Il Reshaping del Sistema di controllo interno
Esperienze a confronto

Umberto Longo

I PUNTI DI CONTATTO DELLA METODOLOGIA OPERATIVA CON I PRINCIPALI MODELLI INTERNAZIONALI (COSO, ERM, COBIT)

Best practices

Plan-Do-Check-Act

- Metodo di gestione in quattro fasi interattivo, utilizzato in attività per il controllo e il miglioramento continuo dei processi e dei prodotti.

CoSO ERM

- Il CoSO ERM integra il CoSO Report con i processi di gestione del rischio.

CoSO Report

- Il COSO framework (Committee o. Sponsoring Organizations of the Treadway Commission) costituisce l'insieme di Best Practice, riconosciute a livello internazionale, impiegate per la gestione dei Controlli Interni e della Corporate Governance.

Standard ISO 31000

- Principi e linee guida sui modelli di gestione dei rischi.

COBIT

- Il Control Objectives for Information and related Technology (COBIT) è un modello (framework) per la gestione della Information and Communication Technology (ICT).

GLI STRUMENTI DI RILEVAZIONE/ MISURAZIONE QUANTITATIVA DEGLI ELEMENTI DEL MODELLO

I PUNTI DI CONTATTO DELLA METODOLOGIA OPERATIVA CON I PRINCIPALI MODELLI INTERNAZIONALI (COSO, ERM, COBIT)

CoSO Report

Differenziazioni

ERM

Ambiente di controllo	1. Dimostrare un «*commitment*» verso l'integrità e i valori etici. 2. Esercitare responsabilità di supervisione. 3. Definire strutture, poteri e responsabilità. 4. Dimostrare un «*commitment*» verso le competenze. 5. Rafforzare le responsabilità.
Risk Assessment	6. Specificare chiaramente gli obiettivi. 7. Individuare e valutare i rischi. 8. Valutare il rischio di frode. 9. Individuare e valutare i cambiamenti.
Attività di controllo	10.Individuare e implementare attività di controllo. 11.Individuare e implementare attività di controllo sui processi tecnologici. 12.Stabilire policy e procedure.
Informazione & comunicazione	13.Utilizzare informazioni rilevanti. 14.Comunicare internamente. 15.Comunicare esternamente.
Attività di monitoraggio	16.Eseguire verifiche continuative e/o singole. 17.Valutare e comunicare eventuali carenze.

Internal Environment
Risk Management Philosophy – Risk Culture – Board of Directors – Integrity and Ethical Values – Commitment to Competence – Management's Philosophy and Operating Style – Risk Appetite – Organizational Structure – Assignment of Authority and Responsibility – Human Resource Policies and Practices

Objective Setting
Strategic Objectives – Related Objectives – Selected Objectives – Risk Appetite – Risk Tolerance

Event Identification
Events –Factors Influencing Strategy and Objectives – Methodologies and Techniques – Event Interdependencies – Event Categories – Risks and Opportunities

Risk Assessment
Inherent and Residual Risk – Likelihood and Impact – Methodologies and Techniques – Correlation

Risk Response
Identify Risk Responses – Evaluate Possible Risk Responses – Select Responses – Portfolio View

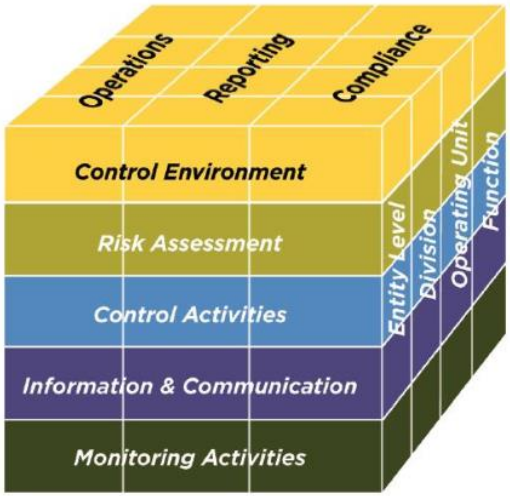
Control Activities
Integration with Risk Response – Types of Control Activities – General Controls – Application Controls – Entity Specific

Information and Communication
Information – Strategic and Integrated Systems – Communication

Monitoring
Separate Evaluations – Ongoing Evaluations

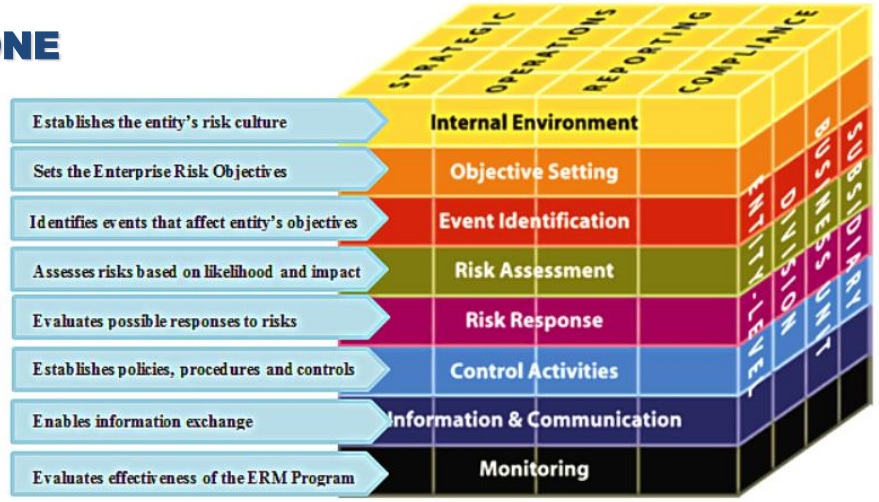
I PUNTI DI CONTATTO DELLA METODOLOGIA OPERATIVA CON I PRINCIPALI MODELLI INTERNAZIONALI (COSO, ERM, COBIT)

