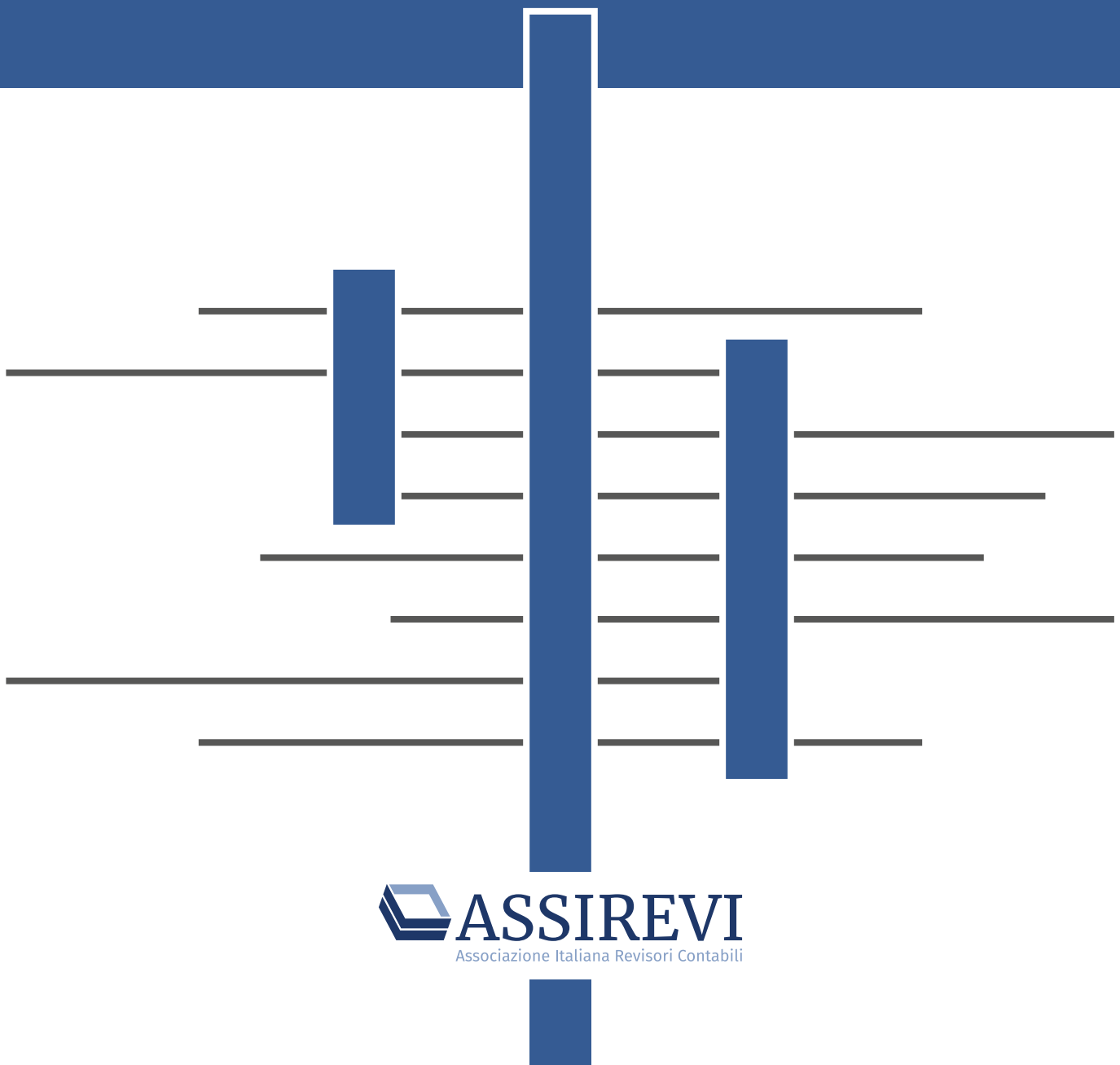
ASSIREVI

MONOGRAFIE

COSO Framework:
guida alla lettura

n°1 - Gennaio 2019



ASSIREVI
Associazione Italiana Revisori Contabili

Indice

PREMESSA

Il Sistema di Controllo Interno quale elemento centrale della *corporate governance*

Il Sistema di Controllo Interno (SCI) assume oggi un ruolo centrale nell'ambito della *corporate governance* aziendale, ovvero del complesso di regole esterne ed interne che influenzano la vita delle imprese.

Nell'ultimo decennio, anche in virtù della crisi finanziaria che ha interessato i mercati e le economie di tutto il mondo, esso ha subito significative evoluzioni nella direzione dell'integrazione, in prima istanza con i processi di gestione del rischio e, più in generale, nei processi aziendali e nell'assetto organizzativo complessivo dell'impresa. Difatti, la sua definizione corrente si riferisce al Sistema di controllo interno e di gestione dei rischi (SCIGR) come un *unicum* e riguarda l'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 Consiglio di Amministrazione ha pertanto una responsabilità primaria sul SCIGR che, qualora venisse valutato carente o non adeguato rispetto al profilo di rischio dell'impresa, determinerebbe un deficit organizzativo rilevante con ricadute sull'impresa stessa (per esempio ai sensi del D.Lgs. 231/01), ma anche sui singoli amministratori.

L'adeguatezza del SCIGR è dunque riferita ai rischi che l'impresa decide di assumere; essa dipende dalla solidità dei processi aziendali e dei relativi presidi di controllo, ma anche dalla capacità dell'impresa di affrontare e adattarsi ai cambiamenti degli scenari di rischio che caratterizzano i mercati in cui opera.

Le cause dei cambiamenti sono riconducibili principalmente a una crescente e più severa competizione, al progresso tecnologico che determina profonde discontinuità nelle filiere produttive e nello stile di vita dei consumatori, a condizioni di instabilità politica e macro-economica e alla conseguente sempre maggiore pressione degli enti regolatori e dei legislatori. È inoltre importante considerare anche i fattori di rischio di lungo periodo, ivi inclusi quelli connessi ai cosiddetti macro-trend (ad esempio al sovra-popolamento del pianeta, all'invecchiamento della popolazione e alla sostenibilità dei sistemi di *welfare*, ai cambiamenti climatici, alla scarsità di risorse energetiche ed idriche), i cui effetti sono apparentemente meno preoccupanti in quanto attesi in un orizzonte temporale più lungo.

