Ordine dei Dottori Commercialisti e degli Esperti Contabili di Roma

La vigilanza del Collegio Sindacale sull'adeguatezza del sistema di controllo interno

IL SISTEMA DI CONTROLLO INTERNO

CARATTERISTICHE, DEFINIZIONI E MODELLI DI RIFERIMENTO

Dott. Leonardo Palma

Il SCI secondo i principali standard di riferimento

SCI

↓

Buone pratiche di governo dell'impresa

↓

Committee of Sponsoring Organizations of the Treadway Commission (CoSO): un'organizzazione privata creata allo scopo di rendere operative le raccomandazioni della **Treadway Commission** in tema di **controlli interni ed assetti societari**, finalizzate ad una **riduzione degli illeciti e dei falsi in bilancio**.

- "*Internal Control - Integrated Framework*", pubblicato nel 1992
- framework "*ERM - Enterprise Risk Management*", pubblicato nel 2004
- framework "*Internal Control over Financial Reporting – Guidance for Smaller Public Companies*", pubblicato nel 2006
- aggiornamento dell'"*Internal Control - Integrated Framework*", pubblicato nel 2013
- aggiornamento dell'"*ERM - Enterprise Risk Management*", pubblicato nel 2017

Best practices in tema di Sistema dei Controlli Interni e Gestione dei Rischi

Rischi: eventi futuri e incerti che possono influenzare in modo sia positivo che negativo il **raggiungimento degli obiettivi di un'azienda**.

Il *framework CoSO Internal Control* (1992)

Il Sistema dei Controlli Interni è *un insieme di meccanismi, procedure e strumenti – "controlli" – predisposti dalla direzione per assicurare il conseguimento degli obiettivi aziendali*

3 OBIETTIVI

- ***Operations***: efficienza e efficacia delle **attività operative**
- ***Financial reporting***: attendibilità delle **informazioni di bilancio**
- ***Compliance***: **conformità** alle leggi e ai regolamenti in vigore

5 ELEMENTI COSTITUTIVI

DIMENSIONI D'ANALISI

- Attività, processi, unità organizzative

Framework:

il **controllo** non si deve rifare ai concetti di **verifica o accertamento repressivo**

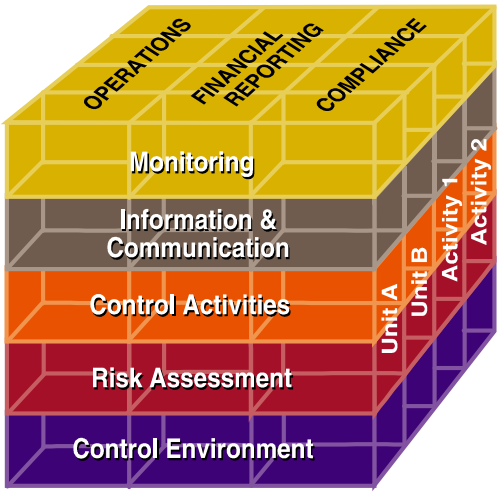
ma deve essere **modello di guida e coordinamento** volto a regolare e garantire il **corretto funzionamento di un sistema**, indirizzandolo verso "*il conseguimento degli obiettivi aziendali*".

Il **controllo** non rappresenta quindi un'attività supplementare o un onere necessario, ma una **parte integrante delle attività aziendali insita nelle "*procedure*" e nei "*meccanismi*" in grado di costituire un fattore critico di successo**.

Dal *framework CoSO Internal Control* al *framework CoSO ERM*

Framework **CoSO** *Internal Control (1992)* → *Framework* **CoSO ERM** *(2004)*

- Inserimento degli **obiettivi strategici a** un livello superiore rispetto agli altri



- Inserimento della componente di ***objective setting***
- Suddivisione del ***risk assessment*** nelle **tre componenti** che descrivono le fasi in cui tipicamente si articola il ***risk management***:
  1. identificazione degli eventi negativi (***event identification***)
  2. valutazione di probabilità e impatto economico (***risk assessment***)
  3. individuazione delle contromisure applicabili (***risk response***)

- Estensione delle dimensioni d'analisi all'intera azienda (*legal entities*, divisioni, *business units e subsidiaries*)

Principale caratteristica del **Framework ERM**:
enfatizzazione del legame tra

- strategia,
- obiettivi,
- rischi e controlli,

elementi imprescindibili, in quanto l'assenza di una **strategia aziendale** comporterebbe l'impossibilità di declinare **obiettivi** chiari e condivisi a tutti i livelli organizzativi e, di conseguenza, l'impossibilità di identificare gli **eventi negativi/rischi** che potrebbero pregiudicarne il raggiungimento.

