Il sistema di controllo interno
L'applicazione dei principi del CoSO 2013-

Introduzione al CoSO Report 2013

Dott.ssa Simona Pastorino

AGENDA

1. L’evoluzione del “framework“
2. I motivi dell’aggiornamento
3. Le principali novità introdotte

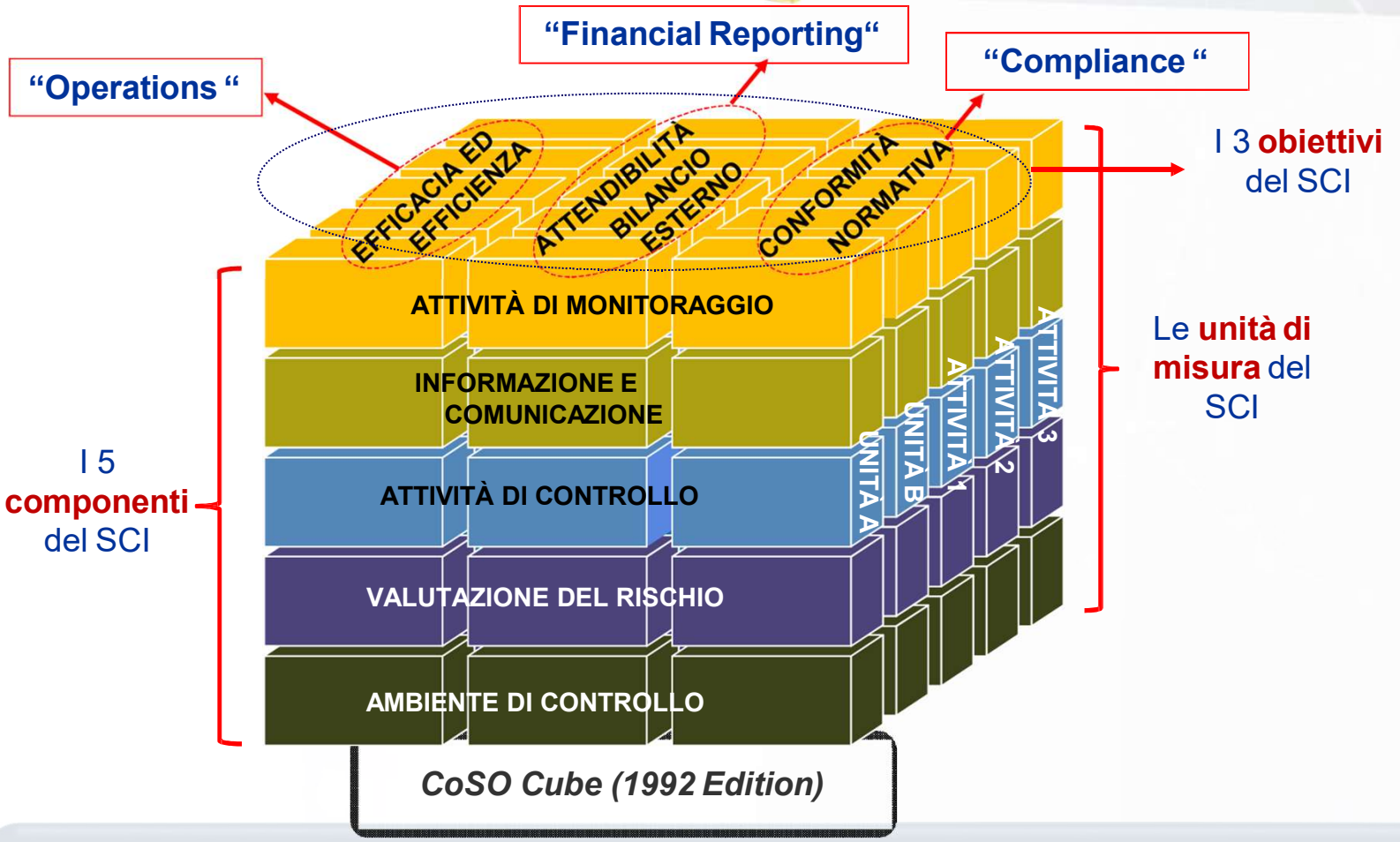
L'evoluzione del "framework"

CoSO = The Committee of Sponsoring Organizations of the Treadway Commission

È un'organizzazione privata indipendente costituita nel 1985 in USA, dalle **5 principali organizzazioni** della professione contabile e di internal auditors americane, finalizzata a migliorare la qualità dell'informativa economico-finanziaria, in risposta agli scandali economico – finanziari accaduti negli anni 70-80.

Tale comitato redige, con la supervisione di Coopers & Lybrand nel 1992, il documento definito "*Internal Control - Integrated Framework*" definito "*CoSO IC-IF 1992*", "*CoSO Cube 1992*" o "*CoSO 1*".

L'evoluzione del "framework"



Tale documento è diventato nel tempo, il più utilizzato ed avanzato «**standard**» di riferimento sia per le società che per i revisori esterni, **per valutare l'adeguatezza del sistema di controllo interno (SCI)**, con particolare riferimento all'informativa economico – finanziaria.

CoSO 1992 Originario

COSO's *Internal Control–Integrated Framework* (Edizione 1992)

Aggiornamento degli obiettivi ("Refresh Objectives")

Rifllessi i cambiamenti sia operativi che di business dell'ambiente di riferimento

Incrementati gli obiettivi "operations" e di "reporting"

Dettagliati in modo più analitico i principi di un efficace SCI (17 Principi)

Miglioramento ("Enhancements")

Aggiornato il contesto di riferimento

Incrementate le applicazioni

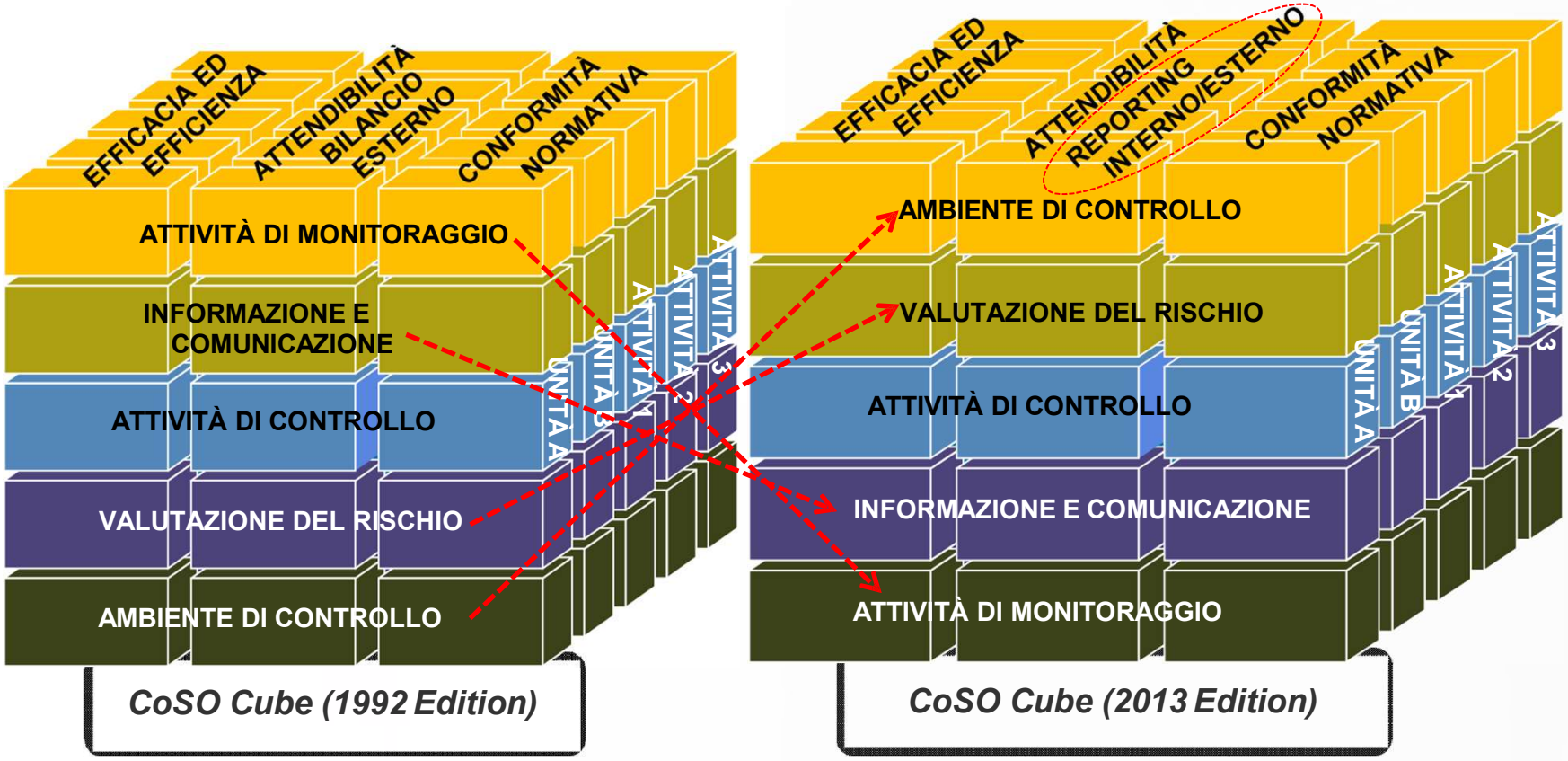
Chiariti meglio i principi di riferimento (Introduzione dei punti di attenzione – *"point of focus"*)

CoSO 2013 Aggiornato

COSO's *Internal Control–Integrated Framework* (Edizione 2013)

Il contesto di riferimento, notevolmente mutato rispetto al 1992, è il principale "*driver*" del cambiamento del "*framework*":

- **globalizzazione e interdipendenza dei mercati;**
- **maggiore complessità dei modelli di riferimento dei business;**
- **adempimenti normativi sempre più numerosi e stringenti;**
- **governance quale elemento imprescindibile per l'implementazionee la gestione di un SCI efficace;**
- **maggiore attenzione agli approcci «risk based»;**
- **accresciuto ruolo assunto dalla tecnologia;**
- **aspettative di prevenire e scoprire le frodi:**
- **accresciuta importanza delle «*non financial information*».**



Che cosa è cambiato e cosa invece non si è modificato?

1. La definizione di SCI

2. La propria familiarità del "Cube":

- Le finalità sono rappresentate dalle colonne
- I componenti sono rappresentati dalle righe
- Gli obiettivi sono definibili a livello di "legal entity", divisione, funzione, unità etc.

3. I criteri utilizzati per valutare l'efficacia di un SCI

4.Il significativo ruolo svolto dalla competenza professionale "judgment" nel "disegnare", "implementare" e "valutare" l'efficacia di un SCI ("*Tailored made approach*").