Inoltre vanno considerate, tra le cause dell'incremento della volatilità e dell'incertezza dei mercati, l'interconnessione e la velocità con cui i rischi si propagano: un evento che accade in un mercato o in una geografia, attraverso percorsi non sempre prevedibili, può produrre conseguenze indirette anche in settori ed aree molto distanti.

Infine, per completare il quadro, non si può fare a meno di valutare le conseguenze reputazionali dei rischi, i cui effetti sono talvolta di gran lunga superiori alle perdite economiche e, in taluni casi, assumono dimensioni catastrofiche.

Gli attori del Sistema di Controllo Interno

Analizzati tali fattori, è di primaria importanza per le imprese istituire e mantenere un efficace ed efficiente SCIGR; il Consiglio di Amministrazione, nel suo ruolo di indirizzo strategico, è chiamato a definire le linee di indirizzo del SCIGR e a vigilare (*oversight*) sulla loro effettiva attuazione, valutando periodicamente l'adeguatezza complessiva del SCIGR rispetto al profilo di rischio dell'impresa e ai suoi obiettivi strategici.

Naturalmente la gestione e il controllo dei rischi sono affidati al *management* dell'impresa che, nell'ambito delle proprie deleghe e nei processi aziendali di competenza, deve fornire il proprio contributo secondo un assetto definito nella letteratura aziendalista come il

"modello delle tre linee di controllo o di difesa". Va rilevato che la validità di tale modello è riconosciuta anche in taluna normativa secondaria che ad esso si riferisce.

Infatti, la prima linea di controllo riguarda il *management* operativo, cosiddetti *risk owner*; spetta a loro il compito di implementare ed eseguire i controlli di processo necessari alla gestione dei rischi nelle attività *day-to-day*.

La seconda linea di controllo è composta dalle cosiddette funzioni di controllo, ossia da funzioni aziendali caratterizzate da autonomia di giudizio e limitata indipendenza che svolgono attività di monitoraggio dei rischi e dei controlli a supporto del *management* operativo (prima linea di controllo); tali funzioni possono essere molteplici in relazione al settore di attività e alla rilevanza del rischio quali, ad esempio, le funzioni di *risk management*, *compliance*, controllo di gestione, *security*, qualità, sicurezza sul lavoro, ecc.

Infine, la terza linea di controllo può essere rappresentata dalla funzione di *Internal Audit,* che ha il compito di svolgere un monitoraggio indipendente, non potendole essere affidato alcun compito operativo, sull'adeguatezza del Sistema di controllo interno e di gestione dei rischi e di riferire direttamente al Consiglio di Amministrazione e/o al Vertice.

In tale complesso e articolato contesto, diviene necessario per le imprese identificare un modello di *leading practice* al quale fare riferimento per sviluppare e valutare nel continuo l'adeguatezza del proprio SCI.

Il COSO *Framework* quale modello di riferimento del Sistema di Controllo Interno

Il più autorevole tra i modelli di controllo interno a livello internazionale è senza dubbio il COSO - *Internal Control-Integrated Framework* (cd. "COSO *Framework*"), emesso dal *Committee of Sponsoring Organizations of the Treadway Commission* negli Stati Uniti nel 1992 e aggiornato nel 2013.

Il COSO *Framework* ha costituito, in tutti questi anni, il modello di riferimento più importante sia per le autorità di vigilanza (*standard setter*) sia per le imprese.

Tra i vari ambiti di applicazione del COSO *Framework,* senza dubbio quello relativo al sistema di controllo interno sull'informativa finanziaria è uno tra i più noti e diffusi a livello internazionale.

Più recentemente, l'affermazione delle tematiche di sostenibilità nell'ambito della *corporate governance* e l'obbligo per alcuni enti di interesse pubblico (che rientrano nei limiti definiti dalla legge) di dare *disclosure* sull'informativa non finanziaria (cfr. Direttiva 2014/95/UE attuata in Italia con il D.Lgs. 254/16) ha introdotto, per tali imprese, un nuovo ambito di rendicontazione delle proprie *performance* di sostenibilità (ambiente, comunità di riferimento, personale, rispetto dei diritti umani, lotta alla corruzione attiva e passiva).

Al fine di assicurare, anche in questo ambito, l'affidabilità delle informazioni non finanziarie diffuse al pubblico, le imprese dovrebbero predisporre e implementare un adeguato Sistema di Controllo Interno. Assumere come modello di riferimento il COSO *Framework,* consente, tra le altre cose, di valorizzare quanto già esistente a presidio dei rischi sull'informativa finanziaria. D'altra parte come avremo modo di commentare ampiamente nel corso di questa Monografia, il COSO *Framework* è stato concepito, sin dalla sua prima edizione del 1992, come un modello integrato ovvero idoneo a stabilire un Sistema di Controllo Interno a presidio di tutti i rischi aziendali.

L'ultima versione del COSO *Framework* coglie e tratta tutti gli elementi che caratterizzano l'attuale scenario di rischio. L'approccio olistico e integrato di tutte le componenti del Sistema di Controllo Interno, ancorché riorganizzato per principi e punti di attenzione (*principles based approach*), presenta un certo livello di complessità, in fase di applicazione, derivante soprattutto dalla scalabilità delle soluzioni proposte al contesto e alle dimensioni dell'impresa.

In particolare, il COSO *Framework* definisce il Sistema di Controllo Interno come "un processo messo in atto dal Consiglio di Amministrazione, dal *management* e da tutto il personale, volto a fornire una ragionevole garanzia sul raggiungimento dei seguenti obiettivi: efficacia ed efficienza delle attività operative; attendibilità delle informazioni (interne ed esterne, finanziarie e non finanziarie); conformità alle leggi e alle norme vigenti cui l'impresa è soggetta". Il Sistema di Controllo Interno è articolato in 5 componenti di controllo (*Ambiente di Controllo, Valutazione del Rischio, Attività di Controllo, Informazione e Comunicazione e Attività di Monitoraggio*) e risulta efficace se, con riferimento a uno o più obiettivi, tutte e cinque le componenti esistono nel disegno e nell'implementazione del complessivo sistema aziendale e funzionano in maniera integrata nell'operatività. Il COSO *Framework* enfatizza l'importanza del giudizio del *management* sull'efficacia del sistema di controllo, attraverso la valutazione del disegno, dell'implementazione e del funzionamento delle sue componenti.