Carattere sistemico dei controlli interni

*«L'**ERM** è un **processo**, posto in essere dal Consiglio di Amministrazione, dal management e da altri operatori della struttura aziendale, utilizzato per la formulazione delle **strategie** in tutta l'organizzazione e progettato per:*

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

Framework CoSO ERM (2004)

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

Internal Control over Financial Reporting – Guidance for Smaller Public Companies

Imprese di dimensioni minori:
l'implementazione di un Sistema dei Controlli Interni strutturato secondo i Framework illustrati può risultare **anti-economica.**

"*Internal Control over Financial Reporting - Guidance for Smaller Public Companies*",(giugno 2006): supporto alle imprese di dimensioni minori nella realizzazione di sistemi di controllo interno "***cost effective***".

Raggiungere i benefici di un **controllo interno efficace** e al tempo stesso di **contenerne i relativi costi incrementali**.

Alcuni **principi applicativi** contenuti nella "Guidance":

- **codice di condotta** fondato dalle posizioni apicali dell'impresa su integrità e valori etici;
- adeguata attribuzione dei **poteri e delle responsabilità** (impatto su ambiente di controllo; separazione dei compiti; corretto equilibrio tra i poteri necessari per svolgere i compiti assegnati ed il bisogno di mantenere un adeguato controllo interno sui processi chiave);
- identificazione dei **rischi** relativi al **financial reporting**;
- selezione e sviluppo delle **attività di controllo** (in funzione del costo e della potenziale efficacia nel mitigare i rischi);
- **monitoraggio continuo e valutazioni specifiche del SCI**, che consentono al management di determinare se le componenti del controllo interno sono presenti ed operative;
- ecc..

Internal Control - Integrated Framework

La crescente complessità delle strutture di business e le maggiori aspettative in termini di efficacia della *governance* societaria hanno indotto il CoSO a pubblicare nel maggio 2013 un aggiornamento del documento originario.

L'aggiornamento riprende sostanzialmente tutti gli aspetti principali del *framework* originario.

Le **modifiche di maggior rilievo** rispetto al *framework* originario:

- maggior enfasi sulla **capacità** del Sistema di Controllo Interno di **prevenire le frodi**;
- ampia trattazione di **tematiche di *corporate governance***, in quanto la **supervisione da parte del Consiglio di Amministrazione** e dei comitati costituiti al suo interno è ritenuta essenziale ai fini della **realizzazione di un controllo interno efficace;**
- riconoscimento del **ruolo rilevante assunto dalla tecnologia** nell'implementazione del Sistema dei Controlli Interni;
- allargamento della categoria degli obiettivi di *reporting* all'**informativa di carattere non finanziario** ed alla **reportistica interna**.

Internal Control - Integrated Framework

APPROCCIO «*PRINCIPLE – BASED*»

Vengono esplicitati **17 principi applicativi** associati ai **cinque elementi costitutivi** del controllo interno

I 17 **«principi»** hanno lo scopo di illustrare **i requisiti** necessari per **realizzare un Sistema dei Controlli Interni efficace**

CONTROL ENVIRONMENT

1. L'organizzazione rispetta **valori etici e di integrità**
2. Il **Consiglio di Amministrazione** si dimostra **indipendente** dal *management* e **vigila** sul funzionamento e sullo sviluppo del controllo interno
3. Il management definisce, con la supervisione del Consiglio di Amministrazione, strutture, **linee di riporto, poteri e responsabilità funzionali al perseguimento degli obiettivi**
4. L'organizzazione attrae, sviluppa e trattiene **risorse competenti**
5. Il personale è adeguatamente responsabilizzato in merito al perseguimento degli **obiettivi e all'esercizio dei propri poteri di controllo**

Control Environment
(Attuazione dei principi)

- Statuto societario
- Sistema di deleghe e procure
- Codice etico
- Codice di condotta e di comportamento
- Modello di Organizzazione, Gestione e Controllo ex D.Lgs.231/2001
- Linee guida sul SCIGR (società quotate)
- Procedure di whistleblowing
- Organigramma, Funzionigrammi, mansionari e job descrition
- Enterprise Risk Management (ERM)
- Norme in materia di anticorruzione
- Sistema sanzionatorio
- Politica delle retribuzioni e sistema di incentivi
- Verifiche periodiche con riferimento agli aspetti etici e di integrità
- Procedure per la valutazione e gestione del conflitto di interesse
- Politiche di recruiting
- Processi di formazione e sviluppo del personale
- Sistema di valutazione delle prestazioni
- Piano di audit