I 17 principi

1^ NOVITÀ

L'ARTICOLAZIONE DEI 17 PRINCIPI PER L'ADEGUATO FUNZIONAMENTO DI UN EFFICACE SCI SECONDO IL COSO 2013

Ambiente di controllo "AC" (5 principi)	1. Rispetto dei valori etici e di integrità 2. Attività di supervisione del Board e del Senior Management 3. Struttura organizzativa, linee di riporto, deleghe poteri e responsabilità 4. Orientamento alla "competenza" delle risorse aziendali 5. Responsabilizzazione del personale aziendale
Valutazione del rischio ("VR") (4 principi)	6. Definizione di chiari obiettivi da perseguire 7. Identificazione e analisi dei rischi 8. Valutazione dei rischi di frode 9. Identificazione ed analisi del cambiamento
Attività di controllo ("ATC") (3 principi)	10. Identificazione e sviluppo di adeguate attività di controllo 11. Identificazione e sviluppo di adeguate attività di "IT control" 12. Sviluppare e definire adeguate policy e procedure aziendali di controllo
Informazione e comunicazione ("IC") (3 principi)	13. Utilizzo di informazioni affidabili e rilevanti 14. Adeguate comunicazioni interne 15. Adeguate comunicazioni esterne
Attività di monitoraggio ("AM") (2 principi)	16. Monitoraggio continuo e/o indipendenti valutazioni 17. Valutazione, comunicazione e correzione delle carenze del SCI

I 17 principi hanno lo scopo di illustrare i requisiti obbligatori di ogni componente del SCI, al fine di garantire l'esistenza di un adeguato funzionamento del SCI («*present and functioning*»)

Ogni principio è «adattabile» ad ogni realtà aziendale, ma vige una presunzione di «rilevanza» in ognuno di essi. Rare dovrebbero essere cioè le casistiche aziendali nelle quali un principio non sia significativo e quindi non applicabile.

Tutti i principi e quindi i 5 componenti devono essere presenti e funzionare in modo integrato («*integrated manner*»).

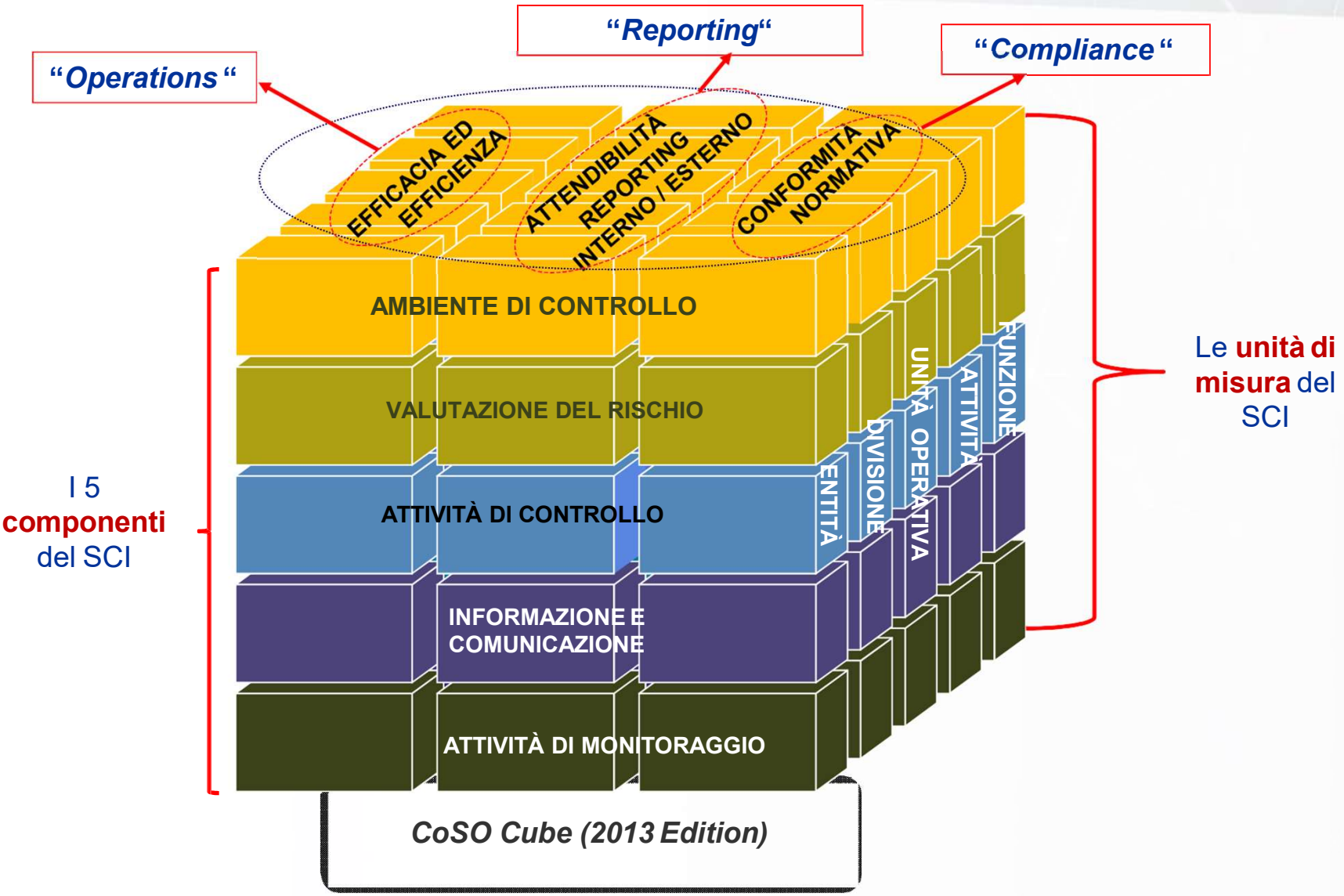
Il sistema di controllo interno
-L’applicazione dei principi del CoSO 2013-

Il Sistema di Controllo interno

Definizione e obiettivi

AGENDA

1. La definizione di SCI
2. Gli obiettivi:
   - Efficacia ed efficienza operativa («Operations»)
   - Attendibilità del reporting interno ed esterno
   - Conformità alle normative di legge e volontarie


"Operations"
"Reporting"
"Compliance"
EFFICACIA ED EFFICIENZA
ATTENDIBILITÀ REPORTING INTERNO / ESTERNO
CONFORMITÀ NORMATIVA
AMBIENTE DI CONTROLLO
VALUTAZIONE DEL RISCHIO
ATTIVITÀ DI CONTROLLO
INFORMAZIONE E COMUNICAZIONE
ATTIVITÀ DI MONITORAGGIO
ENTITÀ
DIVISIONE
UNITÀ OPERATIVA
ATTIVITÀ
FUNZIONE
I 5 componenti del SCI
Le unità di misura del SCI
CoSO Cube (2013 Edition)

Il Sistema di Controllo Interno (SCI) è costituito dall'insieme di **strumenti/regole/procedure** informative e organizzative disegnate e operanti allo scopo di consentire - sia preventivamente sia a consuntivo – l'indirizzo ed il monitoraggio delle performance aziendali in relazione al perseguimento degli obiettivi definiti dall'Alta Direzione.

- è un ***processo***. Non è la compilazione di mere check list. È un mezzo non il fine di un'attività di controllo;
- è effettuato da ***persone***. Non è solo costituito da manuali e procedure. Esso riguarda il *comportamento* delle *risorse personali* (non sono *interne*) di un'organizzazione;
- mira al raggiungimento di obiettivi più o meno ***interdipendenti*** tra di loro. Attenzione al fenomeno di ***"overlapping categories"***. Non è la burocratica applicazione di procedure;
- garantisce solo in merito alla ***"reasonable assurance"*** da parte del management che la società abbia operato nel rispetto delle procedure e degli obiettivi preposti. Non può dare garanzie di successo assoluto al 100% «*no absolute assurance*».

OGNI SCI PERSEGUE I SEGUENTI 3 OBIETTIVI GENERALI:

1. Economicità (Operations) delle operazioni di gestione, la quale implica:
   - efficacia nel raggiungimento degli obiettivi economici;
   - efficienza in termini di minor consumo di risorse per il perseguimento degli obiettivi.
2. Attendibilità (Reporting) del Sistema Informativo Aziendale (SIA), la quale implica:
   - a fini interni: che il SIA costituisca il presupposto di conoscenze che supportano il sistema delle decisioni aziendali (SIA come supporto alle decisioni);
   - a fini esterni: che il SIA alimenti la produzione di report oggetto di valutazioni autonome (SIA come supporto alla redazione del bilancio e di altre informative esterne).
3. Conformità alle normative (Compliance), poiché nello svolgimento delle operazioni di gestione occorre che siano rispettate le normative applicabili, siano esse:
   - di provenienza legislativa (civilistica, fiscale, penale, ambientale, sicurezza su lavoro, privacy, normative di prodotto/settore, ecc.);
   - appartenenti a sistemi "volontari" (certificazione qualità, norme etiche, ecc.).

Gli Obiettivi del SCI (2)