Il COSO *Framework* prevede una relazione diretta tra le seguenti tre dimensioni:

- Obiettivi: ciò che l'organizzazione mira a raggiungere, in linea con la *mission*, la *vision* e le strategie aziendali;
- Componenti: ciò che è necessario per il raggiungimento degli obiettivi;
- Struttura organizzativa: gruppo, divisioni, società, unità operative o funzioni, fino ad includere processi di business, quali vendite, acquisti, produzione e marketing, a cui si applica il Sistema di Controllo Interno.

Secondo il COSO *Framework,* la definizione degli obiettivi, categorizzati in operativi, di *reporting* e di conformità, è un prerequisito per il Sistema di Controllo Interno e riveste un ruolo chiave nel processo manageriale di pianificazione strategica.

Una significativa innovazione dell'ultima versione del COSO *Framework* consiste nell'esplicitazione dei 17 principi in cui si articolano le 5 componenti del controllo interno, che si applicano ad ogni categoria di obiettivi e che nella precedente versione avevano solo carattere implicito. I principi hanno un ruolo fondamentale nella valutazione di efficacia sulla presenza (ossia sull'esistenza nel disegno e nell'implementazione) e sul funzionamento delle componenti del Sistema di Controllo Interno a cui si riferiscono, al fine del raggiungimento degli obiettivi stabiliti. Di conseguenza, se un principio non è presente e funzionante, non lo sarà neanche la componente a cui esso è associato.

Il COSO *Framework* descrive, inoltre, 87 punti di attenzione quali importanti caratteristiche dei principi. I punti di attenzione supportano il *management* nel disegno, nell'implementazione e nella conduzione del Sistema di Controllo Interno e nel valutare se i relativi principi sono di fatto presenti e funzionanti. Il principio è attuato nel caso in cui tutti o parte degli aspetti declinati nei punti di attenzione risultino efficacemente applicati; l'esistenza ed il livello di profondità degli elementi di attenzione previsti dai singoli principi devono essere valutati in relazione al contesto aziendale, alle sue dimensioni ed alla sua operatività; parimenti possono essere individuati ulteriori elementi di rilievo in relazione alle caratteristiche della Società che, ancorché non siano direttamente richiamati nell'ambito del COSO, costituiscono comunque elementi del Sistema di Controllo Interno e di gestione dei rischi utili al raggiungimento degli obiettivi del principio.

Alcuni strumenti applicativi del COSO *Framework*

L'obiettivo di questa Monografia è quello di fornire, sulla base dell'esperienza maturata dal Gruppo di Ricerca sulla *Governance*, alcune indicazioni in merito agli strumenti utili ai fini dell'attuazione del COSO *Framework*.

La Monografia – seguendo la struttura del COSO – dedica, quindi, un capitolo a ciascuna delle 5 componenti. Ogni capitolo si articola poi in paragrafi dedicati ai singoli principi e per ciascuno di questi sono presentati appositi sotto-paragrafi per i punti di attenzione e un

paragrafo conclusivo specifico per individuare alcuni **strumenti applicativi,** esposti a titolo esemplificativo.

Per agevolare il lettore e fornire un quadro d'insieme degli strumenti applicativi, indicati a titolo esemplificativo in ciascun capitolo, sono state introdotte, alla fine del documento, due tabelle riepilogative che riportano i suddetti esempi sia per componente/principio del COSO *Framework* sia per ambito aziendale di riferimento (es. *compliance*, IT/*Cyber risk*, etc.).

Riteniamo che questo sforzo di condivisione delle prassi consolidate su un argomento così importante per la *corporate governance* delle imprese possa fornire un valido contributo alle attività di tutti i soggetti coinvolti nella gestione e nel monitoraggio del Sistema di controllo interno e di gestione dei rischi.

Infatti, come lo stesso COSO *Framework* ribadisce a più riprese, le misure di controllo interno proposte necessitano di adattamento al settore di attività e al contesto in cui ciascuna impresa opera; pertanto anche gli strumenti applicativi del *Framework*, riportati nella presente Monografia, dovranno essere valutati in quest'ottica.

Prossimi passi

Ancorché il COSO *Framework* affronti specificatamente il tema del SCI nell'ambito del SCIGR, esso mantiene una sua autonoma validità e applicabilità rispetto al COSO *Enterprise Risk Management – Integrated Framework,* modello di riferimento per la gestione integrata dei rischi e delle opportunità connessi con le strategie, il cui ultimo aggiornamento è del settembre 2017. Entrambi i modelli pertanto possono essere presi come riferimento in modo indipendentemente l'uno dall'altro.

Il gruppo di ricerca sulla *governance* valuterà, tra i prossimi progetti, di realizzare una Monografia dedicata al COSO ERM – *Integrated Framework* con l'analoga finalità di diffusione e condivisione delle esperienze maturate dai professionisti dei network associati nonché di divulgazione delle *leading practice* sui temi del controllo interno e del *risk management.*

CAPITOLO I

AMBIENTE DI CONTROLLO (*CONTROL ENVIRONMENT*)

1. Principio n. 1 – L'organizzazione dimostra il proprio impegno rispetto ai valori etici e all'integrità - 2. Principio n. 2 – Il Consiglio di Amministrazione è indipendente rispetto al *management* ed esercita la propria supervisione sullo sviluppo e sull'implementazione del Sistema di controllo interno e di gestione dei rischi - 3. Principio n. 3 – Il *management* definisce, sotto la supervisione del Consiglio di Amministrazione, la struttura organizzativa, le linee di riporto, i livelli autorizzativi e le responsabilità funzionali al fine di perseguire gli obiettivi aziendali - 4. Principio n. 4 – L'organizzazione dimostra il proprio impegno ad attrarre, sviluppare e trattenere risorse competenti in linea con il conseguimento degli obiettivi aziendali - 5. Principio n. 5 – L'organizzazione, nel raggiungimento degli obiettivi aziendali, ritiene i singoli individui responsabili per la parte di Sistema di controllo interno e di gestione dei rischi di propria competenza

***

L'Ambiente di Controllo è l'insieme di norme, valori, processi e strutture alla base del Sistema di controllo interno e di gestione dei rischi delle organizzazioni.

