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

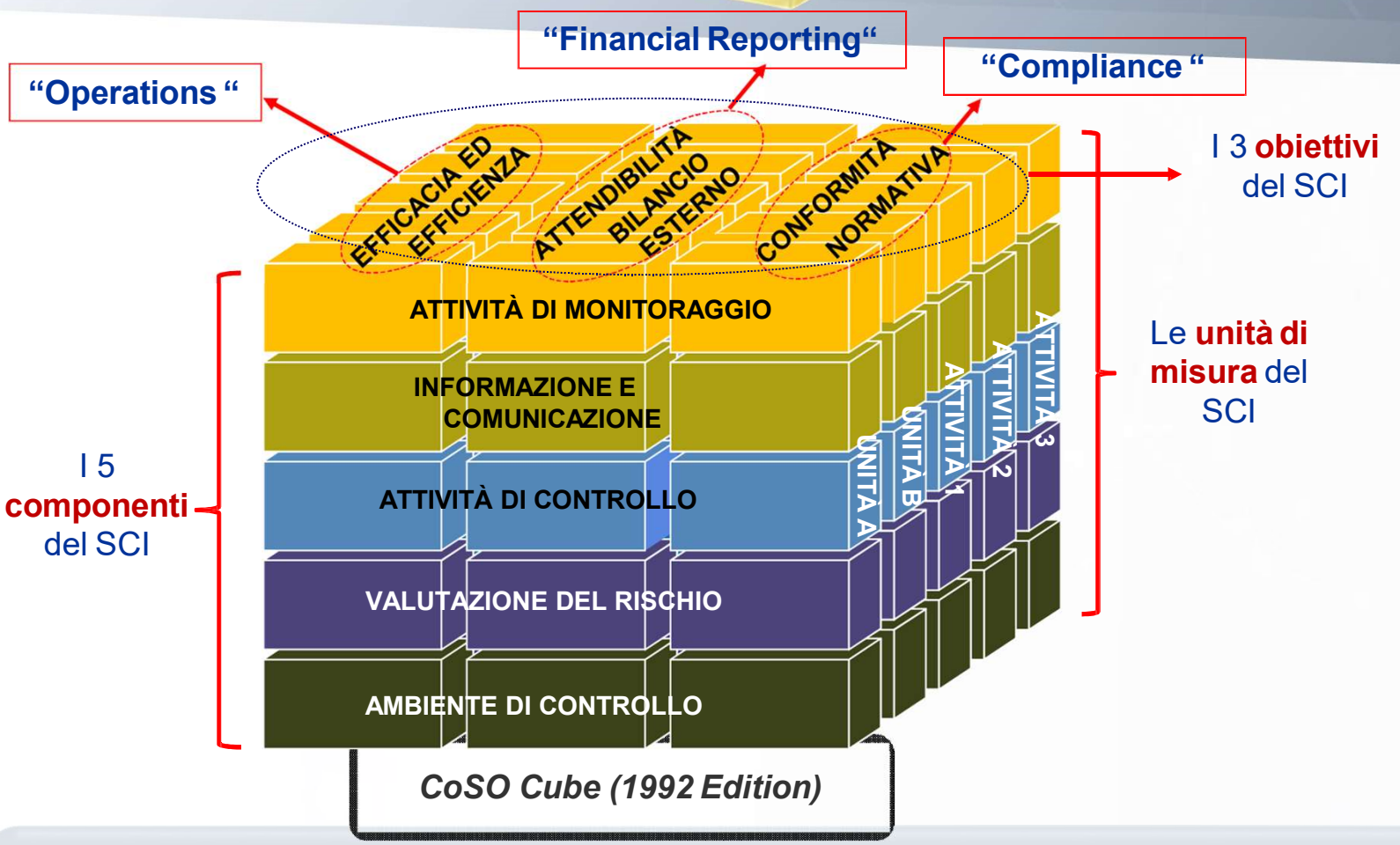
L'evoluzione del "framework"

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

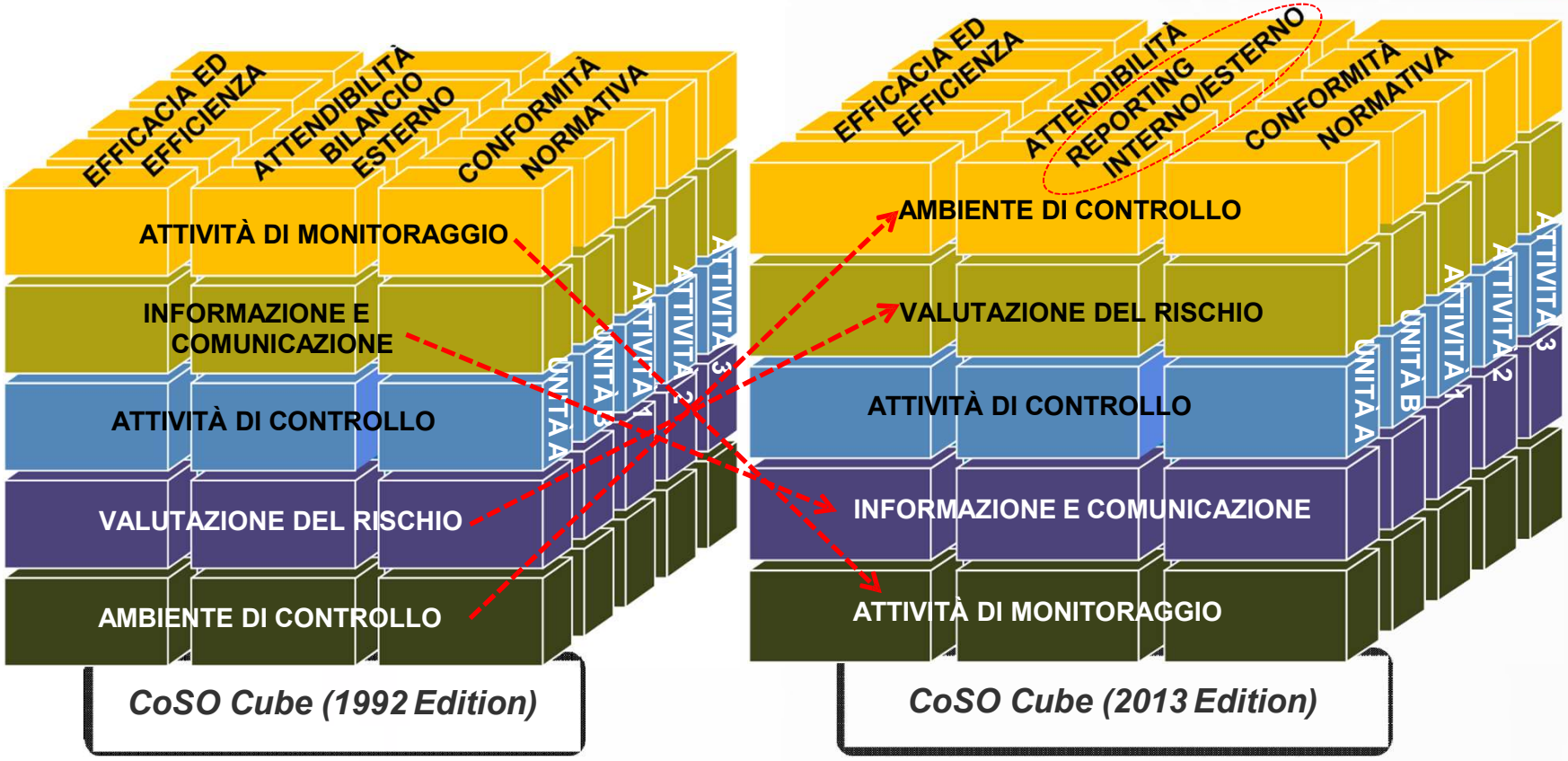
Chiariti meglio i principi di riferimento (Introduzione dei punti di attenzione – *"point of focus"*)