Il ***CoSO Report*** persegue **obiettivi operativi** (relativi all'efficacia e all'efficienza delle operazioni aziendali), **obiettivi di reporting finanziario** (relativi all'efficacia del sistema di reporting aziendale con riferimento all'informativa finanziaria) e **obiettivi di compliance** (relativi alla conformità delle attività aziendali rispetto alle leggi e regolamenti applicabili).



dal *CoSO Report (1992)*

EVOLUZIONE



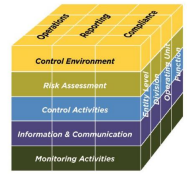
all'ERM (2004)

L'***ERM*** introduce **Obiettivi Strategici** da cui discendono gli obiettivi operativi, di reporting (di bilancio e previsionali) e di conformità.

GLI STRUMENTI DI RILEVAZIONE/ MISURAZIONE QUANTITATIVA DEGLI ELEMENTI DEL MODELLO

I PUNTI DI CONTATTO DELLA METODOLOGIA OPERATIVA CON I PRINCIPALI MODELLI INTERNAZIONALI (COSO, ERM, COBIT)

Differenziazioni



CoSO

CoSO Report	ERM
Ambiente di riferimento Si focalizza sull'insieme di standard, processi, strutture, integrità e valori etici che forniscono la base per la realizzazione di un sistema di controllo interno.	Generalizza il concetto all'Ambiente interno nel suo complesso enfatizzando gli aspetti culturali relativi alla consapevolezza della pervasività del rischio e della sua accettabilità.
Definizione degli obiettivi. Gli obiettivi di business e di governo sono dati a priori e non sono oggetto del processo di gestione dei rischi.	Partendo da obiettivi strategici dinamici e non predefiniti, determina l'esigenza di una ridefinizione dinamica degli obiettivi dell'organizzazione.
Processo di gestione dei rischi. Dinamico e continuativo per identificare e valutare i rischi che potrebbero compromettere il raggiungimento degli Obiettivi (livello di rischio tollerato),	Considera, oltre ai rischi puri, i **rischi – opportunità** e introduce un portafoglio di risposte al rischio che oltre alla minimizzazione prevede di poter evitare, condividere o accettare il rischio (quando tollerabile e accettabile).
Approccio al rischio. Controlla **rischi puri** offrendo come unica opzione di gestione la ricerca delle modalità più **efficienti** per **minimizzarli.**	Considera, oltre ai rischi puri, i **rischi – opportunità** e introduce un portafoglio di risposte al rischio che oltre alla minimizzazione prevede di poter evitare, condividere o accettare il rischio (quando tollerabile e accettabile).

ERM

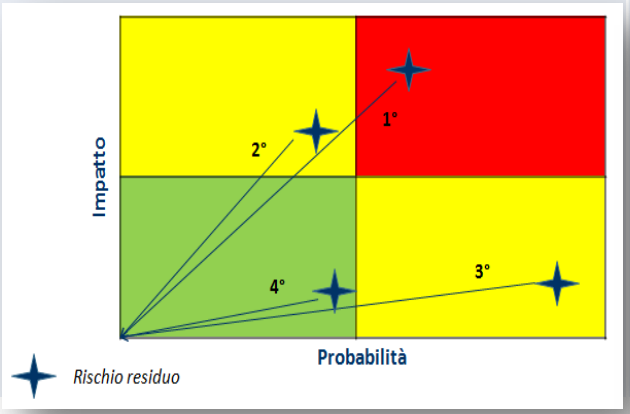
I PUNTI DI CONTATTO DELLA METODOLOGIA OPERATIVA CON I PRINCIPALI MODELLI INTERNAZIONALI (COSO, ERM, COBIT)

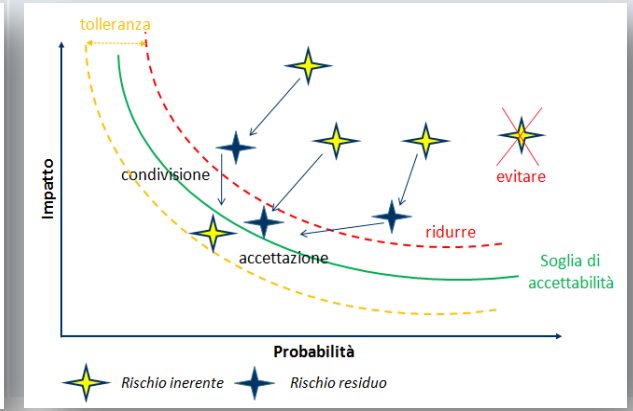
CoSO

Differenziazioni

ERM

CoSO Report	ERM
Prioritizzazione dei rischi. Focalizzazione sui rischi residui classificati in base a priorità e impatto per stabilire le priorità di controllo con l'unico limite rappresentato dall'onerosità del controllo.	Accettabilità, tollerabilità e risposta al rischio.



