

# Security governance & Risk management

## Introduzione

E-security lab  
28 gennaio 2010  
Carlo Guastone

1

# La Mission dei Sistemi ICT

Ottimizzare e innovare i processi aziendali  
tramite la identificazione e l' utilizzo mirato e  
innovativo delle tecnologie ICT.

## COME?

Tramite un **insieme di aree di intervento**, relative alle principali leve organizzative e tecnologiche che da sempre caratterizzano i servizi ICT aziendali

Adottando un approccio sistemico di **IT Governance**

Assicurando un' **efficace ed efficiente Security Governance**

2

## Alcune aree di intervento (I)



AREE	Anni settanta - ottanta	Anni novanta	Anni Duemila
<b>Strategie</b>	Realizzare e gestire le <b>applicazioni informatiche gestionali per automatizzare i processi aziendali</b> , tramite le novità tecnologiche in termini di terminali, reti e potenti risorse di calcolo	- <b>Ottimizzare i processi aziendali</b> tramite soluzioni ICT in logica BPR  - <b>Nuovi servizi ICT</b> di base: PC, cellulari, email, etc	-Individuare le <b>tecnologie abilitanti</b> il sistema competitivo  -Individuare e reperire le <b>risorse professionali</b> chiave interne o esterne  -Contribuire al <b>miglioramento dell'organizzazione aziendale</b>
<b>Architetture</b>	- <b>Mainframes</b>  - <b>Sistemi on line, data base</b>	- Arch. <b>client-server</b>  - <b>Sistemi erp</b>	-Nuove <b>architetture emergenti</b> (Soa, Enterprise. 2.0, virtualizzazione, etc)  - <b>Nuovi campi applicativi</b> (Business Intelligence, CRM, Knowl. Manag., dematerializzazione, etc)  -SAAS ( <b>Software as a service</b> ) e Cloud Computing

3

## Alcune aree di intervento (II)



AREE	Anni settanta - ottanta	Anni novanta	Anni Duemila
<b>Sourcing</b>	Prevalente ricorso a <b>specialisti ICT interni</b>	- <b>Terziarizzazione</b> sviluppo applicativo  - Centri di calcolo interni e in <b>outsourcing</b>	- <b>Strategic sourcing</b>  - <b>Rinegoziazione dei Contratti</b> di outsourcing in logica di flessibilità)
<b>Fornitori ICT</b>	-Posizioni <b>oligopolistiche globali</b> - <b>Standard proprietari</b>	-Posizioni <b>Oligopolistiche Settoriali</b>  - <b>Sistemi open</b>	- <b>Concentrazioni e concorrenza</b> - <b>Specializzazione settoriale</b> - <b>Systems integrator</b>
<b>Direzioni utenti</b>	- <b>Limitati contributi</b> alle specifiche dei sistemi  -Controllo dei <b>livelli di servizio</b>  - <b>Limitata competenza ICT</b>	-Partecipazione alla <b>sceita delle soluzioni</b> (es. erp) -Controllo dei <b>costi ICT</b> - <b>Crescente competenza ICT</b>	-Spinta alla <b>ricerca di nuove soluzioni</b>  -Responsabilità della <b>compliance</b> dei sistemi  - La <b>digitalizzazione</b> , in alcuni settori, unifica i processi produttivi con i servizi ICT