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?

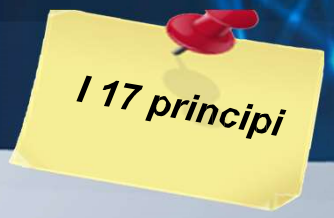
1. La definizione di SCI

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*").



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-

L'ambiente di controllo

AGENDA

1. I principi applicativi dell’ ambiente di controllo
2. I punti di attenzione (PoF/PdA) dell’ambiente di controllo
3. Le questioni aperte
4. Gli aspetti operativi

L'Ambiente di controllo

Esprime **la cultura** e i valori di fondo dell'organizzazione.

Determina il livello di sensibilità del personale alla necessità di controllo ed è influenzato da fattori quali:

- modelli di assegnazione di autorità e responsabilità;
- stili di direzione del management (integrità, valori etici, rigidità di valutazione);
- presenza di organi amministrativi indipendenti dalle direzioni esecutive;
- competenza degli operatori;
- chiara indicazione degli obiettivi.

È costituito da **5** principi

E da **20** punti di attenzione (PoF/PdA)

AMBIENTE DI CONTROLLO

Principi		Punti di attenzione (Point of focus)	
1	**L'organizzazione dimostra il proprio impegno rispetto ai valori etici e all'integrità**	1.1	Definisce il "*Tone at the top*"
		1.2	Definisce degli standard di Condotta
		1.3	Valuta il rispetto degli standard di condotta
		1.4	Affronta tempestivamente le devianze
2	**Il CdA è indipendente rispetto al Management ed esercita la propria supervisione sullo sviluppo e sull'implementazione del SCI**	2.1	Stabilisce responsabilità di supervisione
		2.2	Applica competenze specifiche
		2.3	Opera in modo indipendente
		2.4	Esercita la supervisione sulle componenti del SCI
3	**Il Management definisce, sotto la supervisione del CdA, la struttura organizzativa, le linee di riporto, i livelli autorizzativi e le responsabilità funzionali al fine di perseguire gli obiettivi aziendali**	3.1	Considera tutte le strutture dell'entità
		3.2	Definisce le linee di riporto
		3.3	Definisce, assegna e limita i poteri e le responsabilità
4	**L'organizzazione dimostra il proprio impegno ad attrarre, sviluppare e trattenere risorse competenti, in linea con il conseguimento degli obiettivi aziendali**	4.1	Stabilisce politiche e prassi
		4.2	Valuta le competenze e affronta le carenze
		4.3	Attrae, sviluppa e trattiene le risorse
		4.4	Pianifica e prepara le successioni/sostituzioni
5	**L'organizzazione, nel raggiungimento degli obiettivi aziendali, ritiene i singoli individui responsabili per la parte di SCI di propria competenza.**	5.1	Rafforza le responsabilità attraverso strutture e poteri
		5.2	Definisce misure di performance, incentivi e premi
		5.3	Valuta misure di performance, incentivi e premi
		5.4	Valuta eccessive pressioni
		5.5	Valuta le performance e i premi o sanziona le risorse

Gli aspetti operativi per l'adeguatezza dell'Ambiente di controllo: i principi 1 e 2

1. Integrità e valori etici

Points of Focus o Punti di Attenzione:

1. *Definisce il "Tone at the top"*
2. *Definisce degli standard di condotta*
3. *Valuta il rispetto degli standard di condotta*
4. *Affronta tempestivamente le devianze*

Il Board e il Management di ogni livello dimostrano in tutte le loro attività giornaliere («*on a day-to-day basis*») l'attitudine al rispetto dei valori di eticità e di integrità «fare ciò che è corretto, non solo ciò che è stabilito dalla legge o dal regolamento».
Il Board definisce un adeguato Codice Etico, oggetto di continuo aggiornamento, opportunamente diffuso in azienda, agli «*outsourced services providers*» e ai «*business partner*».

2. Attività di supervisione "*oversight*" del Board e di indipendenza dal Management

Points of Focus o Punti di Attenzione:

1. *Stabilisce responsabilità di supervisione*
2. *Applica competenze specifiche*
3. *Opera in modo indipendente*
4. *Esercita la supervisione sulle componenti del SCI*

Il Board agisce in qualità di supervisore del SCI assegnando opportuni poteri e responsabilità al Management. Verifica le proprie competenze e opera con un adeguato livello di indipendenza dal Management.
Il Board mantiene la supervisione per la progettazione, realizzazione e gestione del SCI, definendo le linee guida dei 5 componenti che lo costituiscono.

Gli aspetti operativi per l'adeguatezza dell'Ambiente di controllo: i principi 3 e 4

3. Struttura organizzativa, linee di riporto, deleghe, poteri e responsabilità

Points of Focus o Punti di Attenzione:

1. *Considera tutte le strutture dell'entità*
2. *Definisce le linee di riporto*
3. *Definisce, assegna e limita i poteri e le responsabilità*

Il Management è tenuto a definire («establishes») un'appropriata struttura organizzativa (poteri, responsabilità, linee di riporto, di <u>tutte</u> le strutture societarie, inclusi gli "*outsourced service providers*").