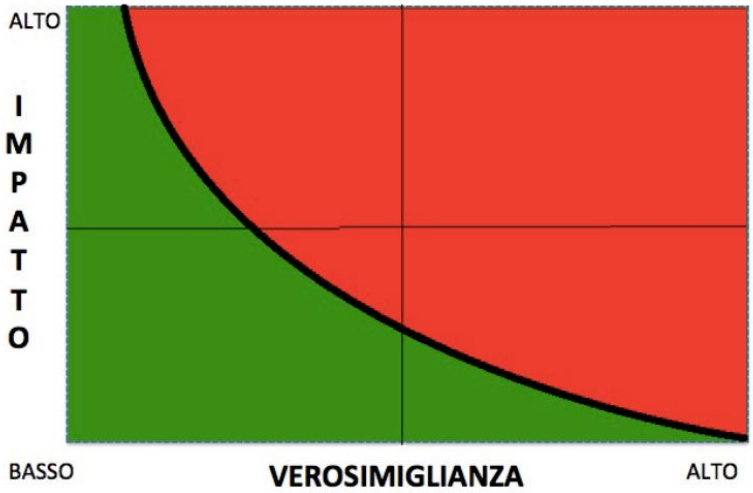


I PUNTI DI CONTATTO DELLA METODOLOGIA OPERATIVA CON I PRINCIPALI MODELLI INTERNAZIONALI (COSO, ERM, COBIT)

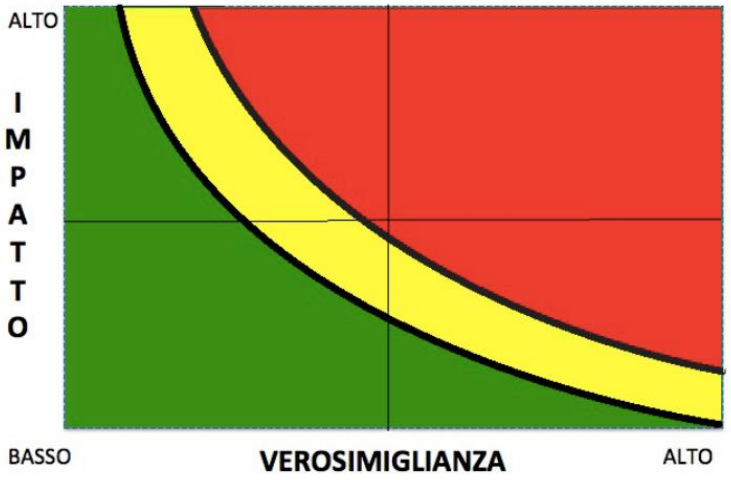
CoSO

Filosofia di fondo riguardo ai rischi

ERM



Propensione al rischio



Tolleranza al rischio

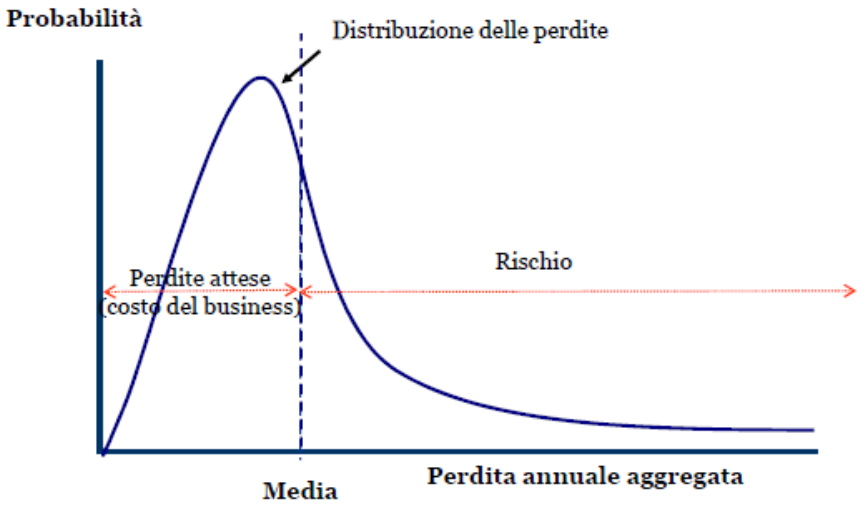
La tolleranza al rischio definisce l'area di gestione del rischio efficientemente gestibile da parte dell'impresa (*frontiera del rischio accettabile).*

I PUNTI DI CONTATTO DELLA METODOLOGIA OPERATIVA CON I PRINCIPALI MODELLI INTERNAZIONALI (COSO, ERM, COBIT)

