiviso tra le società del gruppo);
  - Sistemi centrali a supporto dei processi gestionali della Corporate;
  - Sistemi locali a supporto dei processi gestionali e di business delle Società Operative.
- alto grado di esternalizzazione (Outsourcing) di alcuni processi IT, tra cui l'Application Management



LA REALTA' IT (CONT.)

Con l'obiettivo di gestire al meglio la crescente complessità della realtà IT ed alla luce delle esigenze di carattere informativo, operativo, organizzativo e di controllo interno, è stato avviato un Progetto per la definizione di un Modello di Governance IT

Il modello di Governance IT ha l'obiettivo di indirizzare la definizione e la comunicazione delle responsabilità di gestione dell'IT, facilitare il miglioramento della gestione e dell'erogazione di servizi IT, definire le regole per lo sviluppo, l'implementazione e il monitoraggio delle modalità di gestione dei processi IT, coerentemente alle Strategie del Gruppo e ai relativi processi operativi

Allineamento Strategico

Architettura IT

Trasferimento del Valore

Gestione degli Asset IT

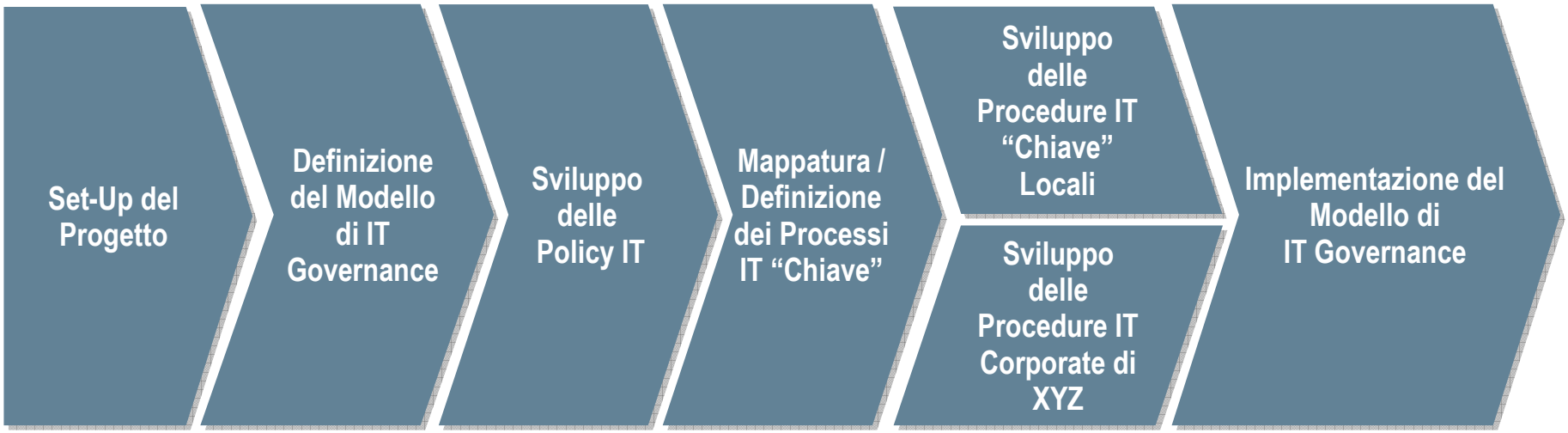
Gestione del Rischio

Misurazione delle Prestazioni

Sinergia

MODELLO DI IT GOVERNANCE

L'approccio utilizzato nella definizione del Modello di IT Governance può essere così sintetizzato



POLICY

Obiettivi:

- definire, promuovere, suggerire, scoraggiare o proibire determinate prassi operative, processi, tecnologie e controlli interni relativi alla gestione dell'IT

Policy IT:

- fornire principi e linee guida per la gestione dell'IT che supporta il business del gruppo

Procedure (operative):

- regolamentare dal punto di vista operativo le varie attività descritte dalle Policy IT

IT GOVERNANCE

- Pianificazione ed Organizzazione
- Acquisizione ed Implementazione
- Erogazione e Supporto
- Continuità Operativa
- Sicurezza delle Informazioni
- Monitoraggio e Valutazione

POLICY (CONT.)

IT GOVERNANCE

Pianificazione ed Organizzazione	***Assicurare l'allineamento dei processi IT alle necessità aziendali mediante un'adeguata pianificazione delle risorse ed una coerente organizzazione a supporto***
Acquisizione ed Implementazione	***Garantire l'efficacia e l'efficienza delle risorse IT, fornendo al Gruppo XYZ strumenti corretti e affidabili***
Erogazione e Supporto	***Garantire Livelli di Servizio IT costanti, efficaci, affidabili, sicuri ed efficienti che consentano il raggiungimento degli obiettivi aziendali e della continuità operativa delle funzioni di staff***
Continuità Operativa	***Garantire la continuità operativa del Business, anche in caso di situazioni o eventi di carattere catastrofico***
Sicurezza delle Informazioni	***Garantire la riservatezza, l'integrità e la disponibilità delle informazioni aziendali***
Monitoraggio e Valutazione	***Assicurare l'adeguatezza e l'efficacia dei meccanismi di controllo che garantiscono il governo dell'IT***

PROCEDURE

Pianificazione ed Organizzazione	• Pianificazione • Gestione dei Rischi • Gestione e Controllo	
Acquisizione ed Implementazione	• *Valutazione dei Requisiti* • Gestione delle Applicazioni SAP • *Acquisizione ed Implementazione Soluzioni IT*	• *Acquisizione delle Infrastrutture IT* • Gestione del Cambiamento Applicativo • Gestione del Cambiamento Tecnologico
Erogazione e Supporto	• Gestione degli SLA • Help Desk • *Supporto operativo*	• *Gestione degli Asset IT*
Continuità Operativa	• Valutazione dei Rischi di Disponibilità • Gestione delle Inefficienze • Gestione delle Crisi	• *Gestione dei Backup*
Sicurezza delle Informazioni	• Gestione degli Accessi Logici e dei Profili utente • Accessi di Emergenza • Sicurezza SAP	• *Registrazione e Monitoraggio degli Eventi di Sicurezza* • *Gestione delle Configurazioni di Sicurezza*
Monitoraggio e Valutazione	• *Monitoraggio dei Rischi IT*	

Procedure IT Corporate e Locali

Procedure IT Corporate

INDICE DELLA PRESENTAZIONE

- L'IT Governance
- Case study
- **Riferimenti bibliografici e sitografici**

Grazie per l'attenzione!

Link

www.protiviti.it
www.knowledgeleader.com
www.itgi.org
www.itpolicycompliance.com

Riferimenti

Enrico Ferretti
enrico.ferretti@protiviti.it
346 7981 427