4. Attrarre, formare e mantenere risorse competenti

Points of Focus o Punti di Attenzione:

1. *Stabilisce politiche e prassi*
2. *Valuta le competenze e affronta le carenze*
3. *Attrae, sviluppa e trattiene le risorse*
4. *Pianifica e prepara le successioni/sostituzioni*

L'entità è tenuta a definire («establishes») adeguate politiche e prassi relative al processo di selezione, formazione e rotazione del personale.
Il Board e il Management valutano il livello di «competenza» ritenuto adeguato per lo svolgimento delle attività, anche degli «*outsourced service providers*" e si attiva in caso di "deficiencies" riscontrate per risolverle.
Il Senior Management e il Board valutano "*contingency plans*" per la sostituzione/successione di risorse chiave anche esterne all'entità.

Gli aspetti operativi per l'adeguatezza dell'Ambiente di controllo: il principio 5

5. Responsabilizzazione delle risorse

Points of Focus o Punti di Attenzione:

1. ***Rafforza le responsabilità attraverso strutture e poteri***
2. ***Definisce misure di performance, incentivi e premi***
3. ***Valuta misure di performance, incentivi e premi***
4. ***Valuta eccessive pressioni***
5. ***Valuta le performance e i premi o sanziona le risorse***

Il Management e il Board definiscono adeguate strutture organizzative che attribuiscono chiare responsabilità di controllo ai vari livelli dell'entità e se non efficacemente operanti, stabiliscono degli idonei correttivi. Definiscono inoltre e valutano misure di performance, incentivi e premi coerenti con gli obiettivi sia a breve che a lungo termine per tutti i livelli dell'entità.
Il Management e il Board valutano la presenza di eccessive «pressioni» contenute nel sistema incentivante, che potrebbero favorire sia inadeguate performance che incoraggiare le frodi.

ESEMPLIFICAZIONE

AMBIENTE DI CONTROLLO

PRINCIPIO AC 1	Test PoF - Points of Focus PdA - Punti di Attenzione -	1	2	3	4	5
1.Integrità e valori etici **AC1.1 Definisce il "Tone at the top"** **AC1.2 Definisce degli standard di condotta** **AC1.3 Valuta il rispetto degli standard di condotta** **AC1.4 Affronta tempestivamente le devianze**	**AC1.1** La gestione del Board e del Senior management, improntata a criteri di integrità ed eticità, fornisce una valida guida/esempio a tutti i livelli organizzativi					
	AC1.1 I subfornitori/business partners/outsourced service providers, cui sono affidate funzioni/attività chiave sono dotati di adeguati standard etici					
	AC1.2 E' stato approvato un Codice Etico, che è oggetto di continuo aggiornamento					
	AC1.2 Il Codice Etico è adeguatamente diffuso all'interno ed all'esterno dell'organizzazione					
	AC1.3 Sono definiti indicatori volti a monitorare il rispetto del Codice Etico					
	AC1.3 Sono previste funzioni incaricate di verificare il rispetto del Codice Etico					
	AC1.4 Le devianze dal Codice Etico eventualmente riscontrate sono affrontate tempestivamente					
	AC1.4 I provvedimenti relativi al mancato rispetto del Codice Etico rappresentano un forte deterrente					

1 = inadeguato; 2 = marginale; 3 = sufficiente; 4 = soddisfacente; 5 = forte

ESEMPLIFICAZIONE

AMBIENTE DI CONTROLLO

PRINCIPIO AC 1	Test PoF - Points of Focus PdA - Punti di Attenzione -	1	2	3	4	5
1.Integrità e valori etici **AC1.1 Definisce il "Tone at the top"** **AC1.2 Definisce degli standard di condotta** **AC1.3 Valuta il rispetto degli standard di condotta** **AC1.4 Affronta tempestivamente le devianze**	**AC1.1** La gestione del Board e del Senior management, è improntata a criteri di integrità ed eticità, fornisce una valida guida/esempio a tutti i livelli organizzativi					X
	AC1.1 I subfornitori/business partners/outsourced service providers, cui sono affidate funzioni/attività chiave sono dotati di adeguati standard etici				X	
	AC1.2 E' stato approvato un Codice Etico, che è oggetto di continuo aggiornamento					X
	AC1.2 Il Codice Etico è adeguatamente diffuso all'interno ed all'esterno dell'organizzazione				X	
	AC1.3 Sono definiti indicatori volti a monitorare il rispetto del Codice Etico				X	
	AC1.3 Sono previste funzioni incaricate di verificare il rispetto del Codice Etico					X
	AC1.4 Le devianze dal Codice Etico eventualmente riscontrate sono affrontate tempestivamente					X
	AC1.4 I provvedimenti relativi al mancato rispetto del Codice Etico rappresentano un forte deterrente				X	

1 = inadeguato; 2 = marginale; 3 = sufficiente; 4 = soddisfacente; 5 = forte

Risultati dei controlli dei test ("Summary of Controls") afferenti il Principio AC 1:

La società ha una storia di integrità e di comportamento etico, in tutta la sua organizzazione.Tutti i dipendenti, i business partners, gli "outsourced service providers" principali, devono dare prova di conoscere e correttamente applicare il Codice Etico della Società, che viene costantemente aggiornato e valutato.

- il Framework dedica 5 principi e 20 POF («*l'importanza della governance è stata aumentata* - «*oversight board*»);
- risulta molto improbabile trovare adeguatamente funzionante un SCI in presenza di una inadeguatezza del componente «Ambiente di Controllo»;
- management override of controls;
- sono molto efficaci per questo componente gli «Entity Level Controls»;
- non è sempre agevole valutare l'efficacia di questo componente.

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

La valutazione del rischio

AGENDA

1. I principi applicativi della valutazione del rischio
2. I PoF/PdA della valutazione dei rischi
3. Le questioni aperte
4. Gli aspetti operativi

La Valutazione del rischio

Attiene alla capacità della direzione di identificare le situazioni di rischio che hanno delle ripercussioni sul mancato/parziale raggiungimento degli obiettivi aziendali e di progettare controlli ad hoc che consentano di fronteggiare tali situazioni di rischio.