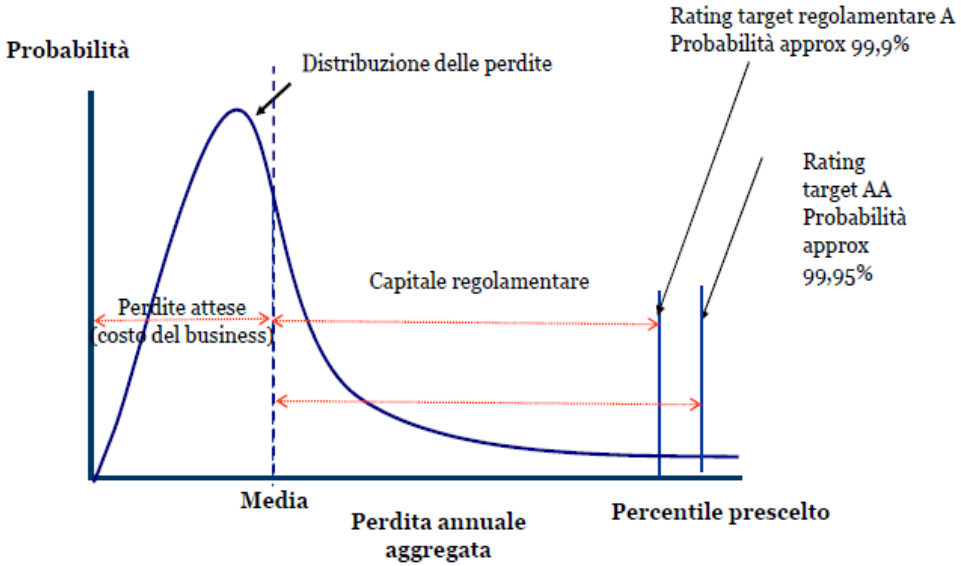
CoSO

Filosofia di fondo riguardo ai rischi

ERM



Propensione al rischio tradizionale



Propensione al rischio e allocazione di capitale

GLI STRUMENTI DI RILEVAZIONE/ MISURAZIONE QUANTITATIVA DEGLI ELEMENTI DEL MODELLO

I PUNTI DI CONTATTO DELLA METODOLOGIA OPERATIVA CON I PRINCIPALI MODELLI INTERNAZIONALI (COSO, ERM, COBIT)

CoSO

L'"ERM" assiste il management con lo scopo di comprendere i rischi aziendali e gestirli, permettendo di sviluppare le competenze interne necessarie per adottare le scelte migliori.

(COSO, 2006, "La gestione del rischio aziendale, ERM –Enterprise Risk Management: modello di riferimento e alcune tecniche applicative", il Sole 24 Ore)

ERM

Gestione dei rischi tradizionale	Enterprise Risk Management [ERM]
Rischi come pericoli individuali (visione settoriale)	Rischi valutati nel contesto delle strategie di business
Identificazione e assessment dei rischi	Sviluppo del "portafoglio dei rischi"
Focus su rischi discreti (parcellizzazione dei rischi)	Focus su rischi ***critici*** per l'organizzazione
Mitigazione dei rischi (visione solo negativa)	Ottimizzazione dei rischi (rischi anche come opportunità)
Soglia di rischio	Strategia di rischio
Rischi senza responsabilità	Assegnazione di responsabilità ("risk ownership")
Quantificazione dei rischi non sistematica	Monitoraggio e misurazione dei rischi
"Il rischio non è di mia competenza"	"La gestione dei rischi è di competenza di tutti"

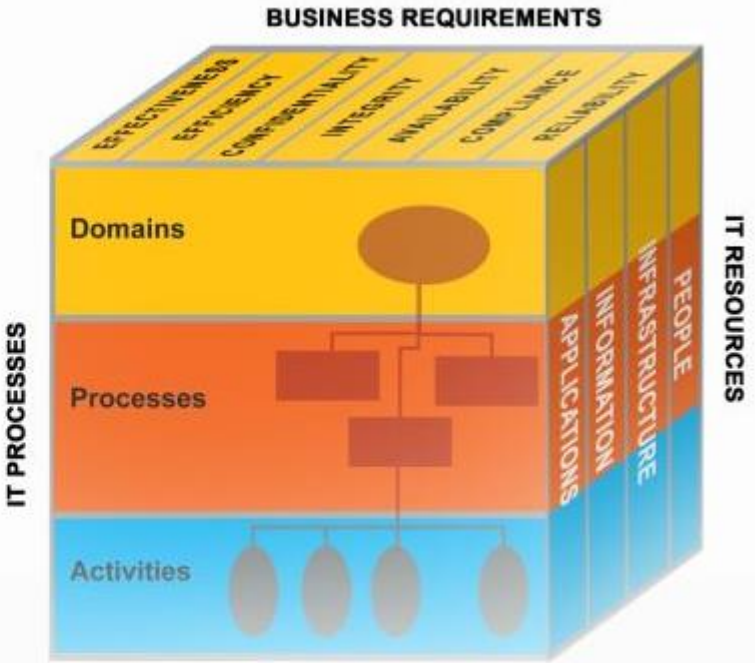
Fonte: C. Pomodoro e T. Luccini, 2012. Enterprise risk management e linee guida dello ISO 31000. Disponibile su <www.hspi.it>

I PUNTI DI CONTATTO DELLA METODOLOGIA OPERATIVA CON I PRINCIPALI MODELLI INTERNAZIONALI (COSO, ERM, COBIT)

La **VALUTAZIONE DEL SISTEMA DI CONTROLLO INTERNO** in base ai modelli di analisi vigenti si realizza comunemente con un approccio integrato che consideri gli aspetti qui evidenziati.