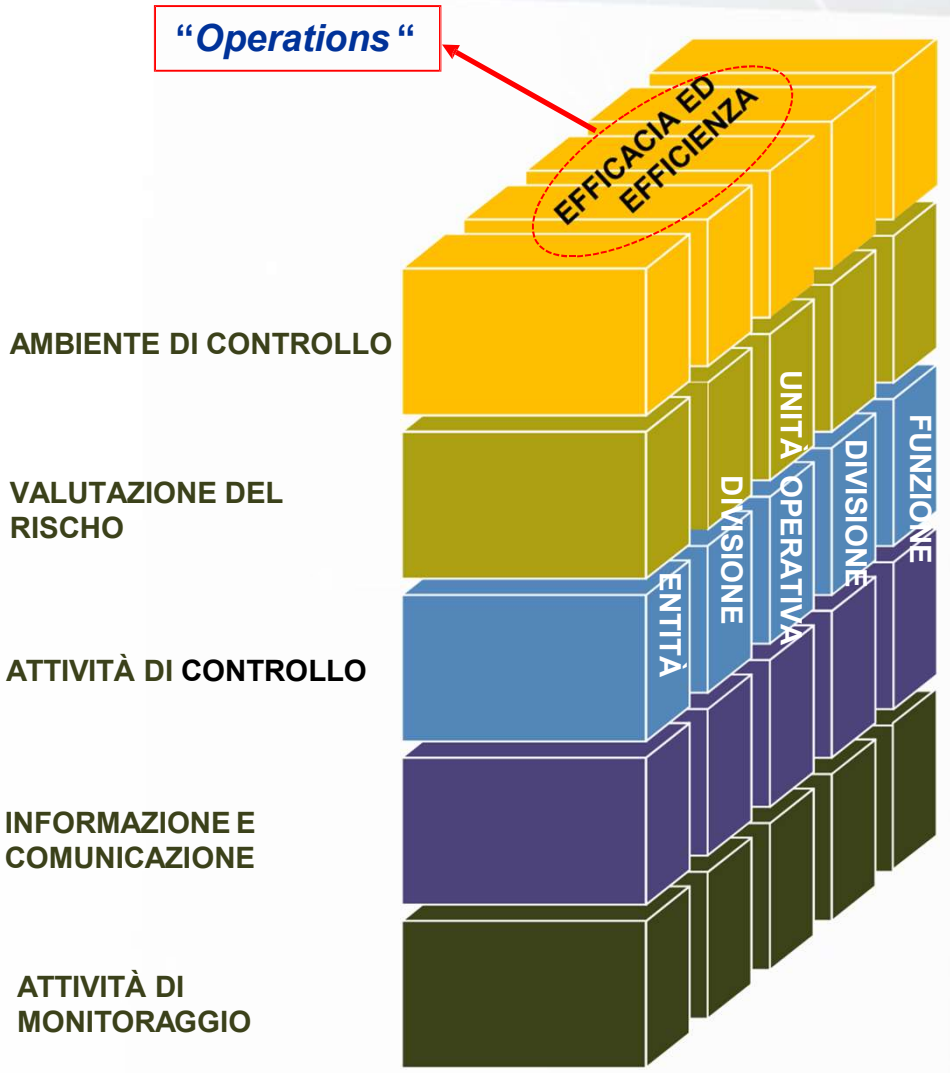
- Pertanto il SCI agevola il perseguimento degli obiettivi aziendali (indirizzo e vigilanza)
- Il mancato perseguimento degli obiettivi aziendali può comportare il verificarsi di "danni" qualificabili come:
  1. Perdite economiche (reddituali/patrimoniali e distruzione di valore) nel caso del mancato raggiungimento degli obiettivi di economicità (inefficacia e/o inefficienza).
  2. Perdite economiche nel caso di un Sistema Informativo Aziendale (SIA) che produce informazioni inattendibili, derivanti da:
     1. cattive performance a seguito di decisioni assunte sulla base di informazioni errate (SIA come supporto alle decisioni);
     2. sanzioni correlate alla produzione di bilanci ed altre informative esterne inattendibili (SIA come supporto all'informativa esterna).
  3. Perdite economiche derivanti direttamente o indirettamente da sanzioni causate dal mancato rispetto della normativa.
- Il SCI, quindi, presidia la minimizzazione di perdite economiche.

Operations: riguardano l'utilizzo **efficace** ed **efficiente** delle risorse aziendali:

- Immobilizzazioni
- Personale
- Disponibilità liquide
- Reputazione
- Capacità produttiva etc.

L'adeguatezza del SCI in merito all'efficienza operativa può ritenersi raggiunta se:

l'alta direzione e il senior management hanno la "*reasonable assurance*" di aver ben compreso il **grado di economicità** con cui sono state raggiunte le principali performance operative.



Le “*operations*” dipendono dal particolare business in cui opera la società.
Sono molto legati alla “pressione competitiva” (qualità, cicli di produzione, cambiamenti tecnologici etc.)

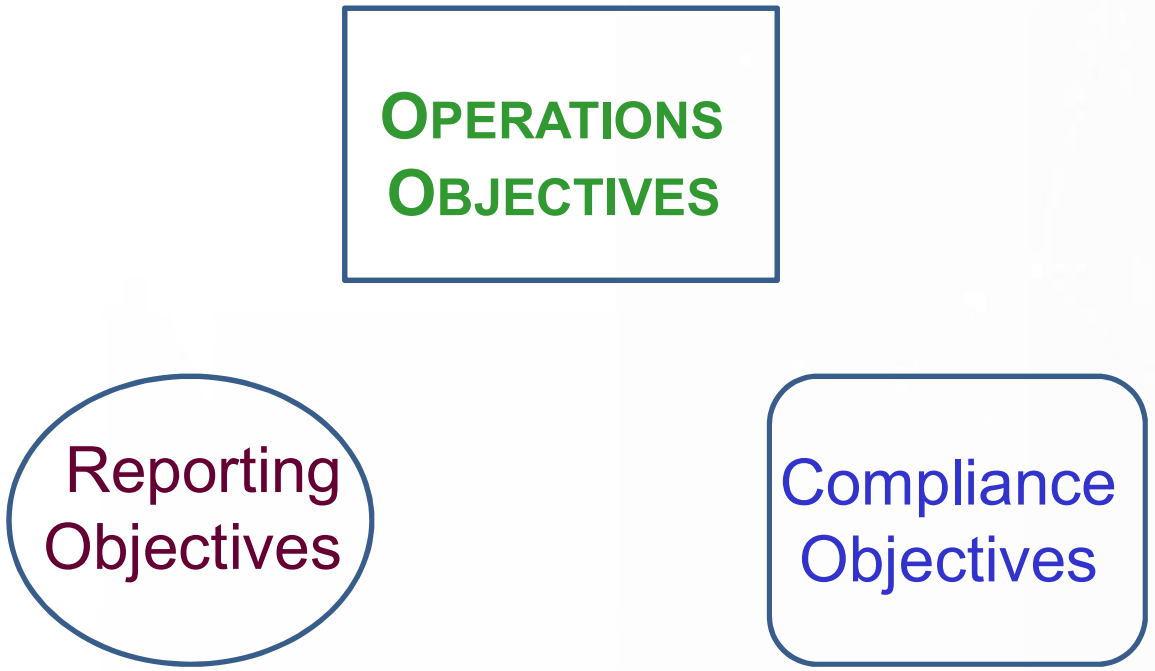
Riguarda **l'attendibilità sostanziale** della reportistica aziendale sia interna che esterna "**finanziaria**" e "**non finanziaria**".

Nel Framework 2013, questo obiettivo viene "**ampliato**" comprendendo, (rispetto alla versione del 1992) anche l'informativa **INTERNA** (non solo quella esterna).
Viene inoltre enfatizzato il ruolo che sta sempre più prendendo piede dalle "***non financial information***".

Rispetto delle **norme di legge** e dei **regolamenti** anche di natura **volontaria.**

Viene evidenziata sempre più l'importanza oltre che del rispetto della legge, anche al rispetto di normative volontarie ("codici di autodisciplina", di "legalità" , di "leading practises" etc.

Vale l'assunto: "***Say what you do, do what you say***".


OPERATIONS OBJECTIVES
Reporting Objectives
Compliance Objectives

IL SCI È COSTITUITO DALL'INSIEME DELLE REGOLE, DELLE FUNZIONI, DELLE STRUTTURE, DELLE RISORSE, DEI PROCESSI E DELLE PROCEDURE CHE MIRANO AD

assicurare, nel rispetto della sana e prudente gestione, il conseguimento delle seguenti finalità:

- **verifica dell'attuazione delle strategie e delle politiche aziendali;**
- **contenimento del rischio entro i limiti indicati nel quadro di riferimento per la determinazione della propensione al rischio della banca (RAF);**
- **salvaguardia del valore delle attività e protezione delle perdite;**
- **efficacia ed efficienza dei processi aziendali;**
- **affidabilità e sicurezza delle informazioni aziendali e delle procedure informatiche;**
- **prevenzione del rischio che la banca sia coinvolta, anche involontariamente, in attività illecite (riciclaggio, usura e finanziamento terrorismo);**
- **conformità delle operazioni con la legge, la normativa di vigilanza nonché con le politiche, i piani, i regolamenti e le procedure interne**

I SOGGETTI INTERESSATI ALLA VALUTAZIONE DEL SCI

Gli attori del sistema

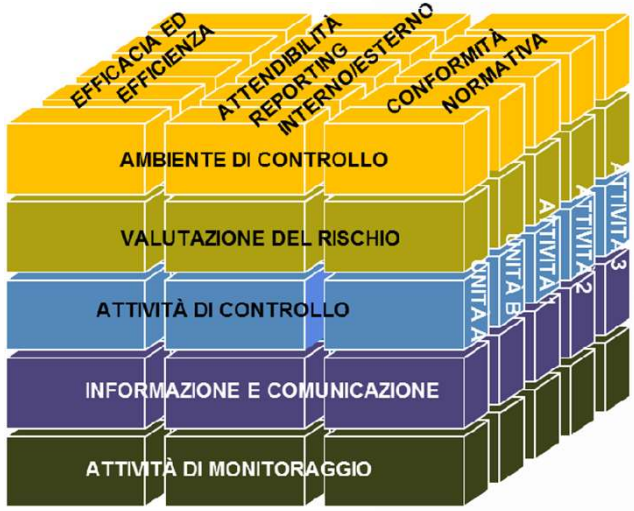
OdV
(Vigila su adeguatezza ed effettività del sistema «**231**»)

Internal Audit
(Verifica su adeguatezza ed effettivo funzionamento del sistema nel suo complesso»)

Collegio Sindacale
(Vigila sull'efficacia del sistema)

Revisore
(Valuta l'attendibilità sostanziale del sistema amministrativo - contabile)

Organi di Vigilanza
(Monitora su adeguatezza ed effettività del sistema)



CoSO Cube (2013 Edition)

Il Board
(Definisce indirizzo e valuta l'adeguatezza del sistema)

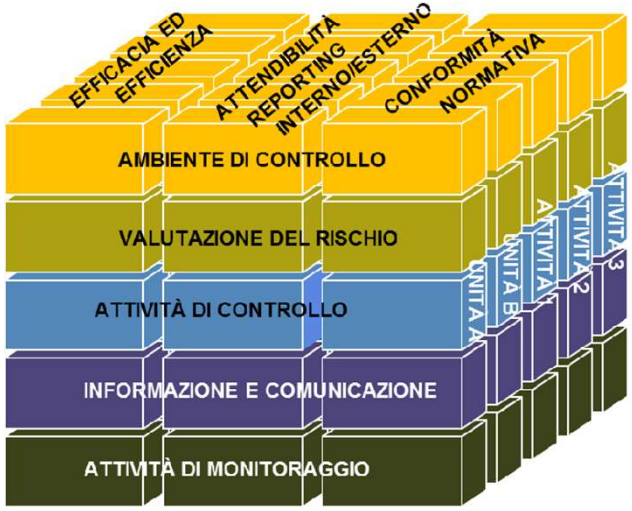
Amministratore Delegato (incaricato)
(Implementazione del Sistema e mantenimento della sua efficacia)

Comitato Controllo e Rischi
(Supporta il Board mediante adeguata istruttoria)

Management (Process/Risk owner)

Altre funzioni aziendali (compliance – risk management etc.)
(Specifiche competenze)

24



CoSO Cube (2013 Edition)

- ✓ Il **disegno** di un Sistema di Controllo Interno è di competenza del **Management** della società

- ✓ L'**applicazione** di un Sistema di Controllo Interno è di competenza di **tutte le risorse** aziendali