È costituito da **4** principi

E da **27** punti di attenzione (PoF/PdA)

VALUTAZIONE DEL RISCHIO

Principi		Punti di Attenzione/Point of Focus	
6	**L'organizzazione esplicita con sufficiente chiarezza i propri obiettivi, consentendo l'identifiazione e la valutazione dei rischi ad essi legati**		
	- obiettivi operativi	6.1	Riflettono le scelte del management
		6.2	Considerano la tolleranza al rischio definita dall'organizzazione
		6.3	Includono gli obiettivi operativi e di performance finanziaria
		6.4	Costituiscono la base per il *commitment* delle risorse
	- obiettivi di informativa finanziaria esterna	6.5	Rispettano i principi contabili applicabili
		6.6	Considerano i livelli di materialità
		6.7	Riflettono le attività dell'entità
	- obiettivi di informativa non finanziaria esterna	6.8	Rispettano gli *standards* e i *frameworks* più diffusi
		6.9	Tengono conto del livello di precisione richiesto
		6.10	Riflettono le attività dell'entità
	- obiettivi di reporting interno	6.11	Riflettono le scelte del management
		6.12	Tengono conto del livello di precisione richiesto
		6.13	Riflettono le attività dell'entità
	- obiettivi di compliance	6.14	Riflettono le leggi ed i regolamenti in vigore
		6.15	Considerano la tolleranza al rischio definita dall'organizzazione

I Principi applicativi e i PoF/PdA della Valutazione del rischio (Principi 7-8-9)

VALUTAZIONE DEL RISCHIO

Principi		Punti di attenzione (Point of focus)	
7	**L'organizzazione identifica i rischi connessi al conseguimento degli obiettivi aziendali e ne determina le modalità di gestione**	7.1	L'analisi è svolta a livello di entità, subsidiaries divisioni, unità operative e funzioni
		7.2	L'organizzazione analizza i fattori interni ed esterni
		7.3	Vengono coinvolti livelli appropriati di management
		7.4	Viene valutata la significatività dei rischi identificati
		7.5	Vengono determinate le risposte ai rischi
8	**L'organizzazione prende in considerazione potenziali frodi nel valutare i rischi di conseguimento dei propri obiettivi aziendali**	8.1	Considera i vari tipi di frode
		8.2	Valuta gli incentivi e le pressioni
		8.3	Valuta le opportunità
		8.4	Valuta i comportamenti e le giustificazioni
9	**L'organizzazione identifica e valuta i cambiamenti che potrebbero avere impatti significativi sul Sistema di Controllo Interno**	9.1	Valuta i cambiamenti nell'ambiente esterno
		9.2	Valuta i cambiamenti nel modello di business
		9.3	Valuta i cambiamenti nella leadership

Gli aspetti operativi per l'adeguatezza della Valutazione del rischio: il principio 6

6. Definizione di chiari obiettivi da perseguire

Obiettivi Operativi (PoF o PdA):

1. ***Riflettono le scelte del Management***
2. ***Considerano la tolleranza al rischio definita dall'organizzazione***
3. ***Includono gli obiettivi operativi e di performance finanziaria***
4. ***Costituiscono la base per il «commitment» delle risorse***

Gli obiettivi operativi riflettono le scelte del Management riguardanti la struttura, il settore di riferimento, e le performance dell'entità.
Il Management considera la tolleranza al rischio, ovvero l'accettabile livello di variazione relativo all'obiettivo prefissato.
Il Management utilizza gli obiettivi operativi come base per allocare le risorse necessarie per ottenere i desiderati livelli di performance operativa e/o finanziaria.
Va da sé che se gli obiettivi operativi di un'entità non sono chiari e ben delineati, le risorse possono essere male indirizzate («*misdirected*»).

Obiettivi di informativa finanziaria esterna (PoF o PdA):

5. ***Rispettano i principi contabili applicabili***
6. ***Considerano i livelli di materialità***
7. ***Riflettono le attività dell'entità***

Attengono agli obiettivi di attendibilità sostanziale dell'informativa finanziaria (es. il bilancio).

6. Definizione di chiari obiettivi da perseguire (segue)

Obiettivi di informativa non finanziaria esterna (3 PoF o PdA):

8.Rispettano gli standards e i frameworks più diffusi

9.Tengono conto del livello di precisione richiesto

10. Riflettono le attività dell'entità

Obiettivi di reporting interno (3 PoF o PdA):

11.Riflettono le scelte del management

12.Tengono conto del livello di precisione richiesto

13. Riflettono le attività dell'entità

Obiettivi di compliance (2 PoF o PdA):

14.Riflettono le leggi ed i regolamenti in vigore

15.Considerano la tolleranza al rischio definita dall'organizzazione

Gli aspetti operativi per l'adeguatezza della Valutazione del rischio: i principi 7 e 8

7. Identificazione e analisi dei rischi

Points of Focus o Punti di Attenzione (PoF o PdA):

1.L'analisi è svolta a livello di entità, subsidiaries, divisioni, unità operative e funzioni

2. ***L'organizzazione analizza i fattori interni ed esterni***
3. ***Vengono coinvolti livelli appropriati di management***
4. ***Viene valutata la significatività dei rischi identificati***
5. ***Vengono determinate le risposte ai rischi***

8. Valutazione dei rischi di frode

Points of Focus o Punti di Attenzione (PoF o PdA):

1. ***Considera i vari tipi di frode***
2. ***Valuta gli incentivi e le pressioni***
3. ***Valuta le opportunità***
4. ***Valuta i comportamenti e le giustificazioni***

La valutazione delle frodi, comprende il «*fraudulent reporting*», la possibile perdita di beni «*misappropriation of assets*» e l'attività di corruzione «*illegal acts*», derivante da qualsiasi forma di frode o di inappropriato comportamento ("*misconduct*").

I PoF/PdA 8.2-8.3 e 8.4 riguardano essenzialmente il cosiddetto «triangolo della frode» («*fraud triangle*»). Ovvero bisognerà considerare che le motivazioni che spingono un soggetto a compiere un atto fraudolento sono determinate dal concorso congiunto e simultaneo di 3 elementi: i) una pressione percepita; ii) un'opportunità percepita; iii) una o più modalità per la razionalizzazione del comportamento atta a rendere soggettivamente accettabile il medesimo.

9. Identificazione ed analisi del cambiamento

Points of Focus o Punti di Attenzione (PoF o PdA):

1. ***Valuta i cambiamenti nell'ambiente esterno***
2. ***Valuta i cambiamenti nel modello di business***
3. ***Valuta i cambiamenti nella leadership***

Viene esplicitato il concetto che i cambiamenti significativi da qualsiasi fonte provengano, devono essere considerati e valutati nel processo di valutazione dei rischi.