Il Consiglio di Amministrazione e il *management* stabiliscono la struttura del SCIGR, inclusi gli standard di comportamento attesi, attraverso le direttive emanate, le azioni e i comportamenti agiti.

Il ruolo del *management* della Società, a tutti i livelli, rinforza e sottolinea l'importanza degli standard di comportamento desiderati.

L'Ambiente di Controllo rappresenta le fondamenta dell'intero SCIGR e pertanto esercita la sua influenza sulle altri componenti del COSO nonché su tutta la struttura organizzativa societaria.

In particolare, l'Ambiente di Controllo richiede che siano individuati i seguenti aspetti:

- i principi di integrità ed etici cui l'organizzazione deve adeguarsi;
- gli elementi che consentono al Consiglio di Amministrazione di svolgere azioni di indirizzo per il *management* e di svolgere i propri compiti di supervisione;
- la definizione della struttura organizzativa;
- l'assegnazione di ruoli e responsabilità;
- il processo per attrarre, sviluppare e trattenere il personale;
- la metodologia per la misurazione delle *performance* e la definizione di incentivi e premi.

L'Ambiente di Controllo è influenzato da una varietà di fattori endogeni ed esogeni quali la storia della Società, i valori, i mercati di riferimento, lo scenario competitivo e la normativa di settore.

Inoltre influenza le attività di valutazione dei rischi ai fini del raggiungimento degli obiettivi aziendali, le Attività di Controllo, l'uso delle informazioni e dei sistemi di comunicazione nonché le Attività di Monitoraggio.

In base alla nuova impostazione *principles based* del COSO, tesa a favorire e facilitare la valutazione del SCIGR, l'Ambiente di Controllo è composto da 5 principi e 20 punti di attenzione, il cui disegno e la cui operatività sono il presupposto per la valutazione dell'adeguatezza dell'intera componente.

1. Principio n. 1 – L'organizzazione dimostra il proprio impegno rispetto ai valori etici e all'integrità

Il Principio 1 enfatizza l'importanza di definire i principali valori che guidano l'azione della Società, ritenendo che sia il passo fondamentale per la definizione del complessivo Sistema di controllo interno e di gestione dei rischi.

In particolare, il principio esorta il Consiglio di Amministrazione, il *management* e tutto il personale a mettere in pratica, definire e divulgare standard di condotta che siano ispirati ai valori dell'organizzazione.

Ciascun punto di attenzione può essere attuato attraverso l'adozione di opportuni strumenti di *governance* e di *management*.

Il Principio si compone di 4 punti di attenzione che definiscono più in dettaglio l'ambito e le modalità di applicazione.

1.1. Punto di attenzione – *Tone at the top*

Il Consiglio di Amministrazione e tutti i livelli manageriali dimostrano, attraverso le proprie direttive, le azioni ed il comportamento, l'importanza dell'integrità e dei valori etici a supporto del funzionamento del SCIGR.

Il Consiglio di Amministrazione definisce i principi inderogabili posti alla base del sistema di *Corporate Governance*:

- ponendo l'integrità e la trasparenza alla base dell'architettura societaria;
- definendo le modalità di gestione dei conflitti di interesse, anche potenziali;
- perseguendo le migliori pratiche di governo societario;
- promuovendo all'esterno i principi adottati;
- mantenendo un adeguato efficace ed efficiente Sistema di controllo interno e di gestione dei rischi;
- definendo le politiche e le strategie di sostenibilità.

1.2. Punto di attenzione – Definizione di standard di comportamento

Le aspettative del Consiglio di Amministrazione e del *management* riguardanti i principi di integrità e i valori etici sono definite negli standard di condotta della Società, e recepite da tutti i livelli aziendali, da tutti i collaboratori esterni e dai *business partner*.

L'organizzazione definisce valori e standard di comportamento di riferimento attraverso un Codice Etico, un Codice di Condotta o attraverso l'adozione di *Policy*.

1.3. Punto di attenzione – Valutazione del rispetto degli standard di comportamento

L'organizzazione stabilisce processi funzionali alla valutazione continua della *performance* del personale rispetto agli standard di comportamento stabiliti dalla Società attraverso:

- la verifica del rispetto di tutti gli standard di comportamento previsti da modelli di *compliance* aziendali (es. Sistema di gestione della qualità, D.Lgs. 231/2001, L. 262/2005, Sistema di gestione HSE, *Privacy*, ecc.);
- l'adozione di sistemi di *whistleblowing*, ovvero sistemi di segnalazione, anche in forma anonima, di comportamenti non corretti o violazioni di norme o regolamenti

da parte del personale della Società o di altri *stakeholder*, in linea con i migliori standard internazionali;

- un sistema di comunicazione delle irregolarità ai livelli aziendali adeguati affinché possano gestire opportunamente le misure atte alla correzione dei comportamenti con l'eventuale supporto della funzione Risorse Umane.

Gli standard di comportamento sono diffusi all'interno dell'impresa attraverso l'adozione di direttive (c.d. *policy*) e procedure aziendali e che dovrebbero essere richiamate nei contratti con il personale e con terze parti che entrano in contatto con l'impresa.

1.4. Punto di attenzione – Gestione tempestiva dei disallineamenti rispetto agli standard di comportamento

Le eventuali violazioni dei principi etici e di comportamento stabiliti dall'organizzazione devono essere tempestivamente identificate e sottoposte a specifiche azioni correttive.

L'organizzazione istituisce strutture interne ed eventualmente esterne alle quali attribuire:

- la responsabilità del monitoraggio delle azioni correttive individuate a fronte di violazioni degli standard di comportamento;
- l'analisi periodica delle principali cause sottostanti alle violazioni.