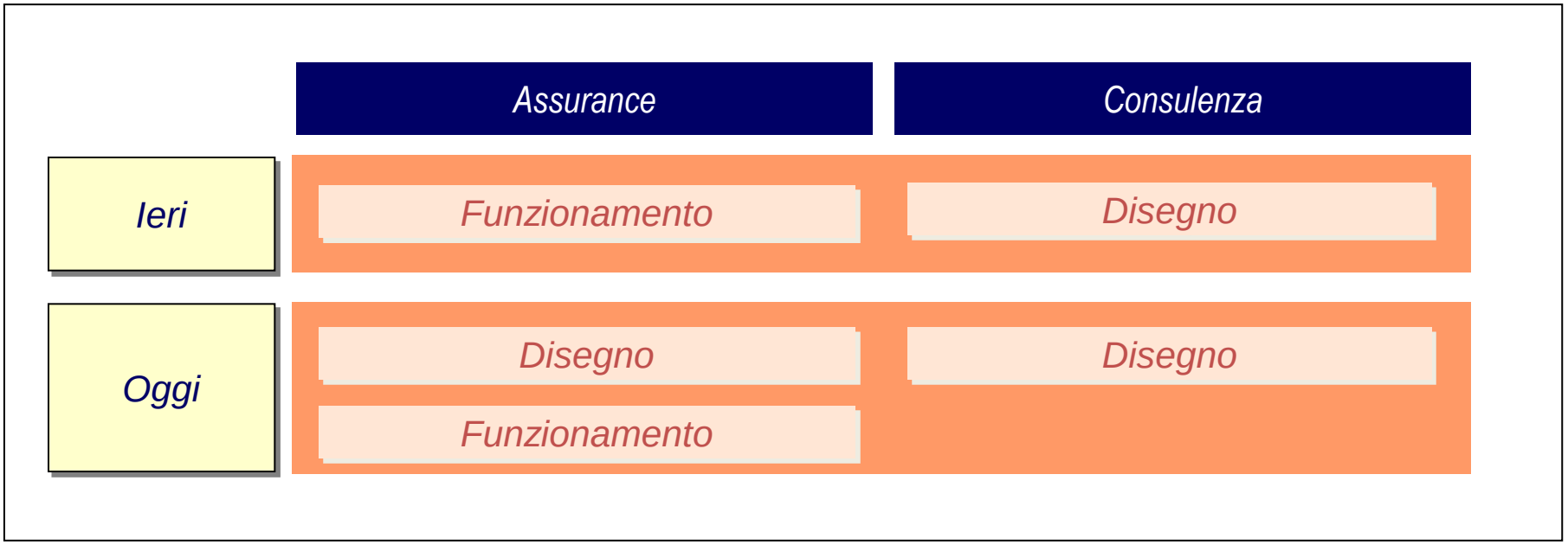
ERM

COBIT



Il ***CoSO Framework*** rimane il modello più diffuso e la sua combinazione con il ***COBIT Framework*** lo rende ancor più efficace ai fini delle analisi e dei riscontri.

L'EVOLUZIONE DELL'ATTIVITÀ DI CONTROLLO INTERNO



LA FORMULAZIONE DELLE VALUTAZIONI

Principi base del controllo

Principi base del controllo

- **Responsabilità**
- **Separazione delle funzioni e dei ruoli**
- **Autorizzazioni**
- **Tracciabilità**
- **Integrità e completezza**

LA FORMULAZIONE DELLE VALUTAZIONI

Principi base del controllo

Nessun sistema di controllo potrà mai funzionare se vengono meno i tre "pilastri" su cui esso si fonda:

Accountability

Principio organizzativo in base al quale qualsiasi attività faccia riferimento ad una persona, che ne sia "responsabile".

Occorre assicurare che non esistano "aree di nessuno".

Separazione dei compiti

Tecnica che consente di suddividere le operazioni afferenti al patrimonio, in modo tale da escludere che si possano verificare appropriazioni indebite, se non per il tramite di fenomeni collusivi.

Essa deve essere perseguita nel rispetto del principio di "proporzionalità" e quindi di equo rapporto costi-benefici.

Check-and-balance

Accorgimento organizzativo in base al quale si attribuiscono a certe funzioni aziendali obiettivi volutamente antagonisti, cioè a dire, di costituire una sorta di "dissenso organizzativo" volto a far si che le decisioni prese siano il risultato di riflessioni ponderate. Il C&B rappresenta un fattore di efficacia gestionale che non può essere gestito da burocrati, bensì da persone competenti e ragionevoli.

LA FORMULAZIONE DELLE VALUTAZIONI

Principi base del controllo

Responsabilità → ***Principio di "ACCOUNTABILITY"***

L'attribuzione delle responsabilità deve essere ispirata a criteri di efficienza organizzativa, identificazione dei ruoli, univocità del presidio delle attività attinenti al processo.

Separazione delle funzioni e dei ruoli → ***Principio di "SEPARATEZZA"***

Le responsabilità devono essere definite e distribuite evitando sovrapposizioni funzionali o allocazioni operative che concentrino le attività critiche, ai vari livelli della transazione, ed i successivi controlli, in un unico soggetto.