- ✓ Il **monitoraggio** di un Sistema di Controllo Interno è di competenza degli **Organi di Controllo e di Vigilanza**

- L'affermazione che il SCI risponde ad un fabbisogno di controllo, ovvero ad un fabbisogno di contenere / minimizzare eventuali perdite economiche connesse a performance insufficienti a livello di economicità, attendibilità e conformità, implica la necessità di:
  - valutare preventivamente l'eventualità (rischio) di incorrere in perdite economiche significative, ovvero la vulnerabilità dei singoli sottosistemi aziendali;
  - valutare il diverso grado di affidabilità dei SCI riferiti ai singoli sottosistemi aziendali;
  - valutare che il diverso grado di affidabilità (e quindi di onerosità) dei SCI, sia correlato alla effettiva esistenza (probabilità) e gravità (impatto) dei rischi di subire perdite economiche nei diversi sottosistemi aziendali (economicità del SCI);
  - correlare le valutazioni di rischio di perdite significative e di affidabilità dei SCI mediante valutazioni quantitative fondate sulle tecniche dell' analisi costi-benefici.
- Tutto ciò riflette la nozione di SCI come sistema flessibile ("un abito su misura") che deve essere strutturato in relazione alle necessità specifiche dell' azienda e dei sottosistemi che la compongono

RISK ASSESSMENT E CONTROLLI INTERNI

ERM – Framework e razionali

IL SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI (SCIGR)

Modelli di gestione più recenti sottolineano la centralità del rischio nel sistema dei controlli: l'ultima versione del Codice di Autodisciplina ne ha riconosciuto ed enfatizzato l'importanza. Il Codice di Autodisciplina fa riferimento a un sistema di controllo interno e di gestione dei rischi come a un sistema unitario in cui il rischio rappresenta il filo conduttore.

La definizione di SCIGR del Codice di Autodisciplina "Ogni emittente si dota di un sistema di controllo interno e di gestione dei rischi costituito dall'insieme delle ***regole, delle procedure e delle strutture organizzative volte a consentire l'identificazione, la misurazione, la gestione e il monitoraggio dei principali rischi****."*

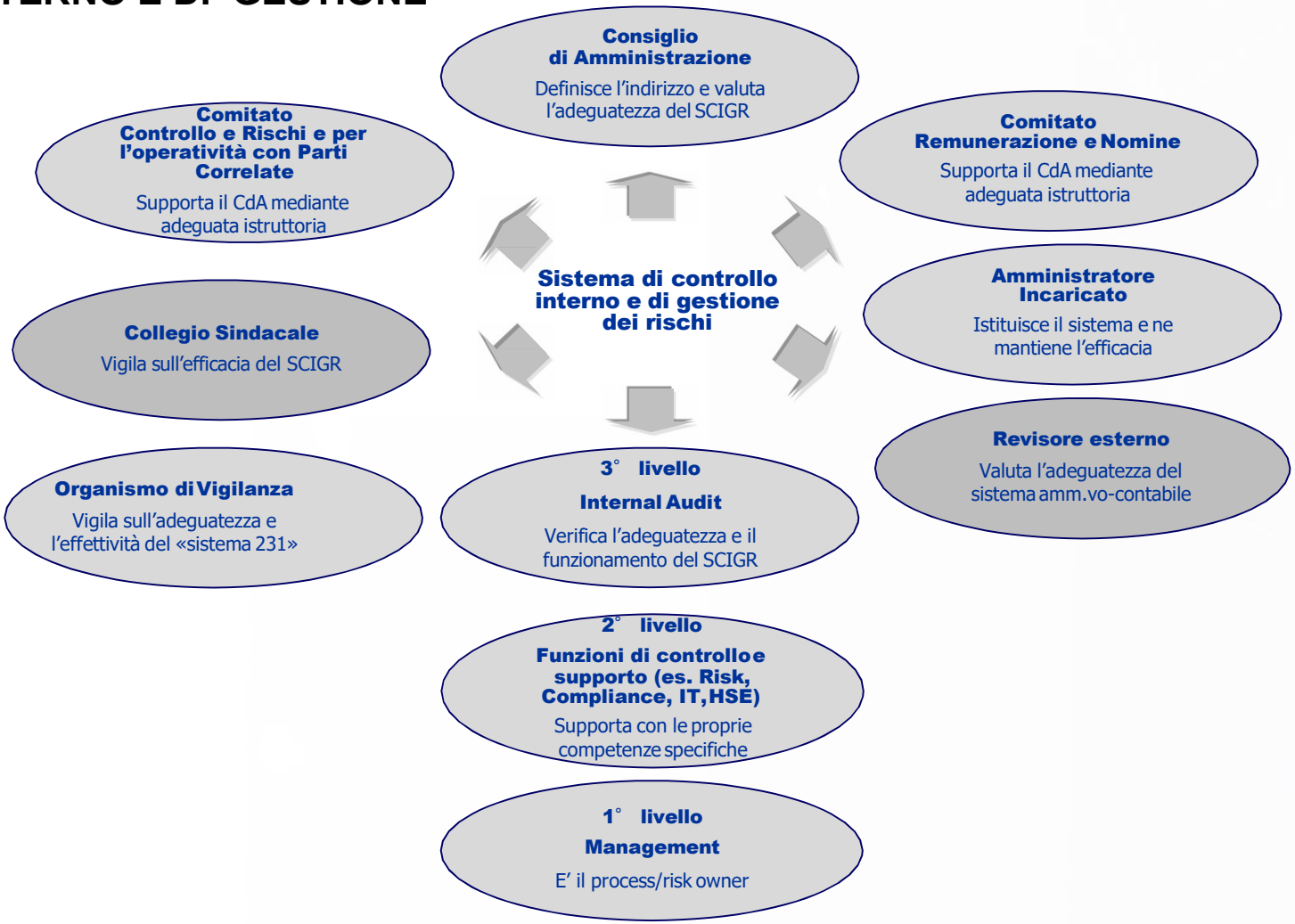
IL SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI (SCIGR)

Obiettivi del SCIGR

"Un efficace sistema di controllo interno e di gestione dei rischi contribuisce a una conduzione dell'impresa coerente con gli obiettivi aziendali definiti dal consiglio di amministrazione, favorendo l'assunzione di decisioni consapevoli. Esso concorre ad assicurare:

- la salvaguardia del patrimonio sociale,
- l'efficienza e l'efficacia dei processi aziendali,
- l'affidabilità dell'informazione finanziaria,
- il rispetto di leggi e regolamenti nonché dello statuto sociale e delle procedure interne."

GLI ATTORI DEL SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI



RISCHIO E INCERTEZZE

Risk is uncertainty that matters

Obiettivi
definiscono ciò che rileva

- *Risk is the effect of uncertainty on objectives. An effect is a deviation from the expected - positive and/or negative (ISO 31000:2009)*

- *"Risk is an uncertain event or condition that, if it occurs, has a positive or negative effect on an objective" (Association of Project Manager, 2013)*

Rischio collega le incertezze agli obiettivi
Rischio include sia opportunità che minacce

DIMENSIONI RILEVANTI DEL RISCHIO

Variabili da misurare

- PROBABILITA' - incertezza
- IMPATTO – effetto sugli obiettivi

R = P x I

1. *Che genere di incertezza?*
2. *Che tipo di effetti («mattering»)?*

CHE GENERE DI IMPATTO RILEVA?

Impatto misurato rispetto agli obiettivi – Quale effetto rileva?

- Può essere positive o negativo
- Incertezza che **aiuta** ma anche incertezza che **danneggia**

Opportunità e Minacce sono entrambe considerate

QUALI OBIETTIVI?

- Ogni obiettivo può essere influenzato da rischi (+/-) :
  - Shareholder value
  - Profittabilità / EBITDA
  - Performance tecnica
  - Costi
  - Compliance regolamentare
  - Customer satisfaction
  - Reputazione
  - Health and Safety

- Tutti gli obiettivi corporate sono «in scope»
- Impatti positivi e negativi (opportunità e minacce)

CHE TIPO DI INCERTEZZE?*

- **Stochastic** uncertainty, anche nota come **event risk**
- **Aleatory** uncertainty , anche nota come **variability risk**
- **Epistemic** uncertainty, anche nota come **ambiguity risk**
- **Ontological** uncertainty, anche nota come **emergent risk**

D. Hillson

EVENT RISK

Eventi futuri incerti che possono accadere o non accadere

- Esempi:
  - Shut-down del sistema IT
  - Perdita di risorsa critica quando serve
  - Danni a un prodotto

- Gestiti con processo standard di risk management
  - Identificare, analizzare, pianificare e implementare risposte

VARIABILITY RISK

Alcuni eventi futuri con caratteristiche variabili. **L'incertezza non risiede nell'evento ma nel valore**

- Esempi:
  - La sperimentazione può prendere più tempo del previsto
  - La produttività può essere sopra o sotto il target
  - I costi delle materie prime possono crescere o diminuire
  - Il tasso di cambio può muoversi al rialzo o al ribasso

- Analizzati e gestiti attraverso analisi di rischio quantitative

AMBIGUITY RISK

Alcuni eventi futuri con caratteristiche **ambigue**

- Esempi:
  - Come reagiranno i concorrenti al lancio del nostro nuovo prodotto?
  - Nuove regolamentazioni sono attese ma non è noto l'impatto
  - Clienti domandano l'uso di nuova tecnologia che è oltre la nostra capacità

- Identificati e gestiti attraverso sperimentazione ed esperti
  - benchmarking, input da esperti, analisi di scenario