RISK ASSESSMENT

6. Gli **obiettivi** dell'organizzazione sono **chiari** e permettono l'identificazione e la **valutazione dei rischi a essi correlati**
7. I **rischi** connessi al raggiungimento degli obiettivi sono **identificati** a tutti i livelli dell'organizzazione e **analizzati** al fine di determinare le possibili modalità di gestione
8. I **rischi di frode** sono adeguatamente identificati e valutati
9. I cambiamenti che potrebbero impattare in modo significativo sul Sistema di Controllo Interno sono adeguatamente **identificati e valutati**

Risk Assessment
(Attuazione dei principi)

- Pianificazione strategica
- Analisi SWOT (Strengths, Weaknesses, Opportunities, Threats)
- Reportistica periodica
- Policy sulle remunerazioni
- Definizione, implementazione e aggiornamento del SCIGR
- Analisi dei prodotti/servizi e della clientela
- Analisi dei competitor e Piano di Business Continuity
- Piano di Internal Audit Risk Based
- Definizione degli schemi di frode
- Business Impact Analysis

CONTROL ACTIVITIES

10. Vengono identificate e sviluppate **attività di controllo** che contribuiscono **a contenere i rischi entro livelli accettabili**
11. Vengono identificate e sviluppate **attività di controllo sulle tecnologie**
12. Le attività di controllo vengono inquadrate attraverso **policy aziendali e procedure operative**

Control Activities
(Attuazione dei principi)

- Matrici dei rischi
- Principi di SoD (Segregation of Duties) e svolgimento di analisi SoD
- Controlli in caso di principi SoD non rispettati
- Check list e standard di controllo
- Mappatura delle applicazioni aziendali
- Controlli sull'area Information Technology
- Identificazione dei profili di accesso ai sistemi e relativi diritti
- Procedura per l'abilitazione ai sistemi informatici aziendali
- Vulnerarability assessment
- Piani antiintrusione

INFORMATION & COMMUNICATION

13. Il funzionamento del Sistema di Controllo Interno è supportato dall'ottenimento (o dalla generazione) e dall'utilizzo di **informazioni affidabili e di qualità**

14. **Le informazioni** necessarie al funzionamento del Sistema di Controllo Interno (inclusi gli obiettivi e le responsabilità di controllo) sono **diffuse all'interno dell'organizzazione**

15. L'organizzazione comunica con soggetti esterni in merito a argomenti relativi al funzionamento del Sistema di Controllo Interno

Information & Communication
(Attuazione dei principi)

L'attuazione dei principi avviene in funzione del fabbisogno informativo e comunicativo dell'Entità, e dipende:

- dalle fonti necessarie per reperire le informazioni
- dalla forma delle informazioni
- dal livello di dettaglio delle informazioni
- dalle verifiche necessarie per assicurare la qualità del dato
- dalla struttura divisionale e funzionale

MONITORING

16. L'organizzazione individua, sviluppa e esegue **valutazioni** finalizzate a accertare la **presenza e il funzionamento** delle componenti del Sistema di Controllo Interno
17. Le **carenze** del Sistema di Controllo Interno sono **valutate e comunicate tempestivamente** ai soggetti responsabili di porre in essere le opportune azioni correttive, inclusi il senior management e il Consiglio di Amministrazione

Monitoring
(Attuazione dei principi)

- Risk Assessment del responsabile della gestione dei rischi
- Business Review del Controllo di Gestione
- Attività di benchmarking di processi o controlli rispetto ad altre società
- Review della Funzione Internal Audit
- Sistemi di certificazione (ISO, sicurezza, ambiente, etc.)
- Sistemi di controllo qualità
- Conta fisica delle scorte di magazzino
- Verifica delle riconciliazioni bancarie
- Controlli di produzione
- Verifica dell'ageing dei crediti da parte della Funzione Amministrazione
- Valutazione dei risultati delle attività di monitoraggio svolte
- Informativa del Responsabile della funzione Internal Audit
- Valutazione da parte della Funzione di Risk Management

Enterprise Risk Management – Integrating with Strategy and Performance

La maggiore volatilità dei mercati e l'emersione di nuovi e sempre più complessi rischi da gestire da parte della *governance* aziendale hanno spinto il CoSO a pubblicare nel giugno 2017 un aggiornamento del precedente documento pubblicato nel 2004.

Lo scopo dell'aggiornamento del documento è stato rendere la gestione dei rischi aziendali reattiva allo scenario evolutivo dei mercati internazionali, in modo da tenere in dovuta considerazione i fattori di rischio sia nel processo di definizione della Strategia sia nel processo di definizione della Performance.

L'aggiornamento del documento, al pari di quanto previsto nell' «Internal Control – Integrated Framework», si basa su un approccio fondato sulla definizione di 20 principi guida organizzati in cinque componenti tra loro interconnesse:

1, Governance and Culture
2, Strategy and Objective-Setting
3, Performance
4, Review and Revision
5, Information, Communication and Reporting