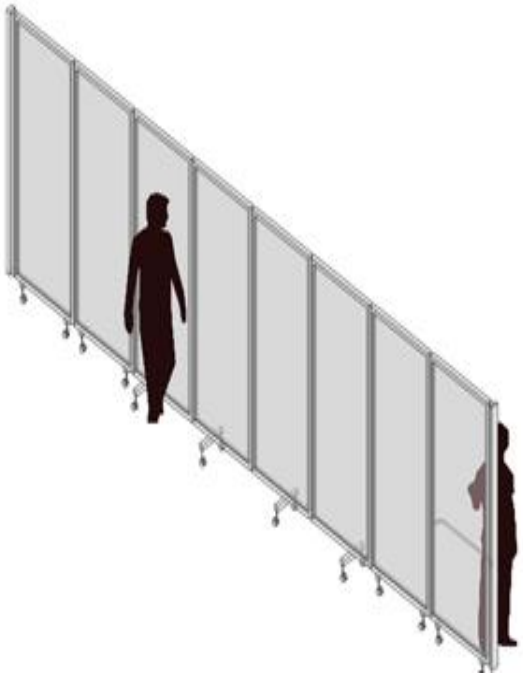
LA FORMULAZIONE DELLE VALUTAZIONI

Principi base del controllo

"SEPARATEZZA" dei compiti

IN AMBITO OPERATIVO

- ✓ **AUTORIZZAZIONE**
- ✓ **ESECUZIONE**
- ✓ **CUSTODIA FISICA**
- ✓ **REGISTRAZIONE**
- ✓ **RICONCILIAZIONE**



DEVONO ESSERE SEPARATE

E POSSIBILE ANCHE NEL RIPORTO.

LA FORMULAZIONE DELLE VALUTAZIONI

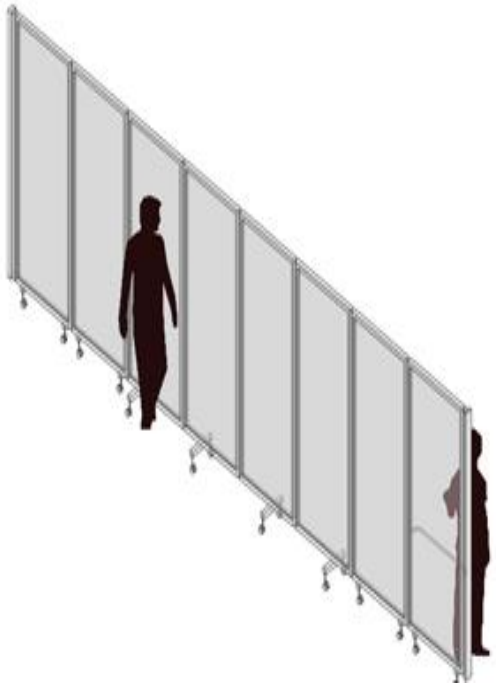
Principi base del controllo

"SEPARATEZZA" dei compiti

IN AMBITO INFORMATICO

SEPARARE

Dovrebbero essere persone diverse



- ✓ **ANALISTA SISTEMI**
- ✓ **PROGRAMMATORE**
- ✓ **OPERATORE**
- ✓ **DATA ADMINISTRATOR**
- ✓ **DATABASE ADMINISTRATOR**
- ✓ **NETWORK ADMINISTRATOR**
- ✓ **LIBRARIAN**
- ✓ **SECURITY ADMINISTRATOR**

Principi base del controllo

Autorizzazioni → ***Principio di "CHECK & BALANCE"***

Devono essere individuati specifici livelli autorizzativi o di supervisione commisurati alle caratteristiche e alla tipologia delle transazioni

Tracciabilità e verificabilità

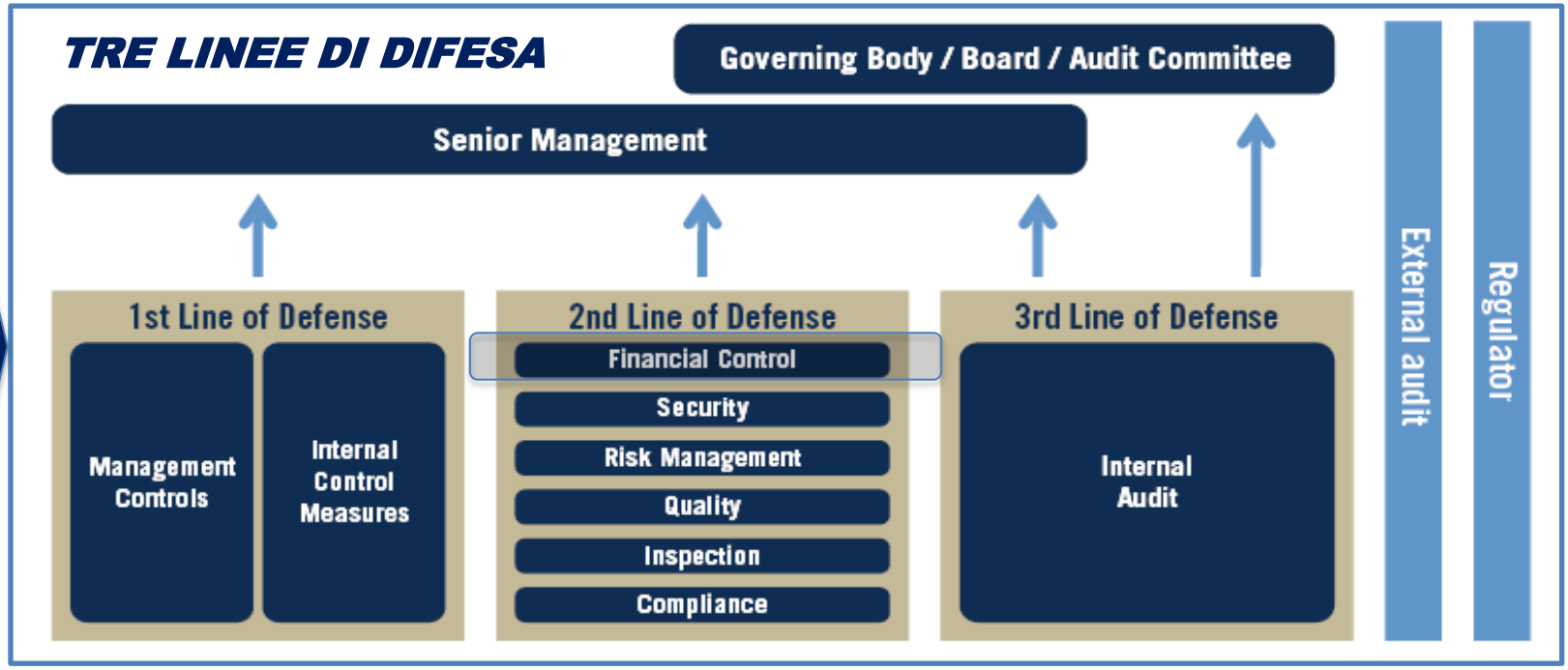
Le operazioni devono essere tracciabili in termini di scelte operative; deve essere previsto un adeguato supporto documentale per assicurare la verificabilità in termini di congruità, coerenza e responsabilità