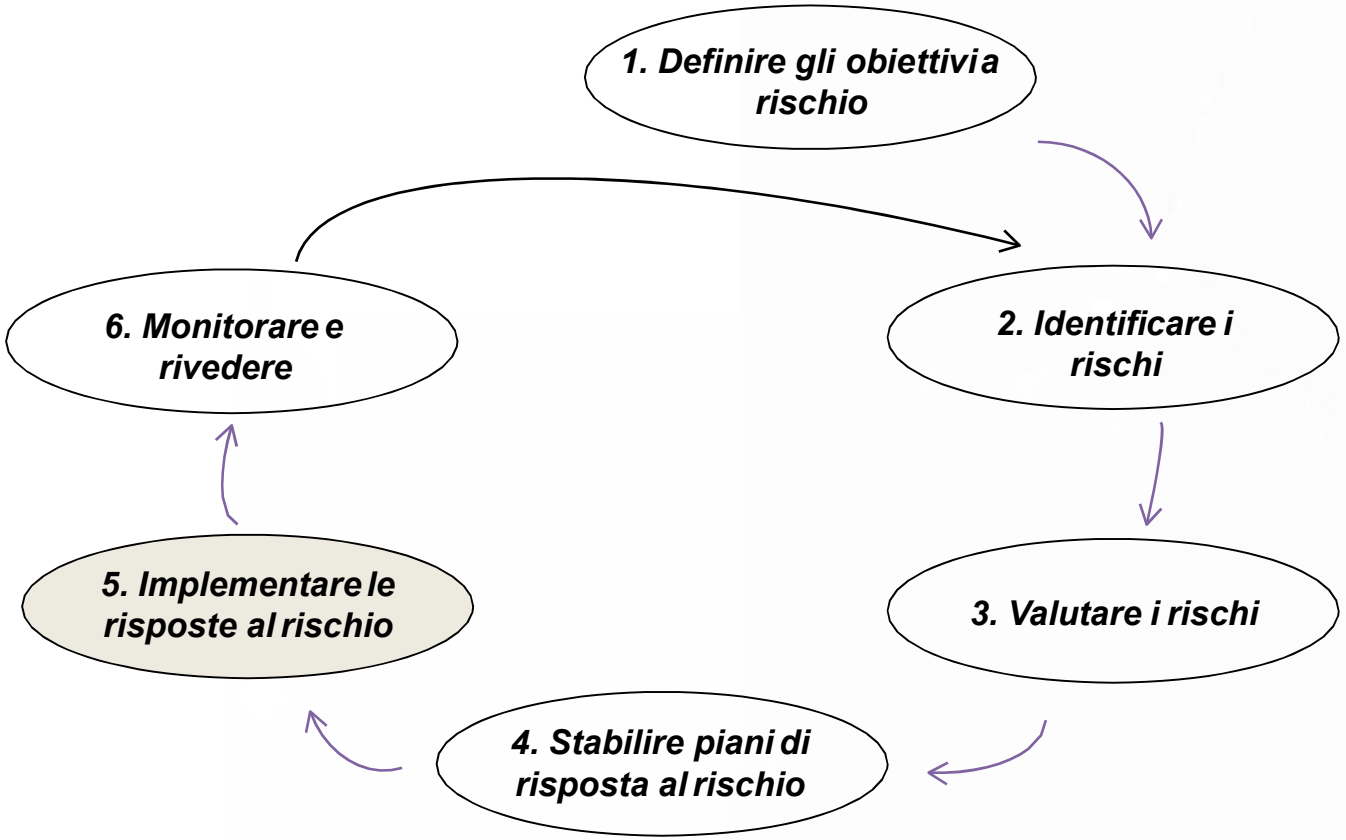
EMERGENT RISK

E’ qualcosa che va **oltre la nostra immaginazione**, abbiamo **limitazioni concettuali. Conosciuto come Black Swan. «**Unknown and unknowable unknowns»

- Esempi:
  - 9/11 attacco
  - Financial Crisis 2008
  - Sviluppo di Internet

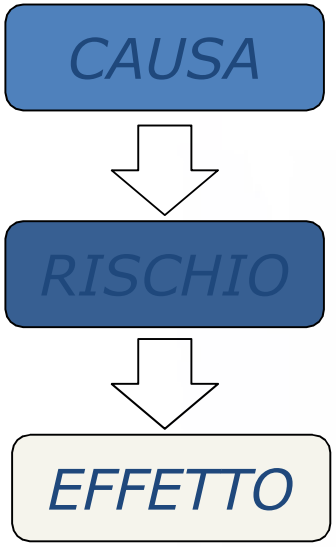
- Gestito attraverso **business continuity management, crisis management**
  - Resilienza e flessibilità , early warning signs, piani di emergenza

PROCESSO DI RISK MANAGEMENT



QUANDO UN RISCHIO NON E' UN RISCHIO?

- Facile confondere il rischio con la causa e/o l'effetto



Fatto

- *Non abbiamo abbastanza persone in un'area/funzione….*
- *Il cliente non ha ancora firmato il contratto*

Incertezza

- *Perché potremmo essere in ritardo?*

Possibile esito

- *Potremmo essere in ritardo*
- *Potrebbe accadere un incidente*

ESEMPI
CAUSE, RISCHI, EFFETTI

Uno dei nostri brevetti scade

Crescente competizione da prodotti introdotti sul mercato

I prezzi potrebbero scendere

Non abbiamo abbastanza risorse

I tassi di interesse potrebbero scendere

Potremmo andare sopra budget

Dobbiamo usare una tecnica non consolidata

Il fornitore potrebbe non consegnare nei tempi pattuiti

ESEMPI
CAUSE, RISCHI, EFFETTI

Uno dei nostri brevetti scade

Crescente competizione da prodotti introdotti sul mercato

I prezzi potrebbero scendere

Non abbiamo abbastanza risorse

I tassi di interesse potrebbero scendere

Potremmo andare sopra budget

Dobbiamo usare una tecnica non consolidata

Il fornitore potrebbe non consegnare nei tempi pattuiti

PIANIFICARE LA RISPOSTA AL RISCHIO

- Cosa possiamo fare con i rischi che abbiamo identificato, prevedendo risposte al rischio? Elementi rilevanti di valutazione:
  - Tipo e natura del rischio
  - Gestibilità
  - Impatto severità
  - Disponibilità di risorse
  - Impatto di costo

  - Chi è responsabile? Gli attori in campo

STRATEGIE DI RISPOSTA AL RISCHIO

MINACCIA (-)	STRATEGIA GENERICA	OPPORTUNITA'(+)
Evitare	Eliminare l'incertezza	Sfruttare/valorizzare
Trasferire	Trasferire la responsabilità/ Allocare la titolarità	Condividere
Ridurre	Modificare l'esposizione	Accrescere
Accettare	Includere in baseline /Controllo e gestione del residuo	Accettare

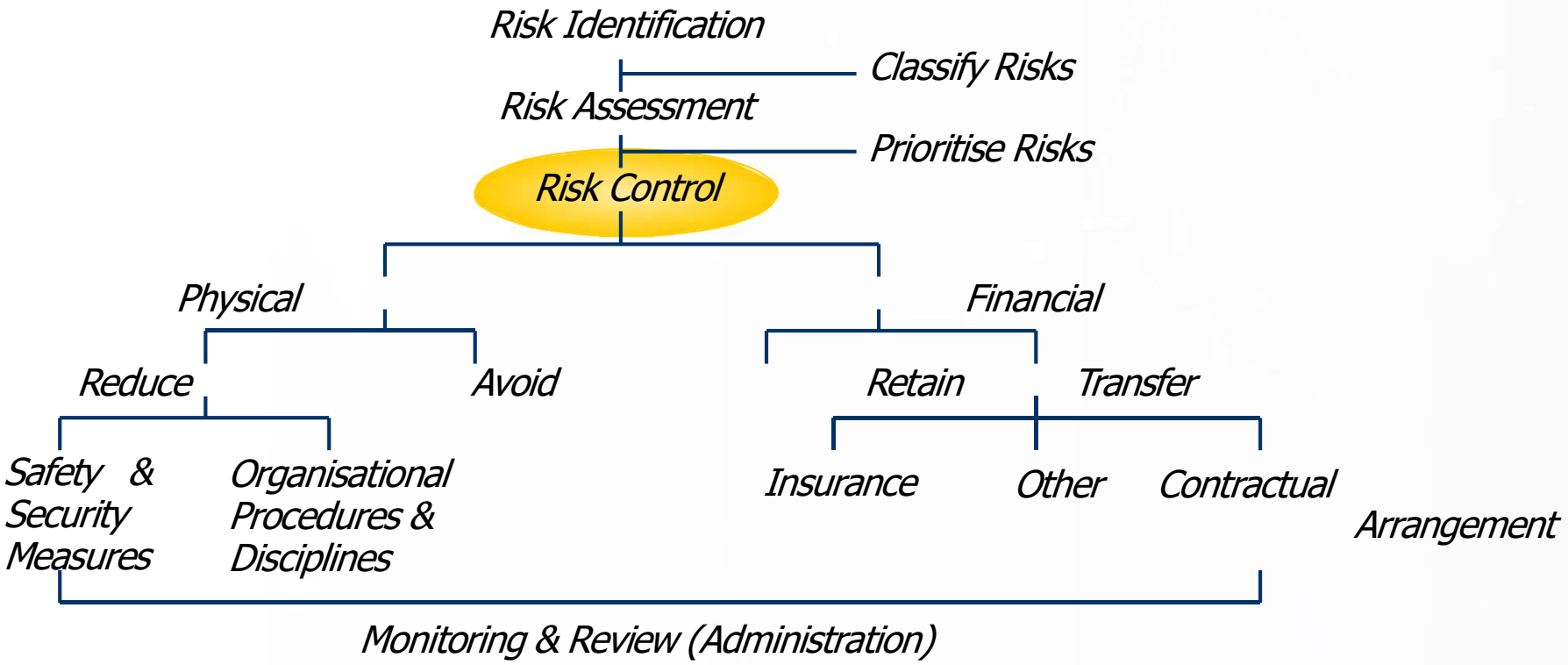
▽

Minacce e opportunità sono trattate allo stesso modo. L'unica differenza è il segno dell'impatto (+) / (-), ma sono trattate con le medesime logiche

▽

Per questo rischi e opportunità sono gestiti nello stesso processo

THE RISK MANAGEMENT PROCESS



KEY POINTS

- Rischio è «incertezza che rileva»
- Rischio include sia minacce che opportunità
- Occorre separare causa-rischio-effetto
- Descrizioni strutturate sono utili
- Selezionare appropriate strategie di risposta al rischio
- Trasformare in azioni implementate i piani di intervento

EVOLUZIONE DEL RISK MANAGEMENT NEGLI ANNI

«Risk is a threat that a company will not achieve its corporate objectives»
(London, Association of Corporate Treasurers, 1998).
Risk pervades every element of the overall business process

Risk Management is a defined set of coordinated activities to direct and control an organization with regard to risk. Risk Management allows an organization to identify Risk Mitigation Strategies so the organization can achieve its goals.

*"a **process**, effected by an entity's **board of directors**, **management** and **other personnel**, applied in **strategy-setting** and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide **reasonable assurance** regarding the achievement of **entity objectives**."*

Source: COSO Enterprise Risk Management – Integrated Framework. 2004. COSO.

IL RISCHIO NELL'ENTERPRISE RISK MANAGEMENT (ERM)

- *Rischio è incertezza che rileva rispetto al raggiungimento degli obiettivi*
- *Rischio include anche l'opportunità (upside volatility)*: non solo minacce o eventi negativi
- **Rischio è deviazione dall'atteso:** *baseline scenario* vs. *worst case scenario*

In un contesto ERM definiremo il **rischio** come **ogni deviazione dall'atteso**

- Definito in questo modo, il rischio include la volatilità negativa e positiva
- La severità o impatto deve includere solo l'eccedenza rispetto all'ammontare atteso

DEFINIZIONE DI ERM (COSO 2004)

L'Enterprise Risk Management (ERM) è un processo, posto in essere dal Consiglio di Amministrazione e dal management, impiegato come framework per la formulazione delle strategie e nello svolgimento delle attività ordinarie, progettato per:

- individuare eventi potenziali che possono influire sull'attività aziendale;
- gestire il rischio entro i limiti del rischio accettabile;
- fornire ragionevole sicurezza sul conseguimento degli obiettivi aziendali.