1.5. Strumenti applicativi

Si riportano di seguito, a titolo esemplificativo e non esaustivo, alcuni tra i principali elementi di concreta attuazione dei punti di attenzione del principio in esame:

- **Statuto societario**, che definisca chiaramente il modello di *governance* adottato (ad es. organi sociali, eventuali comitati e elementi fondamentali dell'assetto organizzativo);
- **Sistema di deleghe e procure,** esterno ed interno chiaro e strutturato, che rifletta le effettive responsabilità previste anche dal Sistema di controllo interno e di gestione dei rischi e garantisca la piena consapevolezza delle norme etiche che devono ispirare i comportamenti aziendali;
- **Linee guida in materia di governo societario** (con riferimento ad esempio al Codice di autodisciplina per le Società quotate), che dettano i principi alla base della *governance* dell'azienda, tra cui anche quelli finalizzati all'integrità e alla trasparenza;
- **Codice etico (e/o di Condotta e/o di Comportamento)**, che indichi chiaramente le norme di comportamento concrete che l'organizzazione ritiene corrette ed i comportamenti ritenuti non etici affinché i principi e i valori in esso contenuti possano costituire una guida pratica nell'operatività aziendale;
- **Modello di Organizzazione, Gestione e Controllo *ex* D.Lgs. 231/2001** e istituzione di un Organismo di Vigilanza al fine di diffondere l'adozione dei principi etici e delle regole comportamentali volte alla prevenzione di condotte che possono integrare le fattispecie di reato previste dal D.Lgs. 231/2001;
- **Linee guida sul SCIGR** (introdotte dal Codice di Autodisciplina per le società quotate), che definiscano chiaramente ruoli e responsabilità, tipologia e livello di rischio che la Società è disposta ad assumere per raggiungere i propri obiettivi, nonché le modalità con cui i rischi devono essere gestiti e i controlli devono essere messi in atto;
- **Sistema sanzionatorio**, che preveda i diversi livelli di sanzioni e le relative modalità di applicazione in relazione a differenti tipologie di violazioni (di norme o procedure aziendali interne, norme di legge, comportamenti contrari all'etica, ecc.) effettuate da parte degli organi sociali, del personale aziendale e di terze parti;

- **Norme in materia di anticorruzione**, che definiscano i principi di riferimento cui si ispira la Società, il comportamento da tenersi in relazione ai rapporti con i soggetti terzi rispetto all'azienda (con soggetti pubblici o meno), il sistema di controllo adottato dalla Società al fine di mitigare o rimuovere fenomeni corruttivi, i controlli di monitoraggio del disegno e dell'operatività;
- **Sistema di segnalazione delle violazioni *(whistleblowing)***, volto a permettere le segnalazioni, anche in forma anonima, di comportamenti non corretti o violazioni di norme o regolamenti, effettuate da parte del personale della Società, da parte di esponenti degli organi sociali o terze parti, che preveda modalità e canali di comunicazione nonché l'analisi e risoluzione delle problematiche da parte dei soggetti responsabili;
- **Politiche di remunerazione e incentivazione,** focalizzate oltre che su obiettivi di *performance* anche su quelli di integrità, al fine di promuovere azioni e comportamenti coerenti con i valori della Società, i principi del Codice Etico da essa adottato e gli obiettivi strategici;
- **Piani di formazione e comunicazione** al Personale sullo SCIGR della Società, sull'etica e sulla legalità nonché in generale sull'importanza del mantenimento di un comportamento etico e corretto nell'ambito dei rapporti interni e dei rapporti con gli *stakeholder*;
- Prevedere **verifiche periodiche sul clima aziendale** con riferimento agli aspetti etici e di integrità.

2. Principio n. 2 – Il Consiglio di Amministrazione è indipendente rispetto al *management* ed esercita la propria supervisione sullo sviluppo e sull'implementazione del Sistema di controllo interno e di gestione dei rischi

Il Principio 2 enfatizza il ruolo del Consiglio di Amministrazione, o degli organi equivalenti al Consiglio in altri modelli di *corporate governance*, nella definizione e monitoraggio del SCIGR della Società.

In particolare, il principio sottolinea che il Consiglio di Amministrazione è responsabile della definizione degli obiettivi e delle linee di indirizzo del SCIGR, la cui effettiva implementazione è di responsabilità del *management* e di tutto il personale.

Il Principio si compone di 4 punti di attenzione che definiscono più in dettaglio l'ambito e le modalità di applicazione.

2.1. Punto di attenzione – Definizione delle responsabilità di supervisione

Il Consiglio di Amministrazione individua gli obiettivi, le strategie, il profilo ed il livello di rischio in relazione alle caratteristiche dell'impresa, espletando così la sua funzione di indirizzo e di supervisione strategica.

Il Consiglio di Amministrazione ha il compito di supervisione dei ruoli e delle responsabilità nel processo di gestione dei rischi e di controllo interno e la definizione della tipologia e del livello di rischio che la Società è disposta ad assumere per raggiungere i propri obiettivi, nonché le modalità con cui i rischi devono essere gestiti.

Il Consiglio di Amministrazione deve essere consapevole delle proprie responsabilità in relazione ai requisiti legali e regolamentari ed alle aspettative degli *stakeholder*, quali clienti, lavoratori, fornitori, investitori.

Il Consiglio nomina uno o più Amministratori Delegati, incaricati di attuare la strategia della Società, di raggiungere gli obiettivi societari, individuando tra loro l'amministratore

incaricato del SCIGR.

Per l'esercizio del potere di supervisione, il Consiglio definisce all'interno dell'organizzazione strutture e processi che il *management* deve seguire per la conduzione del *business*.

2.2. Punto di attenzione – Competenza

Il Consiglio di Amministrazione, in relazione al proprio ruolo di indirizzo e supervisione strategica, anche di medio-lungo termine, valuta periodicamente che le competenze dei propri membri siano adeguate al ruolo di indirizzo e supervisione che è chiamato a svolgere nonché per deliberare azioni commisurate alle esigenze aziendali.

Il numero di membri del Consiglio di Amministrazione deve essere tale da facilitare il processo decisionale, le discussioni e le critiche costruttive.

2.3. Punto di attenzione – Indipendenza

Il Consiglio di Amministrazione dovrebbe essere costituito da un numero appropriato di membri indipendenti e quindi oggettivi nelle valutazioni e nel processo decisionale del Consiglio.

L'indipendenza del Consiglio di Amministrazione deve essere dimostrata nel modo di pensare, nelle azioni e nella conduzione del *business*.

Il requisito di indipendenza deve essere tale da limitare pregiudizi o conflitti di interesse nell'ambito della propria attività decisionale, di indirizzo o supervisione dell'operatività aziendale, derivanti dall'appartenenza degli amministratori della Società anche a Consigli di Amministrazione di altre società.