Integrità e completezza dei dati

Devono essere garantiti meccanismi di controllo, di coerenza e riconciliazioni che assicurino l'integrità e la completezza dei dati gestiti

LA FORMULAZIONE DELLE VALUTAZIONI

Complessità S.C.I.



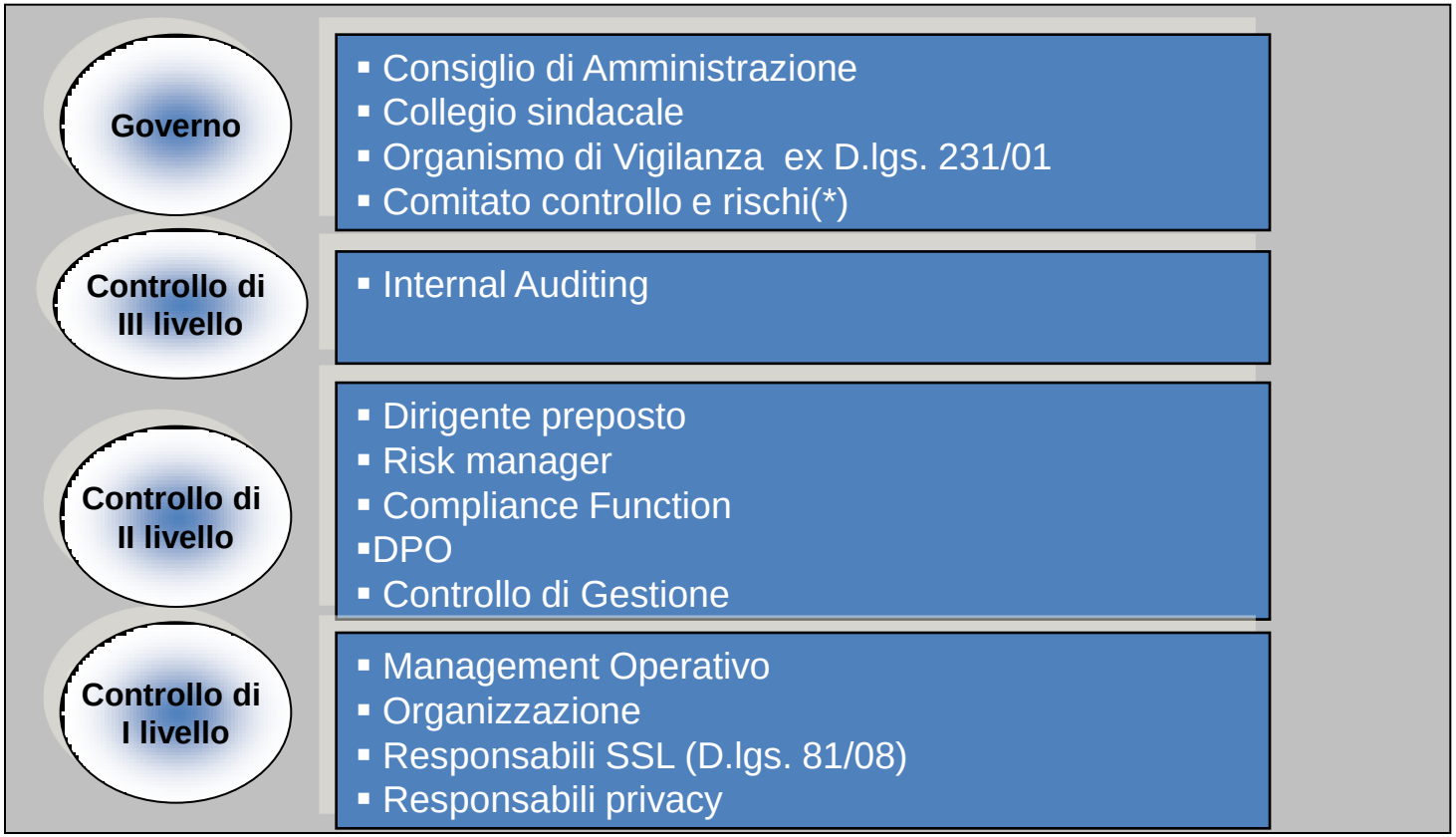
La legge 262/05 non disciplina in dettaglio le modalità di attuazione del Modello di Controllo, solo dall'esperienza di aziende italiane quotate in USA che hanno applicato la ***Sarbanes Oxley Act***, si possono trarre utili indicazioni.