Source: COSO Enterprise Risk Management – Integrated Framework. 2004. COSO.

L'ERM consente al management un'efficace ed efficiente gestione delle condizioni di incertezza e dei connessi rischi ed opportunità, con conseguente possibilità di creazione di valore

LE CATEGORIE DI RISCHI DELL'ERM

- **Tutte le categorie** di rischi di impresa sono considerati nell'**ERM**. Il catalogo di solito è strutturato nelle seguenti classi di rischio:
  - **Rischi esterni:** elementi rilevanti del contesto esterno, come regolamentazione, concorrenza, politica, che possono impattare sul perseguimento degli obiettivi aziendali
  - **Rischi strategici**: cambiamenti inattesi in elementi chiave per la formulazione o esecuzione della strategia
  - **Rischi finanziari**: cambiamenti inattesi nelle condizioni di tasso, prezzo, liquidità sui mercati.
  - **Rischi operativi**: cambiamenti inattesi in elementi correlati alle operations, tipicamente risorse umane, processi, tecnologia e eventi naturali. Molti rischi specifici della categoria «operativa» sono connessi alle tematiche della più ampia compliance o corporate governance; altri richiedono una comprensione della tecnologia e delle infrastrutture che sono di supporto alle attività di core business. La loro eterogeneità di composizione li rende molto numerosi

LA TASSONOMIA DEI RISCHI/ IL RISK MODEL

Esemplificativo

RISCHI ESTERNI

Gusti del pubblico	Mercati finanziari	Disponibilità di capitali	Politico
Fallimento produttore	Concentrazioni di mercato	Regolamentare/normativo	Mercato
Inadempienze fornitori	Rischio Paese	Macroeconomico	Oneri ambientali

RISCHI INTERNI

Strategici

- Politiche di prezzo
- Incremento dei costi operativi
- Gusti del pubblico
- Acquisizioni/M&A
- Partnership
- Marginalità produzioni
- Fallimento di mercato del prodotto
- Pianificazione acquisti
- Dipendenza da fornitori strategici
- Scelte di acquisto
- Rischio Paese
- Ritardo tecnologico
- Reputazione

Operativi

Processi

- Indisponibilità macchinari critici
- Incremento dei costi operativi
- Capacità operativa per funzioni critiche
- Processi critici ancora non informatizzati
- Sistemi informativi non integrati
- Tempi rapidi di vendita dei commerciali – gap procedurali
- Gestione impegni contrattuali
- Frammentazione informatica di processi critici
- Movimentazione materiali in entrata e in uscita (perdita/danni a prodotto)
- Inadempienze fornitori
- Danneggiamento prodotti
- Ritardi esecutivi
- Presidio outsourcing
- Proprietà intellettuale

Persone

- Salute e sicurezza
- Infortuni
- Inasprimento costo del lavoro
- Contenzioso

Sistemi Informativi

- Sistemi frammentati
- Trattamento dati disomogeneo
- Disponibilità del sistema
- Riservatezza dati
- Sicurezza hardware
- Sicurezza software
- Blocco ai sistemi informativi

Legali

- Contenzioso
- Compliance
- Anti-Riciclaggio
- Responsabilità da prodotto
- Penali contrattuali

Informativa/dati

- Privacy
- Compliance regolamentare
- Prezzi di trasferimento
- Immissione dati

Rischi puri

- Responsabilità verso terzi (copyright, diritti…)
- Interruzione attività
- Catastrofi naturali
- Terrorismo
- Interruzioni della produzione
- Infortuni key men
- Scioperi
- Danni all'ambiente

Finanziari

- Credito
- Commodity
- Cambio
- Fallimento produttore
- Tassi di interesse
- Garanzie
- Liquidità

PERCHÉ RISK MANAGEMENT E PERCHÉ ADESSO ?

6. Regolamentazione

Principali riferimenti nazionali e internazionali

I Codici di Corporate Governance

- *I Codici di Corporate Governance, a livello nazionale ed internazionale, individuano i principali attori del Sistema di Controllo Interno e di gestione dei rischi (in Italia: Codice di Autodisciplina – 2011-15)*
- *Codice di Autodisciplina: principali novità introdotte riguardano la centralità del «rischio» nel sistema dei controlli, il coordinamento tra gli attori e l'integrazione con i processi aziendali*

Principali leggi e regolamenti nazionali e internazionali

- *TUF (D.lgs. 58/1998) – informativa sui rischie sui sistemi di gestione*
- *D.Lgs. 39/2010 – il Collegio sindacale vigila sull'efficacia dei sistemi di gestione delrischio*
- *Securities Exchange Act . Informativa sui principali fattori di rischio (Form 20-F).*
- *Sarbanes-Oxley Act (2002)*
- *D.Lgs. 231/2001*
- *Regolamento Europeo Privacy*

CoSO Report CoSO ERM

- *Il CoSO Report costituisce il framework di riferimento per il sistema di controllo interno.*
- *Il CoSO ERM integra il CoSO Report con i processi di gestione del rischio.*

Standard ISO 31000:2009 Nuova ISO 9001

- *Principi e linee guida sui modelli di gestione dei rischi.*
- *Necessità di individuare tempestivamente i rischi*

Agenzie di rating (S&P)

- *I sistemi di risk management sono valutati tra i requisiti per il calcolo del merito di credito.*

Settore bancario e assicurativo

- *Regimi di vigilanza prudenziale per banche e assicurazioni finalizzati a garantire la copertura delle posizioni di rischio assunte (Basilea., Solvency)*

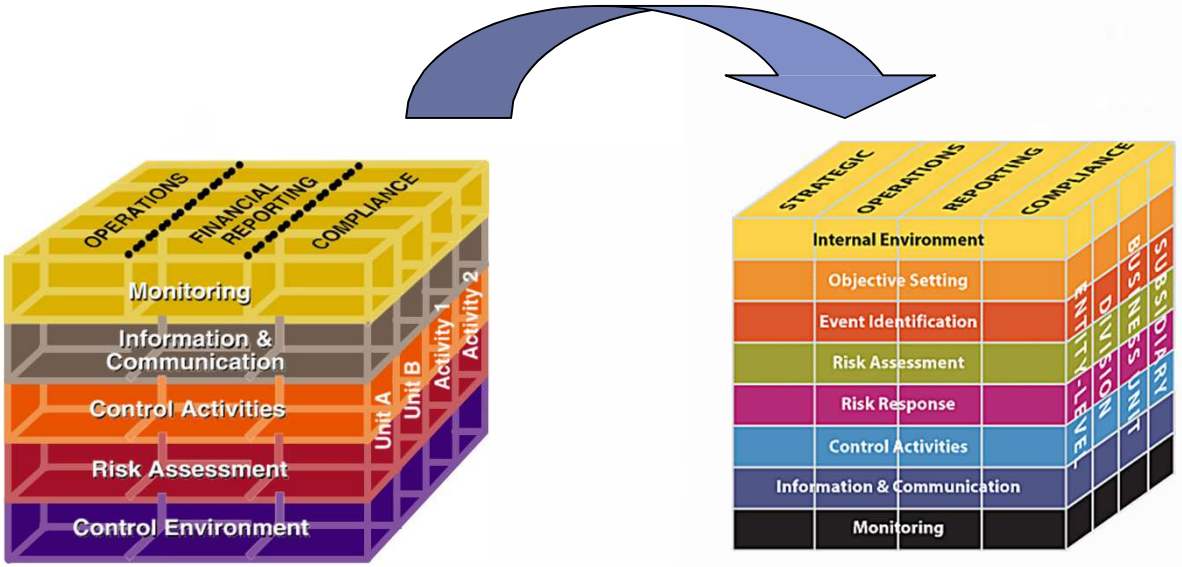
COMPLIANCE VIEW

- Diverse prescrizioni normative impongono all'impresa **un approccio *responsabile* ai rischi connessi alla propria attività**
  - Es: dal 2008, ogni datore di lavoro è tenuto a redigere il **Documento di Valutazione dei Rischi** ai sensi del d.lgs.81/08 (Testo Unico sulla salute e sicurezza sul lavoro)
  - Es: dal 2018 ogni titolare del trattamento di dati personali è obbligato a rispettare quanto previsto dal Regolamento Europeo Generale sulla Protezione dei Dati (che ha sostituito il già vigente d.lgs. 193/2006, prevedendo appunto un *risk based approach*).
  - Es: **Modello di Organizzazione, Gestione e Controllo** adottato ai sensi del **d.lgs.231/2001**, si basa su un'attenta **analisi e un'accurata valutazione dei rischi di tutti i processi aziendali, in ottica di prevenzione da reato.**

Distintività: saper integrare e coniugare le diverse prescrizioni normative

COSO FRAMEWORK – CRESCENTE ATTENZIONE A RISCHI E CONTROLLI

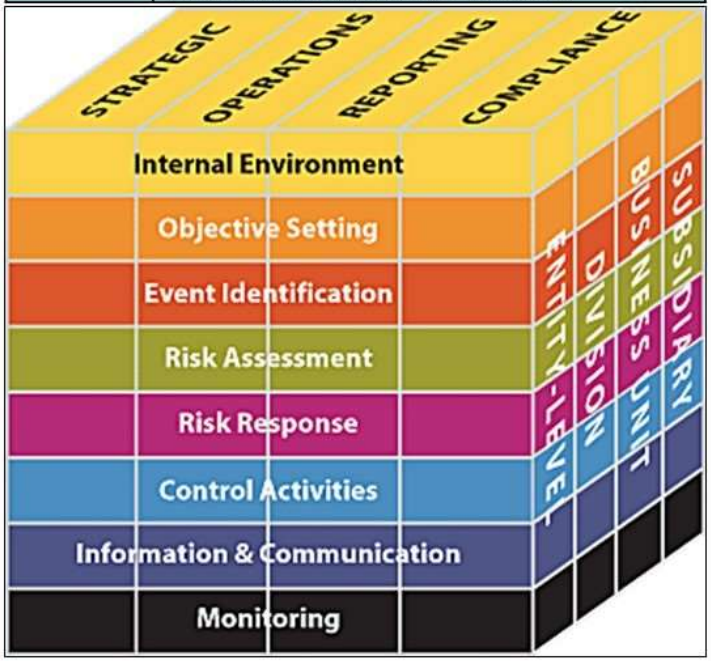
Per aiutare ad assistere nell'implementazione di un processo di ERM, COSO ha sviluppato l'**ERM Integrated Framework** (2004), anche conosciuto come **COSO Cube**. Questo cubo è una evoluzione dell'iniziale COSO I framework sviluppato nel 1992



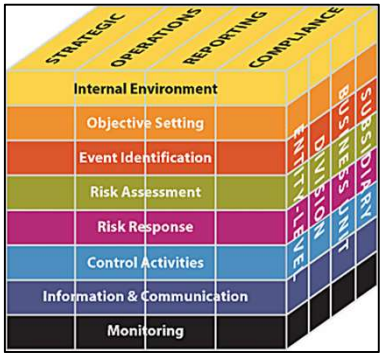
GLI ELEMENTI DEI PROGETTI DI ERM (SECONDO IL COSO-ERM 2004)

Strategic	Obiettivi di sintesi aziendali correlati e di supporto alla vision/mission e alla strategia dell'impresa
Operations	Obiettivi relativi alla efficacia ed efficienza delle operazioni aziendali
Reporting	Obiettivi relativi alla efficacia del sistema di reporting aziendale, sia interno sia esterno, con riferimento all'informativa nomico-finanziaria e a quella operativa
Compliance	Obiettivi relativi alla conformità delle attività aziendali rispetto alle leggi e regolamenti applicabili.