L'indipendenza dei membri del Consiglio deve essere quindi valutata anche in funzione delle relazioni personali e professionali assunte, limitando pertanto le distorsioni ed i conflitti di interesse che potrebbero sorgere dalla partecipazione di ciascun membro ad ulteriori consigli di amministrazione.

I membri del Consiglio di Amministrazione sono considerati indipendenti qualora non abbiano mantenuto relazioni dirette o indirette recenti con la Società o con terze parti legate alla Società che potrebbero minare l'autonomia di giudizio. Tale valutazione dovrebbe essere basata sull'analisi della documentazione riguardante gli incarichi ricoperti attualmente o in passato e su eventuali relazioni o rapporti con il *management* che possano essere considerati rilevanti per la valutazione della loro indipendenza.

2.4. Punto di attenzione – Supervisione del Sistema di controllo interno e di gestione dei rischi

Il Consiglio di Amministrazione ha la responsabilità di definire, implementare e supervisionare il funzionamento del SCIGR, con riferimento a tutte le sue componenti indicate dal COSO. In particolare:

- Ambiente di Controllo: definizione di principi di integrità ed etici, meccanismi di supervisione, autorità e responsabilità, aspettative sulle competenze e *accountability* del Consiglio;
- *Risk Assessment* ed *Enterprise Risk Management* (ERM): supervisione della gestione della valutazione dei rischi rispetto al raggiungimento degli obiettivi, al potenziale impatto dei cambiamenti, alle frodi e all'aggiramento del SCIGR da parte del *management*;
- Attività di Controllo: supervisione del *management* nello sviluppo e nell'efficacia delle Attività di Controllo;

- Informazione e Comunicazione: analisi critica delle informazioni relative al raggiungimento degli obiettivi della Società;
- Attività di Monitoraggio: valutazione e supervisione della natura e dell'ambito delle Attività di Monitoraggio e delle attività correttive implementate dal *management*.

2.5. Strumenti applicativi

Si riportano di seguito, a titolo esemplificativo e non esaustivo, alcuni tra i principali elementi di concreta attuazione dei punti di attenzione del principio in esame:

- **Piano strategico**, che definisca gli obiettivi aziendali funzionali alla gestione del rischio in una logica integrata e al successivo monitoraggio del SCIGR;
- **Programma di *assessment* e di formazione del Consiglio di Amministrazione**, per l'autovalutazione delle competenze e del funzionamento dell'organo amministrativo, nonché per l'acquisizione di una maggiore consapevolezza del ruolo e delle responsabilità attribuite ai singoli membri dell'organo oltre che per lo sviluppo delle competenze tecniche necessarie (c.d. *board evaluation* e *board induction*, con particolare riferimento alle società quotate);
- **Relazione sulla *corporate governance*** (per gli emittenti titoli quotati in mercati regolamentati, come previsto dal TUF), che fornisca una chiara rappresentazione nonché la valutazione periodica di adeguatezza del Sistema di controllo interno e di gestione dei rischi;
- **Regolamento** che disciplina la composizione ed il funzionamento del Comitato Controllo e Rischi e di altri eventuali Comitati istituiti all'interno del Consiglio di Amministrazione;
- ***Policy* di *Enterprise Risk Management (ERM)* e profilo di rischio**, che individui chiaramente i ruoli e le responsabilità del Consiglio di Amministrazione, dei Comitati e del *management* nell'indirizzo e supervisione delle modalità di gestione dei rischi aziendali;
- **Procedura sulle operazioni con parti correlate**, che definisca chiaramente le modalità e i tempi con i quali sono fornite, agli amministratori o consiglieri indipendenti che esprimono pareri sulle operazioni con parti correlate nonché agli organi di amministrazione e controllo, le informazioni sulle operazioni, con la relativa documentazione, prima della deliberazione, durante e dopo l'esecuzione delle stesse;
- ***Corpus* procedurale** (politiche, linee guida e procedure), che includa la valutazione e gestione del conflitto di interesse, che prevedano, tra l'altro, che i membri indipendenti procedano ad una valutazione della propria posizione, al termine della quale il Consiglio di Amministrazione si pronuncia collegialmente sulla posizione di ogni membro indipendente, escludendo dalla votazione l'individuo interessato;
- **Piano di *Internal Audit Risk Based*,** approvato dal Consiglio di Amministrazione quale strumento di supervisione e monitoraggio complessivo del SCIGR.

3. Principio n. 3 – Il *management* definisce, sotto la supervisione del Consiglio di Amministrazione, la struttura organizzativa, le linee di riporto, i livelli autorizzativi e le responsabilità funzionali al fine di perseguire gli obiettivi aziendali

Il Principio 3 richiama il ruolo del *management* nel definire la struttura societaria, sotto la supervisione del Consiglio di Amministrazione.

In particolare la chiara individuazione di ruoli e responsabilità e la definizione delle linee di

riporto è alla base di uno strutturato SCIGR.

Il Principio si compone di 3 punti di attenzione che definiscono più in dettaglio l'ambito e le modalità di applicazione.

3.1. Punto di attenzione – Analisi dell'assetto societario e organizzativo

Il Consiglio di Amministrazione e il *management* valutano l'assetto societario e organizzativo (unità operative, *legal entity*, distribuzione geografica, servizi in *outsourcing*) più adeguato per il raggiungimento degli obiettivi aziendali.

Il Consiglio di Amministrazione esamina e valuta periodicamente, in genere in occasione dell'approvazione della relazione finanziaria annuale e semestrale, l'adeguatezza dell'assetto organizzativo, amministrativo e contabile con particolare riferimento al Sistema di controllo interno e di gestione dei rischi.

3.2. Punto di attenzione – Definizione delle linee di riporto gerarchico e funzionale

Il *management* definisce e valuta le linee di riporto gerarchico e funzionale, necessarie all'esercizio di ruoli e responsabilità, e i flussi informativi per la gestione delle attività aziendali per ogni struttura societaria.

La definizione della struttura organizzativa e delle linee di riporto è supportata dai processi organizzativi e dalla tecnologia, che consentono lo scambio delle informazioni all'interno dell'organizzazione con riferimento a tutte le unità di *business*.

La valutazione del SCIGR dovrebbe essere svolta con riferimento a tutti gli elementi caratterizzanti la propria attività quali ad esempio prodotti, linee di *business*, società e mercati.