FIRST LINE OF DEFENSE	SECOND LINE OF DEFENSE	THIRD LINE OF DEFENSE
Risk Owners/Managers	Risk Control and Compliance	Risk Assurance
• operating management	• limited independence • reports primarily to management	• internal audit • greater independence • reports to governing body

Fonte: IIA POSITION PAPER: THE THREE LINES OF DEFENSE IN EFFECTIVE RISK MANAGEMENT AND CONTROL

L'EVOLUZIONE DELL'ATTIVITÀ DI VALUTAZIONE

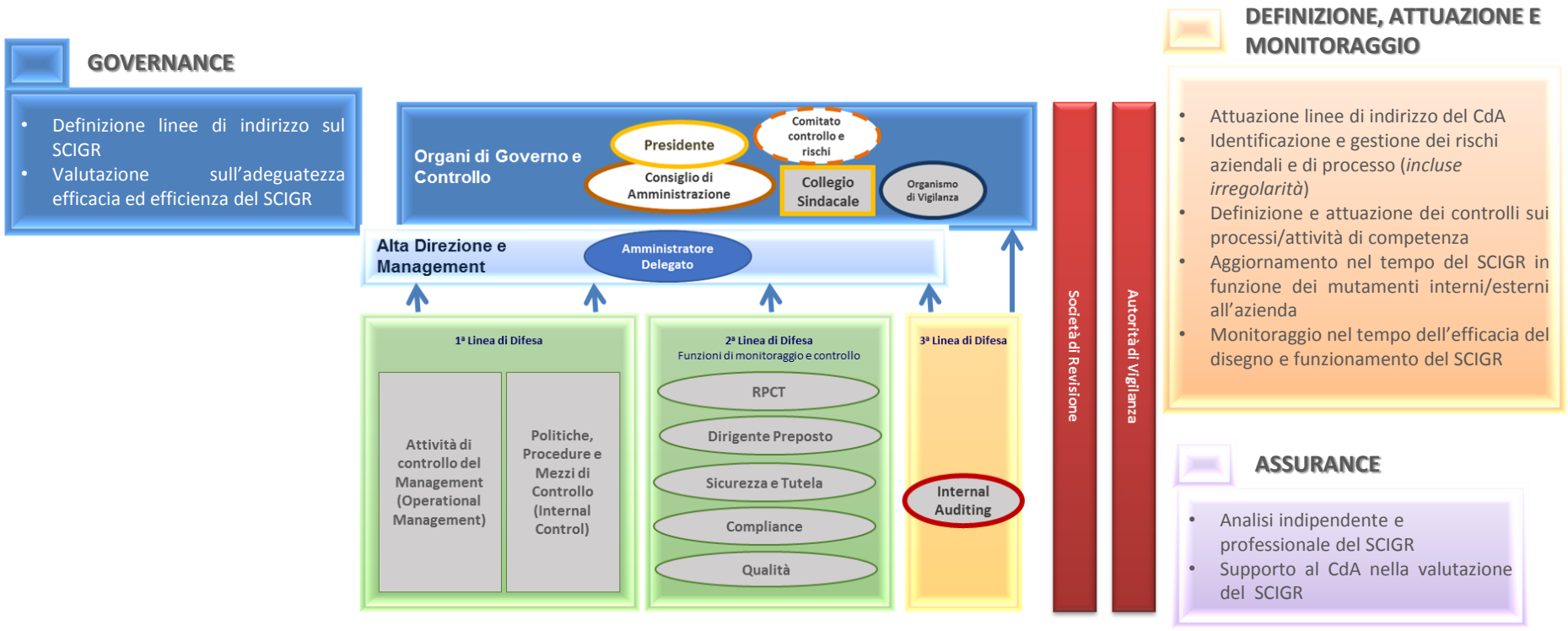
VALUTAZIONE DEL SISTEMA DI CONTROLLO INTERNO (SCI)



* Società quotate

L'EVOLUZIONE DELL'ATTIVITÀ DI VALUTAZIONE

I soggetti coinvolti nel SCI di un'organizzazione sono molteplici, ma la responsabilità ultima spetta al più alto livello gerarchico (chi ha un ruolo centrale in materia).



Gli organi di governo, nell'ambito della conduzione e della supervisione dell'attività di impresa, devono garantire una governance efficace del sistema integrato di gestione dei rischi e dei relativi controlli interni.


Good Job!
Grazie per l'attenzione