4

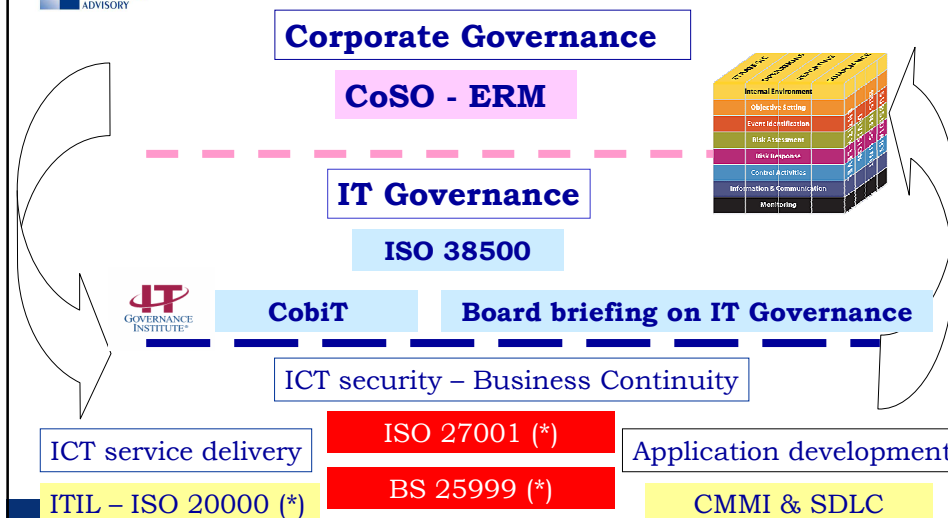
## Alcune aree di intervento (III)



AREE	Anni settanta - ottanta	Anni novanta	Anni Duemila
<b>Sicurezza ICT</b>	Limitata focalizzazione, esperienze in società con Bilanci certificati	Crescita delle sensibilità aziende per il <b>fenomeno Virus</b>	-Alta e crescente focalizzazione per <b>l'incremento dei rischi ICT</b> e per lo sviluppo del <b>quadro Normativo relativo all'ICT</b> (es. Privacy, Legge sul risparmio) - <b>Computer crime</b> e <b>vulnerabilità</b> applicazioni IT - <b>Business continuity</b> richiesta nei settori regolamentati (es. banche)
<b>Consulenza direzionale</b>	<b>Advisory del Vertice</b> dei Grandi gruppi industriali sull'organizzazione ICT aziendale	-Orientamento e <b>supporto nei progetti di BPR</b>  -Studi e <b>ricerche di mercato</b>	- <b>Advisory del management aziendale</b> sulla Governance, Sicurezza e Pianificazione strategica dei sistemi  -Orientamento e supporto <b>nei nuovi campi applicativi</b> (es. CRM, Business Intelligence, etc)