Infatti se la valutazione del SCIGR attraverso un unico elemento potrebbe non rilevare rischi, dalla visione sistemica dei differenti elementi potrebbe emergere la concentrazione di rischi attorno a certe tipologie di clienti, fornitori e, quindi, consentire l'individuazione di situazioni di rischio, e la conseguente attivazione di linee di indirizzo per la loro mitigazione che, altrimenti, non sarebbero state individuate.

3.3. Punto di attenzione – Definire, assegnare e limitare i ruoli e le responsabilità

Il Consiglio di Amministrazione e il *management* delegano i poteri, definiscono le responsabilità e usano appropriati processi e sistemi informativi per assegnarle a tutti i livelli dell'organizzazione nel rispetto del principio di segregazione delle responsabilità e dei compiti.

In particolare il Consiglio di Amministrazione controlla l'assegnazione di ruoli e responsabilità al *management*, limitando la sovrapposizione di incarichi e mantiene l'autorità sulle decisioni significative.

Il *management* implementa *policy* e controlli che permettano al *management* stesso e a tutto il personale di comprendere le proprie responsabilità in materia di controllo interno ed eseguire coerentemente le attività.

Il *management* guida e supporta l'esecuzione delle attività previste dai processi aziendali coerente con le *policy* definite dalla Società e dalle singole unità organizzative. In particolare definisce, nell'ambito dell'operatività aziendale e secondo gli indirizzi ricevuti dal Consiglio di Amministrazione, gli strumenti normativi e organizzativi più opportuni per consentire al personale di operare nell'ambito del rispetto dei ruoli, delle responsabilità e delle regole

definite. A tal fine il *management* assegna le responsabilità al personale tramite specifici strumenti organizzativi (organigrammi, ordini di servizio, mansionari, comunicazioni organizzative, deleghe e procure, ecc.) e ne definisce le modalità di operatività tramite il corpo normativo aziendale (direttive o *policy*, procedure, istruzioni operative, ecc.).

Il personale, nell'espletamento delle attività operative, considera i rischi in relazione al raggiungimento degli obiettivi ed esegue le Attività di Controllo applicabili nel rispetto del proprio livello organizzativo. Assicura il flusso informativo atteso e le Attività di Monitoraggio funzionali al raggiungimento degli obiettivi dell'unità cui sono demandati.

I collaboratori esterni riconoscono i limiti di ruoli e responsabilità applicabili alle terze parti definiti dal *management*, lavorando nel rispetto degli standard di comportamento concordati.

3.4. Strumenti applicativi

Si riportano di seguito, a titolo esemplificativo e non esaustivo, alcuni tra i principali elementi di concreta attuazione dei punti di attenzione del principio in esame:

- **Partecipogramma societario**, utile a rappresentare la struttura del gruppo di riferimento;
- ***Policy*/direttive di Gruppo**, che dettino le linee guida di governo e gestione su singole tematiche/processi per tutte le entità legali del Gruppo;
- **Modelli di controllo implementati a fronte di specifiche norme e *leading practice***, intesi come presidi di natura organizzativa ed operativa volti a garantire il costante e completo rispetto delle disposizioni vigenti da parte di tutto il personale (es. L. 262/2005, sistema di gestione della qualità, sistema di gestione HSE, *privacy*, informativa non finanziaria, ecc.);
- **Organigramma societario**, che consenta al Consiglio di Amministrazione di definire la struttura organizzativa e le principali unità organizzative;
- **Mansionari e *job description***, funzionali a descrivere i ruoli societari e le principali responsabilità assunte in azienda;
- **Sistema di deleghe e procure**, atto a descrivere i poteri autorizzativi e di firma e a comprendere se gli stessi sono coerenti con le responsabilità organizzative e gestionali assegnate;
- **Comunicazioni organizzative**, per diffondere le informazioni all'interno dell'organizzazione;
- ***Corpus procedurale*** (politiche, linee guida e procedure), adeguato alle esigenze operative ed organizzative della Società e che includa gli elementi del SCIGR al fine di assicurare un adeguato presidio dei rischi**.**

4. Principio 4 – L'organizzazione dimostra il proprio impegno ad attrarre, sviluppare e trattenere risorse competenti, in linea con il conseguimento degli obiettivi aziendali

Il Principio 4 enfatizza il ruolo chiave che assume il personale coinvolto nei processi aziendali. La Società deve essere attivamente impegnata nell'individuare le migliori risorse, con competenze adeguate a perseguire il raggiungimento degli obiettivi aziendali.

Il Principio si compone di 4 punti di attenzione che definiscono più in dettaglio l'ambito e le modalità di applicazione.

4.1. Punto di attenzione – Adozione di *policy* e procedure

La Società si deve dotare di un insieme di direttive (*policy*) e procedure che regolamentano i processi interni, disciplinando sia le attività svolte nell'ambito delle singole funzioni, sia i rapporti con le altre entità; le direttive e le procedure devono tenere conto dei rischi presenti nell'ambito dell'organizzazione e prevedere misure per la loro mitigazione. Le *policy* e le procedure devono riguardare anche l'organizzazione del personale, fin dalla definizione delle competenze necessarie a ricoprire determinati ruoli organizzativi, la gestione del personale, dalla sua assunzione, alla definizione di piani di formazione e crescita, alla valutazione delle *performance*.

Le *policy* e le procedure riflettono le aspettative dell'azienda in termini di competenze, devono tener conto dei rischi presenti nell'organizzazione e prevedere misure di mitigazione anche nell'ambito della gestione del personale. Il corpo normativo aziendale, costituito da *policy*, procedure, istruzioni operative, ecc. rappresenta il *modus operandi* dell'azienda e costituisce il punto di riferimento che guida i comportamenti e le aspettative degli investitori, dei *regulator* e di tutti gli *stakeholder*.

Tali documenti sono alla base per la definizione delle competenze necessarie all'interno dell'organizzazione, per valutare le *performance* e per definire le azioni correttive.

4.2. Punto di attenzione – Valutazione delle competenze e gestione delle inefficienze

Il Consiglio di Amministrazione e il *management*, che impartiscono le direttive societarie attraverso l'emissione di *policy* e procedure operative, valutano che le competenze del personale e di terze parti che operano per conto della Società siano tali da consentire lo svolgimento delle attività secondo le linee guida impartite. Qualora siano identificate aree di debolezza, operano in modo da individuare le competenze necessarie al raggiungimento degli obiettivi.