ESEMPLIFICAZIONE

VALUTAZIONE DEI RISCHI (VR 8)

PRINCIPIO VR 8	Test PoF - Points of Focus PdA - Punti di Attenzione -	1	2	3	4	5
8. Valutazione dei rischi di frode **VR8.1 Considera i vari tipi di frode** **VR8.2 Valuta gli incentivi e le pressioni** **VR8.3 Valuta le opportunità** **VR8.4 Valuta i comportamenti e le giustificazioni**	**VR8.1** Sono identificati i fattori che possono accrescere il rischio di frodi contabili (complessità delle transazioni, schemi di frode tipici del business in cui opera l'entità, ecc.)					
	VR8.1 Sono identificati i fattori che possono accrescere il rischio correlato alla salvaguardia del patrimonio (uso improprio di asset aziendali, acquisti non autorizzati, furti di magazzino ecc.)					
	VR8.1 Sono identificati i fattori che possono accrescere il rischio di corruzione					
	VR8.2 Sono valutate le motivazioni che potrebbero indurre comportamenti fraudolenti (soddisfazione dei dipendenti, sistema incentivante molto «sfidante» ecc.)					
	VR8.3 Sono valutate le opportunità che possono accrescere il rischio di frode (debolezza dei controlli, mancanza di supervisione, mancata separazione dei compiti, elevato turnover del personale, ecc.)					
	VR8.4 Sono poste in essere le contromisure necessarie per ridurre il rischio di frode entro limiti accettabili (meccanismi di protezione per i denuncianti «*whistleblowing*», hotline dedicate etc.)					

1 = inadeguato; 2 = marginale; 3 = sufficiente; 4 = soddisfacente; 5 = forte

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

L'attività di controllo

AGENDA

1. I principi applicativi dell’attività di controllo
2. I PoF/PdA dell’attività di controllo
3. Le questioni aperte
4. Gli aspetti operativi

L'Attività di Controllo

Sono attuate a tutti i livelli gerarchici e funzionali della struttura organizzativa. Devono rispettare i principi di:

- ❑ **adeguata separazione** dei compiti;
- ❑ corretta **autorizzazione** per tutte le operazioni;
- ❑ adeguata **documentazione** e **registrazione** delle operazioni;
- ❑ **controllo fisico** su beni e registrazioni.

In base al «***timing***» i controlli possono essere distinti in: controlli **preventivi**, controlli **concomitanti**; controlli **successivi**.

È costituito da **3** principi

E da **16** punti di attenzione (PoF/PdA)

ATTIVITA' DI CONTROLLO

Principi		Punti di attenzione	
10	**L'organizzazione definisce ed implementa attività di controllo che contribuiscono a ridurre i rischi entro livelli accettabili**	10.1	La scelta e lo sviluppo sono integrati con la fase di *risk assessment*
		10.2	Considera fattori specifici dell'entità
		10.3	Determina i processi di business rilevanti
		10.4	Valuta un *mix* di tipologie di attività di controllo
		10.5	Valuta a quali livelli devono essere applicati i controlli
		10.6	Presta attenzione alla separazione dei compiti
11	**L'organizzazione definisce e implementa attività di controllo sulla tecnologia, per supportare il raggiungimento degli obiettivi aziendali**	11.1	Determina la dipendenza tra l'uso della tecnologia nei *processi di business* e l'uso della tecnologia nei *controlli generali*
		11.2	Stabilisce importanti attività di controllo riguardanti le infrastrutture tecnologiche
		11.3	Stabilisce importanti attività di controllo sul processo di gestione della sicurezza
		11.4	Stabilisce l'acquisizione, lo sviluppo e la manutenzione di controlli tecnologici di processo
12	**L'organizzazione declina le attività di controllo in politiche che definiscono i comportamenti attesi e in procedure che ne determinano le modalità operative di applicazione**	12.1	Determina politiche e procedure per supportare l'implementazione delle direttive del management
		12.2	Determina responsabilità per l'esecuzione di politiche e procedure
		12.3	Definisce politiche e procedure in modo tempestivo
		12.4	Pone in essere azioni correttive
		12.5	Si avvale di personale competente nella definizione di politiche e procedure
		12.6	Sottopone politiche e procedure a valutazioni periodiche

Gli aspetti operativi per l'adeguatezza della dell'Attività di controllo (Principio 10)

10. Identificazione e sviluppo di adeguate attività di controllo

Point of Focus/ Punti di Attenzione(PoF o PdA):

1. ***La scelta e lo sviluppo sono integrati con la fase di risk assessment***
2. ***Considera fattori specifici dell'entità***
3. ***Determina i processi di business rilevanti***
4. ***Valuta un mix di tipologie di attività di controllo***
5. ***Valuta a quali livelli devono essere applicati i controlli***
6. ***Presta attenzione alla separazione dei compiti***

Per mix di tipologie di attività di controllo, si considerano i controlli *preventivi, concomitanti o successivi* oppure se sono *manuali o automatici*.

Prestare attenzione alla *separazione dei compiti* e ove questa non fosse realizzabile, è richiesto di selezionare e sviluppare alternative attività di controllo.

Gli aspetti operativi per l'adeguatezza della dell'Attività di controllo (Principio 11)

11 Identificazione e sviluppo di adeguate attività di "IT control"

Point of Focus/ Punti di Attenzione

1.Determina la dipendenza tra l'uso della tecnologia nei processi di business e l'uso della tecnologia nei controlli generali

2.Stabilisce importanti attività di controllo riguardanti le infrastrutture tecnologiche

3.Stabilisce le attività di controllo sul processo di gestione della sicurezza

4.Stabilisce l'acquisizione, lo sviluppo e la manutenzione di controlli tecnologici di processo

Il Management determina il livello di correlazione («*linkage*») tra i processi di business, i controlli automatici delle attività e i controlli tecnologici generali («*IT general controls*»).