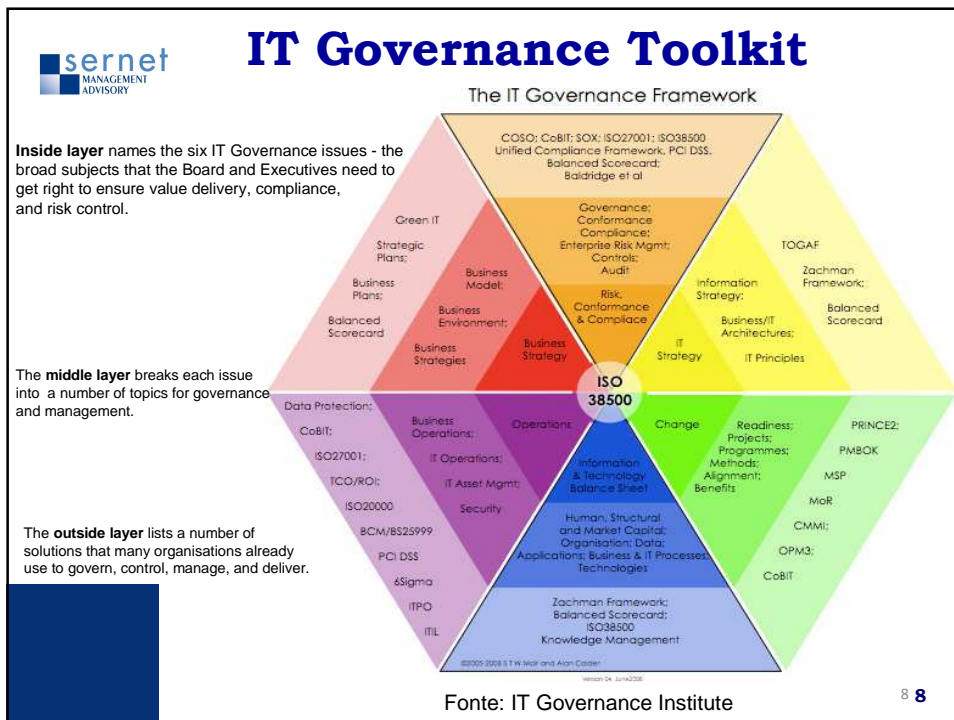
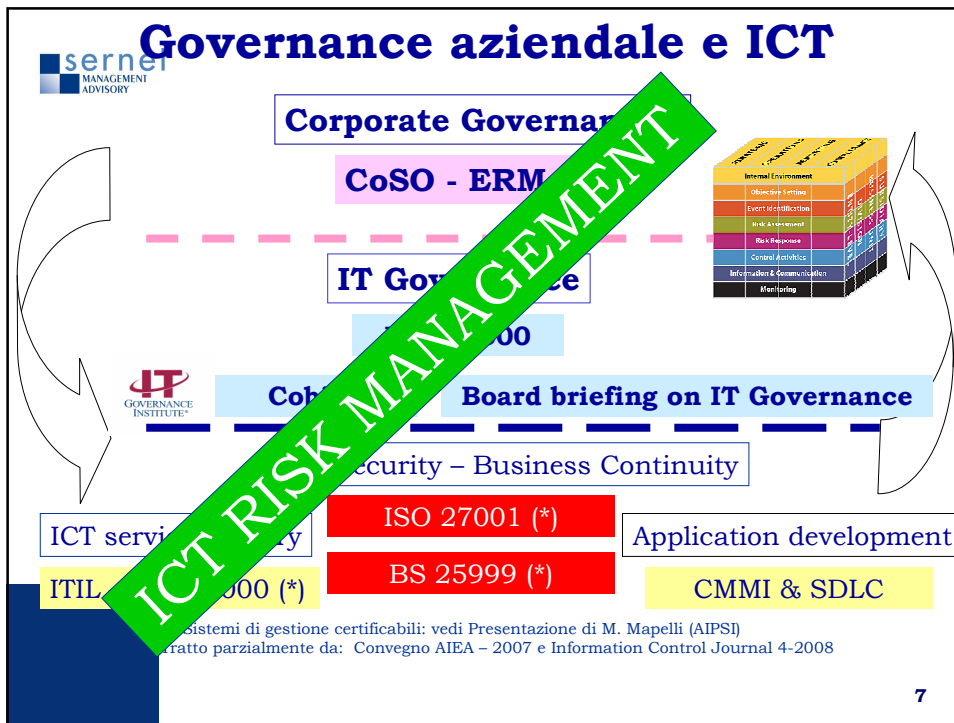
5

## Governance aziendale e ICT



(\*) Sistemi di gestione certificabili: vedi Presentazione di M. Mapelli (AIPSI)  
Tratto parzialmente da: Convegno AIEA - 2007 e Information Control Journal 4-2008

6



## Quali le Tendenze?

- Il **focus** direzionale sulle **tematiche di sicurezza** dei sistemi è ancora di elevata attualità? **Perché?**
- **Come organizzare** con efficacia ed efficienza **il Risk management? Chi coinvolgere?** Bastano le metodologie o servono **Tool di supporto?**
- **Rischi di integrità applicativa:** come affrontarli?
- **Tecnologie emergenti** (Web 2.0, Cloud computing, Devices, etc): **quali gli impatti** sulla sicurezza e le contromisure più appropriate?

9

## Grazie per l'attenzione

[carlo.guastone@sernetspa.it](mailto:carlo.guastone@sernetspa.it)

SERNET spa - via Bassano Porrone 6  
20121 Milano

02-863171

[www.sernetspa.it](http://www.sernetspa.it)