Internal Environment	Ambiente di Controllo, fra cui propensione al rischio e filosofia di risk management
Objective Setting	Sistema degli obiettivi aziendali e correlate attitudini al rischio
Event Identification	Metodologia di identificazione degli eventi che, per ogni processo e unità organizzativa, originano rischi (minacce e opportunità)
Risk Assessment	Metodologia con cui sono valutati la probabilità e l'impatto dei rischi
Risk Response	Metodologia con cui è individuata la reazione da adottare con riferimento ai rischi identificati e valutati. Le opzioni possono essere: accettare, evitare, trasferire (contratti, assicurazioni) e ridurre (controllo interno)
Control Activities	Attività di controllo, con enfasi su integrazione dei controlli con i processi di risk response
Information & Communication	Sistemi informativi e processi di comunicazione (come CoSO Report)
Monitoring	Verifica della adeguatezza di progettazione e operatività di tutti gli elementi dell'ERM. Il monitoraggio può essere continuo, incorporato nei processi manageriali (ongoing monitoring activities) o discontinuo (separate evaluation).



IL COSO 2
LE 20 COMPONENTI DEL FRAMEWORK DEL 2017



Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

PERCHE' L'ERM È IMPORTANTE

Principi sottostanti

- Ogni entità, sia essa profit o non profit, esiste per creare valore per i propri azionisti
- Il valore è creato, preservato, o eroso dalle decisioni del management in tutte le attività, dalla definizione della strategia all'operatività day-to-day

ERM supporta la creazione di valore permettendo al management di:

- *Gestire efficacemente eventi futuri incerti che creano incertezza*
- *Rispondere ad essi in un modo che riduce la probabilità di eventi negativi e incrementa l'upside*

Il COSO ERM framework definisce le componenti essenziali, suggerisce un linguaggio comune e individua una chiara direzione e guida per la gestione dei rischi di impresa nella sua totalità.

GLI ELEMENTI DEI PROGETTI DI ERM

(SECONDO IL COSO-ERM 2004)

1. Definizione obiettivi

ID	Obiettivo
Quantitativo 1	Difesa della marginalità
Quantitativo 2	Sviluppo dei volumi di vendita
Quantitativo 3	Risparmio energetico
Qualitativo 1	Internazionalizzazione
Qualitativo 2	Tutela della reputazione
Qualitativo 3	Sviluppo di una struttura di *Governance*

2. Identificazione minacce e opportunità

3. Valutazione entità dei rischi

Probabilità					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
			Impatto		

4. Gestione dei rischi

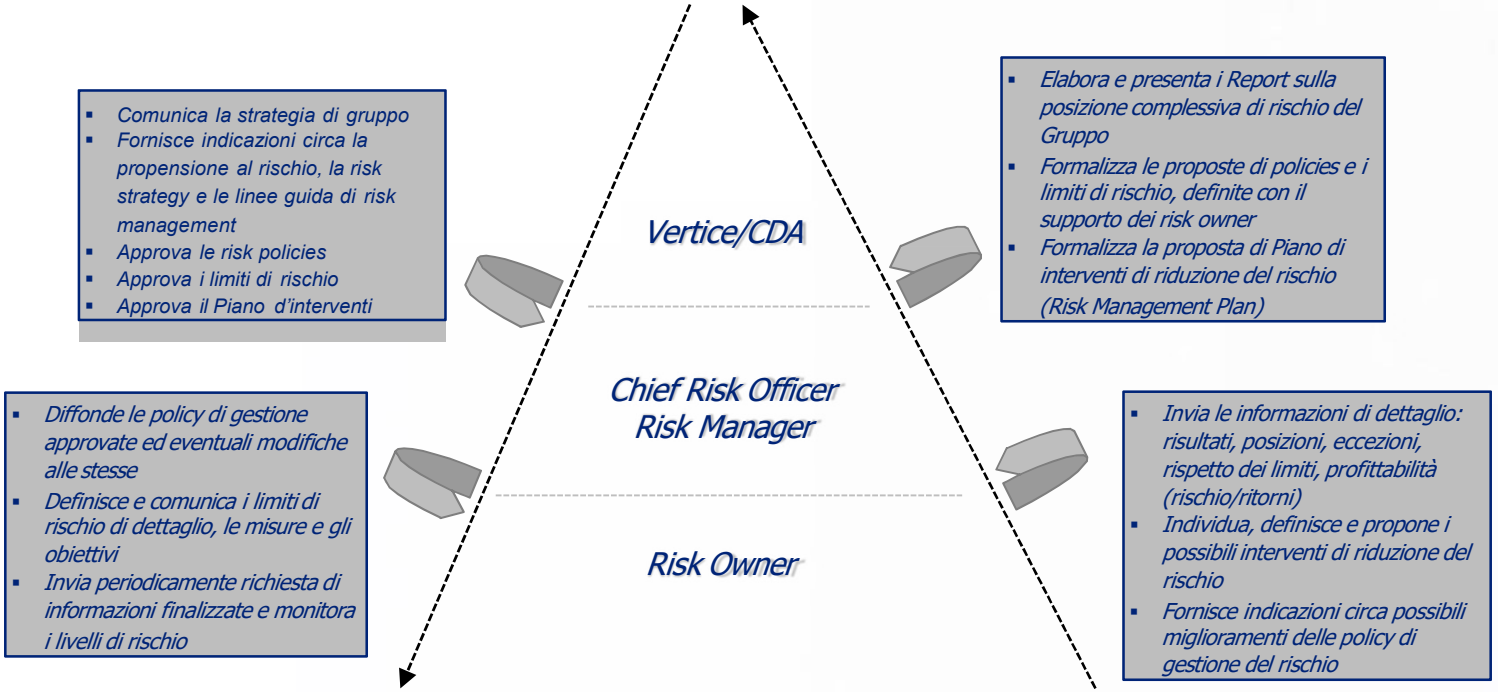
Evitare	Condividere
• Disfarsi di un' unità operativa, di una linea di produzione, di un segm ento del mercato • Decidere di non intraprendere nuove iniziative/attività che potrebbero dar luogo a rischi	• Sottoscrivere una polizza assicurativa per perdite inattese • Entrare a far parte di una joint venture/partnership • Fare un accordo di sindacato • Coprire i rischi im piegando strum enti di *capital m arket* • Esternalizzare i processi produttivi • Condividere il rischio tram ite accordi contrattuali con clienti, fornitori o altri partner
Ridurre	**Accettare**
• Diversificare l' offerta di prodotto • Stabilire limiti operativi • Attivare processi operativi efficaci • Accrescere il coinvolgim ento del m anagem ent nel processo decisionale e nel m onitoraggio • Riequilibrare il portafoglio di attività riducendo l' esposizione a certi tipi di perdite • Riallocare il capitale tra le unità operative	• Auto-assicurarsi contro le perdite • Fare affidam ento sulle com pensazioni naturali che si verificano all' interno del portafoglio • Accettare il rischio in quanto già in linea con la tolleranza alrischio

5. Reporting, controllo e monitoraggio

I FLUSSI INFORMATIVI PER LE DECISIONI

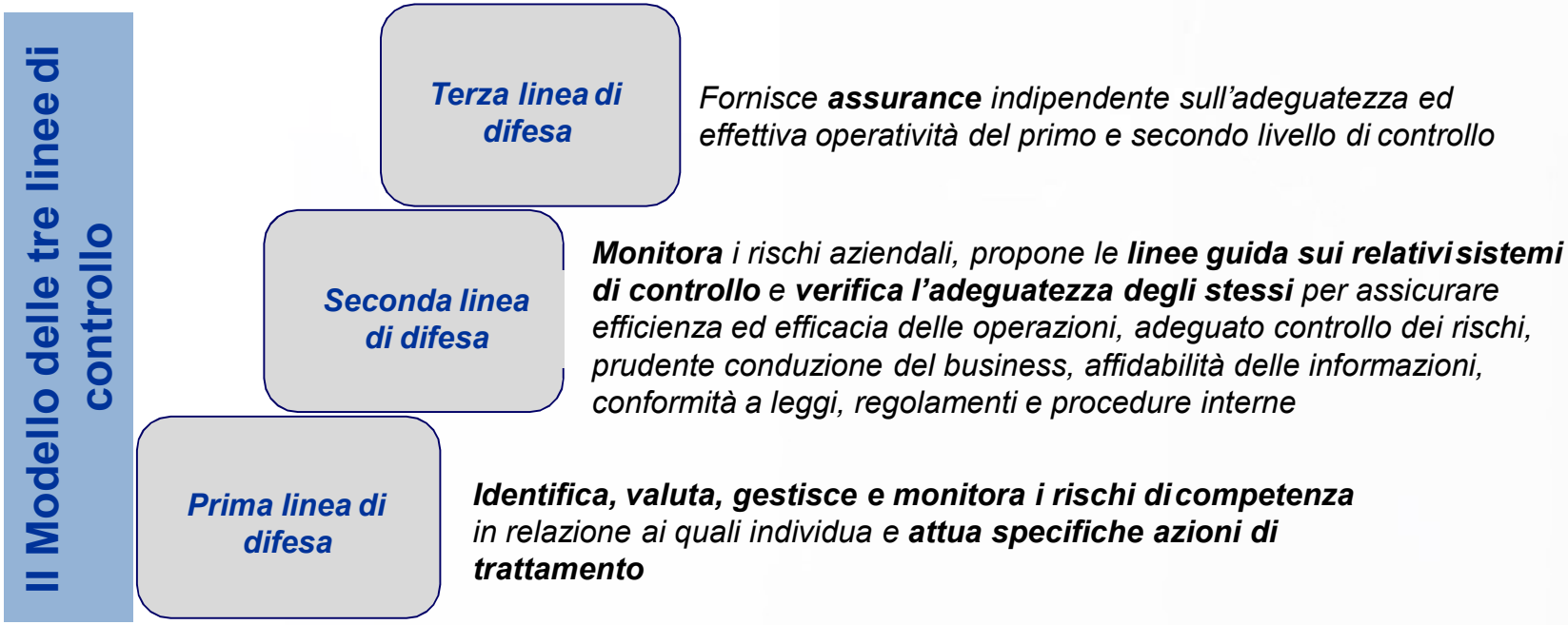
Il sistema di ERM necessita di un costante e corretto flusso di informazioni per poter operare in maniera efficace, efficiente e in linea con la strategia di Gruppo.