Il Management seleziona e sviluppa controlli sia sulla infrastruttura tecnologica, sulla gestione della sicurezza nonché sulla sua manutenzione

12 Sviluppare e definire adeguate policy e procedure aziendali di controllo

Point of Focus/ Punti di Attenzione (PoF o PdA):

1.Determina politiche e procedure per supportare l'implementazione delle direttive del management

2. Determina responsabilità per l'esecuzione di politiche e procedure

3. Definisce politiche e procedure in modo tempestivo

4. Pone in essere azioni correttive

5.Si avvale di personale competente nella definizione di politiche e procedure

6. Sottopone politiche e procedure a valutazioni periodiche

ESEMPLIFICAZIONE

ATTIVITA' DI CONTROLLO						
Principio	**Caratteristiche**	**1**	**2**	**3**	**4**	**5**
10. Sviluppo di attività di controllo	➢ Le attività di controllo sono coerenti con la **complessità** dell'organizzazione					
	➢ Le attività di controllo sono coerenti con il grado di **regolamentazione del business**					
	➢ Le attività di controllo sono coerenti con il grado di **outsourcing** dell'organizzazione					
	➢ Le attività di controllo sono coerenti con la ***risk tolerance*** definita dal Board					
	➢ Sono previsti adeguati **controlli di linea** (I livello) diretti ad assicurare il corretto svolgimento delle operazioni					
	➢ E' previsto un adeguato ricorso a **controlli automatici**					
	➢ E' previsto un adeguato livello di **controllo da parte dei livelli organizzativi più elevati** (*performance review,* confronti con i competitors, programmi di *cost reduction*, ecc.)					
	➢ E' prevista un'adeguata **separazione dei compiti**					
	➢ La separazione dei compiti è a sua volta garantita da adeguate attività di controllo					
	➢ E' garantita l'**indipendenza** della funzione di internal audit					
	➢ La struttura organizzativa **sostanziale** è **allineata** alla struttura organizzativa **formale**					
	➢ E' previsto un adeguato monitoraggio **dell'efficacia e del funzionamento dei controlli**					

1 = inadeguato; 2 = marginale; 3 = sufficiente; 4 = soddisfacente; 5 = forte

ESEMPLIFICAZIONE

ATTIVITA' DI CONTROLLO						
Principio	**Caratteristiche**	**1**	**2**	**3**	**4**	**5**
11. Sviluppo di attività di controllo sulla tecnologia	➢ Sono previsti controlli volti a garantire l'affidabilità **della tecnologia** utilizzata sia a supporto dei processi di business (es. impianti produttivi altamente robotizzati) sia per l'automazione delle attività di controllo (es. controllo automatico degli accessi)					
	➢ Sono previsti adeguati piani di backup dei dati/*recovery procedures*					
	➢ Sono previste adeguate attività di controllo (sistemi di autenticazione, ecc.) in merito agli **accessi** alla tecnologia (dati, software, hardware, ecc.), sia da parte di personale interno che da parte di soggetti esterni					
	➢ E' previsto un adeguato processo di gestione dei cambiamenti tecnologici					
	➢ L'acquisizione di tecnologie in ***outsourcing*** è supportata da adeguate attività di controllo relative alla completezza, accuratezza e validità delle informazioni inviate e ricevute dal subfornitore					

1 = inadeguato; 2 = marginale; 3 = sufficiente; 4 = soddisfacente; 5 = forte

ESEMPLIFICAZIONE

ATTIVITA' DI CONTROLLO						
Principio	**Caratteristiche**	**1**	**2**	**3**	**4**	**5**
12. Definizione di politiche e procedure	➢ Sono definite politiche e procedure che garantiscono un'adeguata **identificazione, valutazione e monitoraggio dei rischi**					
	➢ Le politiche e le procedure consentono di identificare e valutare i rischi connessi all'avvio di **nuove attività** e **progetti**					
	➢ Le politiche e le procedure sono **periodicamente revisionate** al fine di tener conto dei **cambiamenti** intercorsi nella strategia, negli obiettivi e nei rischi dell'organizzazione					
	➢ Le politiche e le procedure sono formalizzate e gestite in modo **documentato**					
	➢ Le politiche e le procedure sono adeguatamente **comunicate** all'interno dell'organizzazione					
	➢ Non si registrano **eccezioni** relative all'applicazione di politiche e procedure					
	➢ Le **azioni correttive** delle anomalie emerse dall'applicazione delle procedure sono poste in essere **tempestivamente**					
	➢ Le **azioni correttive** delle anomalie emerse dall'applicazione delle procedure coinvolgono adeguati **livelli gerarchici**					
	➢ Le politiche e le procedure sono coerenti con la **competenza ed esperienza del management**					
	➢ Le politiche e le procedure assicurano un'adeguata **responsabilizzazione** delle risorse					
	➢ Le politiche e le procedure assicurano il **rispetto delle leggi e dei regolamenti**					

1 = inadeguato; 2 = marginale; 3 = sufficiente; 4 = soddisfacente; 5 = forte

- il Framework introduce per la prima volta il concetto di IT CONTROLS (sicurezza e accessi, cambiamenti tecnologici sempre in corso…)
- è molto legato al componente «Ambiente di Controllo»;
- L'IT control (principio 11) in modo specifico è un principio molto «integrato» con gli altri. Se si verificano delle «deficiencies» in questo principio, gli effetti si propagano anche negli altri componenti;
- necessità di competenze specifiche «IT» e adeguate risorse.

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

Informazione e comunicazione

AGENDA

1. I principi applicativi dell'informazione e comunicazione («sistema informativo»)
2. I PoF/PdA del sistema informativo
3. Le questioni aperte
4. Gli aspetti operativi

Informazione e comunicazione

Deve consentire la tempestiva individuazione, rilevazione e diffusione delle informazioni utili alle persone per adempiere alle proprie responsabilità; le informazioni sono considerate utili quando sono **significative, affidabili, tempestive e accessibil**i.

È costituito da **3** principi

E da **14** punti di attenzione (PoF/PdA)

INFORMAZIONE E COMUNICAZIONE

Principi		Punti di attenzione	
13	**L'organizzazione ottiene o genera e utilizza informazioni rilevanti e di qualità a supporto del funzionamento del Sistema di Controllo Interno**	13.1	Identifica i requisiti delle informazioni
		13.2	Acquisisce dati da fonti interne ed esterne
		13.3	Elabora i dati rilevanti trasformandoli in informazioni
		13.4	Conserva la qualità dei dati durante il loro trattamento
		13.5	Considera costi e benefici
14	**L'organizzazione comunica internameante le informazioni, compresi gli obiettivi e le responsabilità di controllo interno, necessarie a supportare il funzionamento del sistema nel suo complesso**	14.1	Comunica le informazioni relative al controllo interno
		14.2	Comunica con il Board
		14.3	Organizza linee di comunicazione separate
		14.4	Sceglie metodi di comunicazione appropriati
15	**L'organizzazione comunica con parti terze relativamente a questioni che interessano il funzionamento del sistema di controllo interno**	15.1	Comunica con l'esterno
		15.2	Consente comunicazioni in entrata
		15.3	Comunica con il Board
		15.4	Organizza linee di comunicazione separate
		15.5	Sceglie metodi di comunicazione appropriati

13. Utilizzo di informazioni affidabili e rilevanti

Points of Focus o Punti di Attenzione (PoF o PdA):

1. *Identifica i requisiti delle informazioni*
2. *Acquisisce dati da fonti interne ed esterne*
3. *Elabora i dati rilevanti trasformandoli in informazioni*
4. *Conserva la qualità dei dati durante il loro trattamento*
5. *Considera i costi e i benefici*

14. Adeguate comunicazioni interne

Points of Focus o Punti di Attenzione (PoF o PdA):

1. *Comunica le informazioni relative al controllo interno*
2. *Comunica con il Board*
3. *Organizza linee di comunicazione separate*
4. *Sceglie metodi di comunicazione appropriati*

15. Adeguate comunicazioni esterne

Points of Focus o Punti di Attenzione (PoF o PdA):

1. *Comunica con l'esterno*
2. *Consente comunicazioni in entrata*
3. *Comunica con il Board*
4. *Organizza linee di comunicazione separate*
5. *Sceglie metodi di comunicazione appropriati*

ESEMPI DI POSSIBILI TEST DI AUTOVALUTAZIONE SUL PRINCIPIO 13

SISTEMA INFORMATIVO						
Principio	**Caratteristiche**	**1**	**2**	**3**	**4**	**5**
13. Utilizzo di informazioni affidabili e rilevanti	➢ Il management identifica nel continuo i **requisiti** e l'**ampiezza** delle informazioni necessarie per il funzionamento delle altre componenti del sistema di controllo interno					
	➢ I requisiti e l'ampiezza delle informazioni sono coerenti con la **struttura organizzativa**, il **modello di business**, l'**ambiente competitivo** e gli **obiettivi** dell'entità					
	➢ Il management identifica nel continuo **fonti informative** affidabili ed adeguate					
	➢ Il grado di sofisticazione del **sistema informativo** (**persone, processi e tecnologia**) è commisurato alla complessità ed alle esigenze dell'organizzazione					
	➢ Il sistema informativo fa affidamento a **tecnologie** integrate nei processi di business che consentono di incrementare l'**efficienza** e l'**accessibilità** delle informazioni					
	➢ Il sistema informativo prevede meccanismi di **controllo degli accessi** volti a garantire la privacy e la sicurezza delle informazioni					
	➢ Le informazioni utilizzate sono **sufficienti**					
	➢ Le informazioni utilizzate sono **tempestive** ed **aggiornate**					
	➢ Le informazioni utilizzate sono **verificabili** e **documentate**					
	➢ Le informazioni sono **conservate** per un adeguato periodo di tempo					
	➢ Le informazioni consentono di **identificare i rischi** attraverso opportune **analisi di trend**					
	➢ Il management definisce **politiche di gestione delle informazioni** che attribuiscono chiare **responsabilità** in merito alla **qualità** delle informazioni					
	➢ Le informazioni sono soggette a specifiche attività di controllo volte a verificarne la **qualità**, l'**affidabilità** e la **coerenza**					

ESEMPI DI POSSIBILI TEST DI AUTOVALUTAZIONE SUL PRINCIPIO 14

SISTEMA INFORMATIVO						
Principio	**Caratteristiche**	**1**	**2**	**3**	**4**	**5**
14. Comunicazioni interne	➢ Sono definite **politiche** e **procedure** che facilitano comunicazioni interne efficaci					
	➢ Le comunicazioni interne facilitano l'**identificazione di problemi/rischi**, consentendo di individuarne le **cause** e di porre in essere le opportune **azioni correttive**					
	➢ Le modalità con cui avvengono le comunicazioni interne (e-mail, discussioni *one to one*, ecc.) consentono una trasmissione delle informazioni **chiara**, **tempestiva** ed **efficace**					
	➢ La scelta delle modalità di comunicazione sono effettuate sulla base delle **esigenze di conservazione** dettate da leggi e regolamenti					
	➢ Sono previsti incontri/comunicazioni diretti tra il **Board** ed il **personale,** senza filtro da parte del management					
	➢ Per determinate tematiche (violazione del codice etico, ecc.) sono previsti **canali di comunicazione differenti** dal tradizionale riporto gerarchico					
	➢ E' prevista una **valutazione periodica** dell'efficacia delle comunicazioni interne (es. nell'ambito del processo di valutazione delle performance del personale)					
	➢ La reportistica interna è **accurata** ed **affidabile**					
	➢ La reportistica interna è **tempestiva**					
	➢ La reportistica interna consente il monitoraggio di **tutti i rischi rilevanti**					
	➢ La reportistica interna consente la verifica del **rispetto dei limiti di rischio** prestabiliti					
	➢ E' prevista una reportistica periodica sulla **sostenibilità del business**					

ESEMPI DI POSSIBILI TEST DI AUTOVALUTAZIONE SUL PRINCIPIO 15

SISTEMA INFORMATIVO						
Principio	**Caratteristiche**	**1**	**2**	**3**	**4**	**5**
15 Comunicazioni con l'esterno	➢ Sono previsti opportuni **canali informativi bidirezionali** con i differenti *stakeholders* esterni (clienti, Enti di regolamentazione, analisti finanziari, ecc.)					
	➢ Sono definite **politiche** e **procedure** che facilitano efficaci comunicazioni con l'esterno					
	➢ Le comunicazioni verso l'esterno trasmettono chiaramente i **valori** e la **cultura** dell'organizzazione					
	➢ Le **responsabilità** relative alle comunicazioni e al trattamento dei dati nell'ambito di **servizi affidati in *outsourcing*** sono chiare e ben definite					
	➢ La scelta delle modalità di comunicazione sono effettuate sulla base delle **esigenze di conservazione** dettate da leggi e regolamenti					
	➢ Le comunicazioni con l'esterno garantiscono il rispetto delle **leggi** e dei **regolamenti**					
	➢ Sono previsti opportuni **canali informativi bidirezionali** con i differenti *stakeholders* esterni (clienti, Enti di regolamentazione, analisti finanziari, ecc.)					
	➢ Sono definite **politiche** e **procedure** che facilitano efficaci comunicazioni con l'esterno					
	➢ Le comunicazioni verso l'esterno trasmettono chiaramente i **valori** e la **cultura** dell'organizzazione					
	➢ Le **responsabilità** relative alle comunicazioni e al trattamento dei dati nell'ambito di **servizi affidati in *outsourcing*** sono chiare e ben definite					
	➢ La scelta delle modalità di comunicazione sono effettuate sulla base delle **esigenze di conservazione** dettate da leggi e regolamenti					
=	➢ Le comunicazioni con l'esterno garantiscono il rispetto delle **leggi** e dei **regolamenti**					