Principali flussi di comunicazione verticali

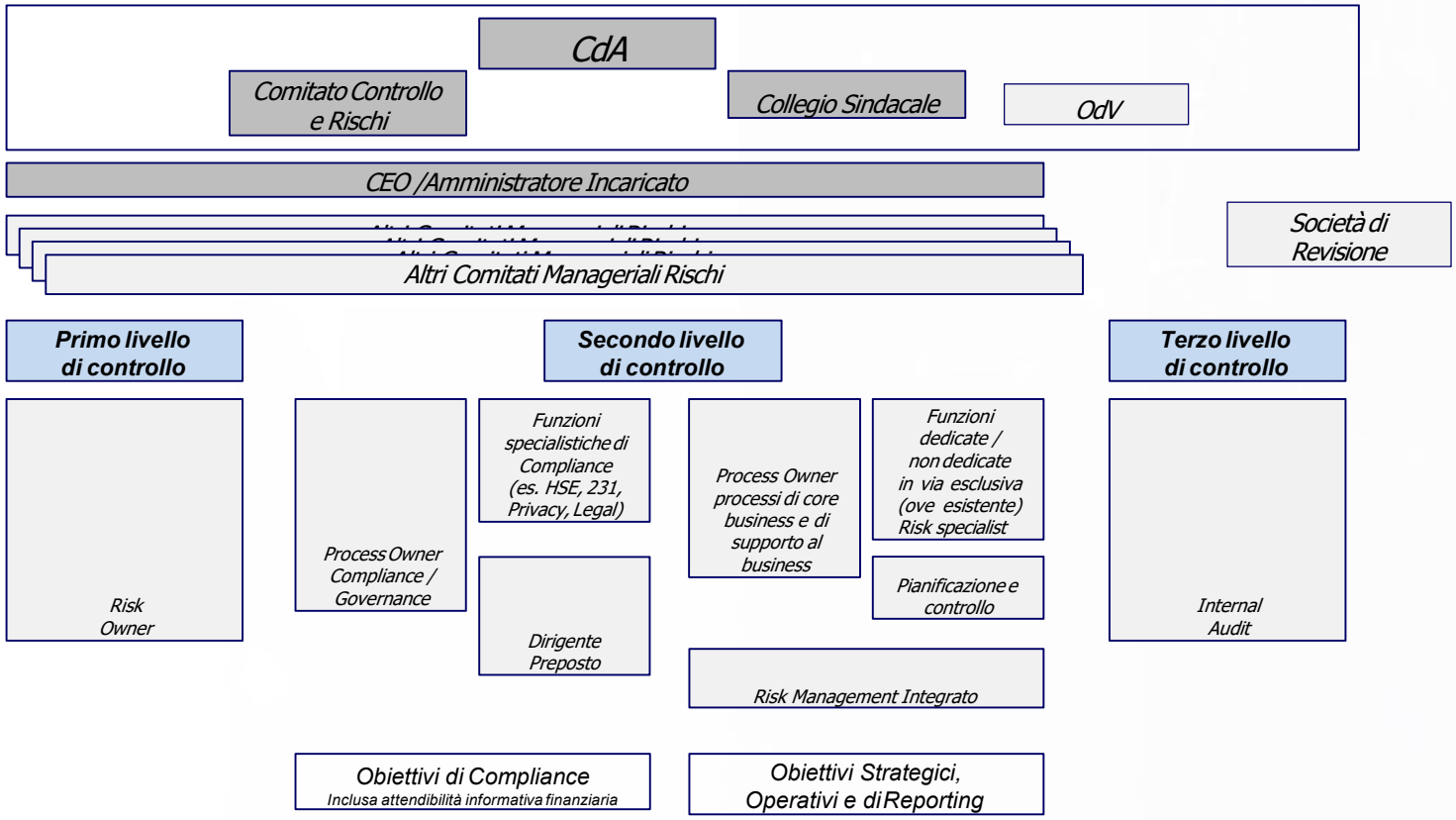


IL MODELLO DELLE TRE LINEE DI DIFESA

- Il controllo deve essere esercitato attraverso linee di difesa chiare, definite e indipendenti – la linea di business, il risk management e l'internal audit – linee che giocano tutte una funzione importante nell'integrated ERM.
- Il modello basato su tre linee di difesa distingue tra funzioni che sono sia owner sia gestori dei rischi, funzioni che supervisionano i rischi e funzioni che forniscono una assurance indipendente.



I TRE LIVELLI DI DIFESA/CONTROLLO
ESEMPLIFICAZIONE



LE LINEE DI DIFESA

- **Il Consiglio di Amministrazione**
  - definisce il risk appetite, approva la strategia per la gestione del rischio ed è il responsabile ultimo per il sistema di controllo interno dell'azienda;
- **Il CEO**
  - supportato dal senior management, ha la responsabilità generale per la gestione dei rischi che riguardano l'intera azienda;
- **Il management e lo staff di ogni linea di business (prima linea di difesa)**
  - hanno la responsabilità "primaria" di gestire il rischio. A loro è richiesto di assumersi le responsabilità per l'identificazione, l'assessment, la gestione, il monitoraggio ed il reporting dei rischi aziendali che nascono all'interno dei rispettivi business.
- **Il chief risk officer (seconda linea di difesa)**
  - supportato dalle funzioni che gestiscono il rischio all'interno dell'azienda, ha la responsabilità generale per la seconda linea di difesa. Il chief risk officer è accountable rispetto al comitato aziendale rischi ed, in ultima istanza, rispetto al Consiglio di Amministrazione. La gestione quotidiana dei rischi non è l'accountability del chief risk officer; ma resta compito della prima linea di difesa. Di solito la funzione che gestisce il rischio:
  - raccomanda le politiche sul rischio al Cda per la sua approvazione, fornisce gli obiettivi di "supervision" e coordina le attività di ERM con l'ausilio di altri specialisti e delle relative funzioni connesse al rischio
  - fornisce un supporto generale e specialistico e fornisce consulenza e consigli ai componenti della gestione operativa nell'identificazione, assessment, gestione, monitoraggio e reporting dei rischi.
- **L'internal audit (terza linea di difesa)**
  - fornisce una assurance indipendente sull'efficacia della gestione dei rischi aziendali attraverso tutta l'azienda. La funzione di internal audit è accountable nei confronti del comitato di audit committee ed, in ultima analisi, nei confronti del Cda.

10 PRINCIPI PER L'ERM

Elementi da considerare per valutare se un'azienda ha un efficace programma di ERM:

1. E' applicato all'azienda nella sua totalità
2. Include tutte le categorie di rischio
3. Focus solo sui key risks
4. Integrato tra le diverse tipologie di rischi
5. Impiega metriche aggregate
6. Include il decision making
7. Bilancia rischio e rendimento
8. Effettua una appropriata risk disclosure
9. Misura l'impatto sul valore
10. Si focalizza sugli stakeholder primari

10 PRINCIPI PER L'ERM

1. **Estensione all'impresa nella sua totalità*:*** ERM deve essere applicato a ogni area dell'azienda. Situazioni critiche:
   - Golden boy unit
   - Aree di valore insignificante
   - Implementazione incompleta

2. **Tutti i rischi devono essere inclusi**:
   3. Rischi finanziari: mercato, credito e liquidità
   4. Rischi strategici: cambiamenti inattesi in elementi chiave della strategia
   5. Rischi operativi: risorse umane, tecnologia, processi e rischi catastrofali

- *Frequente focus solo sui rischi finanziari, perchè?*
  - Incapacità a quantificare i rischi strategici e operativi
  - Falsi miti riguardo all'importanza dei rischi finanziari: diversi studi mostrano che rischi strategici e operativi costituiscono la maggior parte dei rischi più critici di un'azienda e ne rappresentano la principale minaccia.
  - Preferenza degli analisti finanziari

10 PRINCIPI PER L'ERM

3. **Si focalizza sui rischi chiave*:*** ERM è strategico in natura e deve focalizzarsi solo sulle criticità maggiori per l'impresa, circa 15/20 (numero massimo per produrre un valido set di risultati di supporto al processo decisionale)
   - Il numero dei rischi chiave non dipende dalla dimensione dell'impresa – le più grandi organizzazioni possono avere più rischi critici collegati a questioni reputazionali. La grandezza dell'impatto dei key risks può variare significativamente in base alla dimensione aziendale.

4. **Integrato tra le diverse tipologie di rischi:** la gestione per silos produce risultati inefficaci e incompleti (Disarming value Killer – Deloitte research study – nei 10 anni di osservazione dello studio - periodo 1994/2003 - più dell'80% delle 100 maggiori perdite di valore azionario erano il risultato di due o più rischi interagenti)

10 PRINCIPI PER L'ERM

5. **Metriche aggregate*:*** ERM impiega metriche, necessarie almeno due:
   - Set di metriche che aggregano le esposizioni al rischio a livello di impresa (enterprise risk exposure)
   - Risk appetite: definizione quantitativa, definita dal management, dell'ammontare di enterprise risk exposure che è giudicato accettabile. E' il livello target di esposizione al rischio, è il livello limite che il management vuole sia l'esposizione al rischio

6. **Include il Decision Making*:*** ***"***gestire" è la finalità principale dell'ERM. Rispondere al rischio, gestirlo, prendere decisioni. Molti programmi di ERM si focalizzano solo sulle esposizioni al rischio e saltano lo step più importante che è quello di **fare** qualcosa per ridurle o gestirle.

7. **Bilancia gestione del rischio e rendimento:** ERM non prevede solo la mitigazione del rischio. Sono considerate contemporaneamente upside e downside volatility, ovvero è presa in considerazione l'intera gamma di opportunità.

10 PRINCIPI PER L'ERM

8. **Fa una appropriata risk disclosures*:*** il rischio di inappropriata risk disclosure è il più sottostimato. Necessarie informazioni correlate all'impatto sul valore degli eventi.

9. **Misura l'impatto sul valore:** il valore è una metrica essenziale per informare il processo decisionale rispetto a valutazioni di rischio. Adottare metriche di breve periodo può essere non corretto.

10. **Si focalizza sugli stakeholders primari:** gli azionisti sono i primari stakeholder e l'ERM deve focalizzarsi principalmente sul maggiore valore per gli azionisti.