- viene posta enfasi sulla selettività e rilevanza delle informazioni;
- flussi informativi;
- è molto legato ai sistemi IT, alla «*data integrity*»;
- enfasi sulla corretta «comunicazione» sia interna che esterna;
- è molto legato alle attività di controllo

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

L'attività di monitoraggio

AGENDA

1. I principi applicativi dell'attività di monitoraggio
2. I PoF/PdA dell'attività di monitoraggio
3. Le questioni aperte
4. Gli aspetti operativi

Consiste nella verifica **continuativa** o **periodica** dell'efficacia del **disegno** dei controlli interni e dell'effettiva **operatività** dei medesimi, resa necessaria dalla dinamicità del contesto all'interno del quale è inserito il sistema dei controlli.

È costituito da **2** principi

E da **10** punti di attenzione (PoF/PdA)

I Principi applicativi e i PoF/PdA delle Attività di Monitoraggio

ATTIVITA' DI MONITORAGGIO

Principi		Punti di attenzione	
16	**L'organizzazione definisce, sviluppa ed esegue valutazioni continuative e *ad hoc per* accertare che le componenti del SCI siano presenti e funzionanti**	16.1	Considera un mix di *ongoing* e *separate evaluations*
		16.2	Considera il grado di cambiamento
		16.3	Determina una visione di base
		16.4	Utilizza personale ben informato
		16.5	Integra con i processi di business
		16.6	Adatta scopi e frequenze
		16.7	Valuta in modo obiettivo
17	**L'organizzazione valuta e comunica tempestivamente le carenze del SCI ai soggetti responsabili di intraprendere le necessarie azioni correttive, incluso il Senior Management ed il CdA per quanto necessario e di competenza**	17.1	Valuta i risultati
		17.2	Comunica le carenze ai soggetti responsabili di porre in essere le azioni correttive, al senior management ed al Board
		17.3	Monitora l'implementazione delle azioni correttive

16. Monitoraggio continuo e/o indipendenti valutazioni (7 PoF/PdA)

Points of Focus o Punti di Attenzione (PoF o PdA):

1. *Considera un mix di ongoing e separate evaluations*
2. *Considera il grado di cambiamento*
3. *Determina una visione di base*
4. *Utilizza personale ben informato*
5. *Integra con i processi di business*
6. *Adatta scopi e frequenze*
7. *Valuta in modo obiettivo*

17. Valutazione, comunicazione e correzione delle carenze del SCI (3 PoF/PdA)

Points of Focus o Punti di Attenzione (PoF o PdA):

1. *Valuta i risultati*

2.Comunica le carenze ai soggetti responsabili di porre in essere le azioni correttive, al senior management ed al Board

Comunica con il Board

3. *Monitora l'implementazione delle azioni correttive*

Esempi di possibili test di autovalutazione sul principio 16

ESEMPLIFICAZIONE

ATTIVITÀ DI MONITORAGGIO						
Principio	**Caratteristiche**	**1**	**2**	**3**	**4**	**5**
16. Ongoing monitoring e separate evaluations	➢ L'implementazione ed il funzionamento delle componenti del sistema di controllo interno è oggetto di **monitoraggio continuo** (***ongoing monitoring*** insito nei processi) e di **valutazioni periodiche** (***separate evaluations*** realizzate in modo indipendente dall'internal audit)					
	➢ Le valutazioni periodiche (*separate evaluations*) sono effettuate con una frequenza coerente con la profondità del monitoraggio continuo posto in essere dall'organizzazione e con la rapidità del cambiamento					
	➢ Il sistema di controllo interno è **periodicamente aggiornato** al fine di tener conto dei **cambiamenti** dell'ambiente esterno, del contesto competitivo, degli obiettivi dell'organizzazione e dei rischi a cui quest'ultima è esposta					
	➢ Sono effettuate valutazioni periodiche della capacità del sistema di controllo interno di gestire i rischi più significativi					
	➢ L'attività di monitoraggio continuo è supportata da un adeguato utilizzo della **tecnologia**					
	➢ La **copertura**, le **procedure** e le **risultanze** delle *separate evaluations*, nonché le relative **risposte**, sono adeguatamente documentate					
	➢ Sono poste in essere adeguate attività di monitoraggio dell'affidabilità dei controlli posti in essere dai fornitori di servizi in *outsourcing*					

1 = inadeguato; 2 = marginale; 3 = sufficiente; 4 = soddisfacente; 5 = forte

Esempi di possibili test di autovalutazione sul principio 17

ESEMPLIFICAZIONE

ATTIVITÀ DI MONITORAGGIO							
Principio	**Caratteristiche**	**1**	**2**	**3**	**4**	**5**
17. Valutazione, comunicazione correzione delle carenze del sistema di controllo interno	➢ Le carenze (e le eventuali opportunità di miglioramento) del sistema di controllo interno sono **riportate ad adeguati livelli gerarchici**					
	➢ Le carenze (e le eventuali opportunità di miglioramento) del sistema di controllo interno sono oggetto di **tempestive azioni correttive**					
	➢ L'implementazione delle **azioni correttive** è monitorata da opportuni livelli gerarchici					

1 = inadeguato; 2 = marginale; 3 = sufficiente; 4 = soddisfacente; 5 = forte

- **è sotto la responsabilità del Management**

- **è in stretta correlazione sia con il Sistema Informativo che con l’Ambiente di controllo;**
- **nel 2009 il CoSO aveva emesso un documento dal titolo: «*Guidance on Monitoring Internal Control System”* tuttora in vigore che dimostra l’attenzione su tale componente;**
- **è cruciale in quanto può mitigare in tutto o in parte, delle deficiencies («monitoring controls») emerse in altri componenti e/o principi.**