Le competenze rappresentano infatti la qualifica del personale per svolgere i compiti assegnati e adempiere alle proprie responsabilità.

Per verificare che la Società disponga di tutte le competenze necessarie per una gestione efficace ed efficiente dei processi di *business* e del Sistema di controllo interno e di gestione dei rischi, il *management* può effettuare periodicamente una mappatura delle competenze aziendali, valutando eventuali inserimenti, piani di sviluppo o soluzioni di *outsourcing* in caso di lacune.

Al fine di valutare le competenze necessarie per il raggiungimento degli obiettivi aziendali, riducendo così le inefficienze, il *management* formalizza periodicamente gli obiettivi assegnati a ciascun livello dell'organizzazione, provvedendo, mediante parametri quanto più oggettivi possibili, a valutare il raggiungimento degli stessi una volta terminato il periodo predefinito e previamente comunicato.

4.3. Punto di attenzione – Attrarre, sviluppare e trattenere persone

La Società deve fornire il supporto e la formazione necessaria ad attrarre, sviluppare e trattenere il personale e i collaboratori esterni funzionali al raggiungimento degli obiettivi.

L'attenzione alle competenze deve essere supportata da uno strutturato processo di gestione delle risorse umane, volto a definire la selezione, l'assunzione del personale nonché la pianificazione e gestione della formazione.

Il *management* deve implementare le strutture ed i processi per attrarre, formare, indirizzare, valutare e trattenere le migliori persone (talenti, personale ad alto potenziale) all'interno dell'organizzazione.

4.4. Punto di attenzione – Pianificare e gestire la successione

Il Consiglio di Amministrazione e il *management* predispongono un piano di successione per l'assegnazione delle responsabilità chiave per il Sistema di controllo interno e di gestione dei rischi.

Per implementare il piano di successione ed evitare situazioni vacanti, il *management* deve identificare e monitorare continuamente le funzioni principalmente coinvolte nell'ambito del SCIGR, pianificando e organizzando eventuali successioni del personale.

Il Consiglio di Amministrazione ed il *management* definiscono pertanto un piano di successione che pianifichi e organizzi ruoli e responsabilità di rilievo nell'ambito del SCIGR, tenendo conto di una visione prospettica della Società.

4.5. Strumenti applicativi

Si riportano di seguito, a titolo esemplificativo e non esaustivo, alcuni tra i principali elementi di concreta attuazione dei punti di attenzione del principio in esame:

- **Piano strategico**, che individui chiaramente, tra gli elementi strategici, la necessità di attrarre le risorse con adeguate competenze, proponendo gli opportuni piani di intervento in termini di gestione e sviluppo delle risorse, formazione e *knowledge management*;
- ***Corpus* procedurale** (politiche, linee guida e procedure), che disciplini i processi di selezione, gestione, valutazione, formazione e sviluppo delle risorse umane, in linea con gli obiettivi di sviluppo ed efficienza indicati nel piano strategico;
- **Mappa delle competenze**, che consenta di possedere una visione sempre aggiornata sulle competenze necessarie per conseguire gli obiettivi aziendali;
- **Politiche di *recruiting*** finalizzate ad attrarre le competenze necessarie e mappate per conseguire gli obiettivi aziendali;
- **Processi di formazione e sviluppo del personale** (inclusa la possibilità di *job rotation* che consenta di arricchire il bagaglio professionale delle risorse interne);
- **Politiche di remunerazione e incentivazione**, che prevedano, oltre ad obiettivi di breve termine (riferiti all'esercizio), anche obiettivi di medio-lungo termine orientati a premiare l'accrescimento di valore della Società, nell'ambito di un quadro di regole di riferimento indirizzate a un corretto controllo dei rischi aziendali;
- **Piano di successione**, idoneo a garantire continuità nell'esercizio dei ruoli chiave;
- Processo strutturato di definizione degli obiettivi e valutazione della *performance* finalizzato a sviluppare e a trattenere le persone migliori.

5. Principio n. 5 – L'organizzazione, nel raggiungimento degli obiettivi aziendali, ritiene i singoli individui responsabili per la parte del Sistema di controllo interno di propria competenza

Il Principio 5 richiama l'attenzione sulla consapevolezza che le persone coinvolte nel Sistema di controllo interno e di gestione dei rischi devono maturare con riferimento al loro ruolo per il raggiungimento degli obiettivi aziendali.

In particolare, le persone coinvolte nel SCIGR devono essere consapevoli dell'importanza del proprio ruolo nel sistema aziendale, anche attraverso la partecipazione a piani di incentivazione e remunerazione.

Il Principio si compone di 5 punti di attenzione che definiscono più in dettaglio l'ambito e le

modalità di applicazione.

5.1. Punto di attenzione – Rafforzare la consapevolezza tramite strutture, ruoli e responsabilità

Il Consiglio di Amministrazione e il *management* definiscono i meccanismi per comunicare e mantenere consapevoli delle loro responsabilità le persone che eseguono le Attività di Controllo interno e di gestione dei rischi e che implementano, ove necessario, le azioni correttive.

L'Amministratore Delegato e il *management* sono responsabili della definizione, implementazione, conduzione e valutazione delle strutture e dei ruoli per rafforzare la responsabilità nell'ambito del Sistema di controllo interno e di gestione dei rischi all'interno di tutta l'organizzazione.

Il Consiglio di Amministrazione e, a cascata, il *management*, forniscono comunicazioni chiare sui ruoli e le responsabilità del SCIGR.

5.2. Punto di attenzione – Definire il sistema di misurazione delle *performance*, di incentivi e di *rewarding*

Il Consiglio di Amministrazione e il *management* definiscono il sistema di misurazione delle *performance*, degli incentivi e delle altre modalità di *rewarding* appropriato per tutti i livelli della Società, in considerazione dell'entità della *performance* e degli standard di comportamento attesi, tenuto conto degli obiettivi di breve e medio-lungo periodo.

La valutazione e monitoraggio del sistema di incentivazione del *management* devono essere atti ad attrarre e motivare le risorse in possesso della capacità ed esperienza adeguata, a sviluppare il senso di appartenenza ed assicurare il loro supporto nella creazione di valore per la Società.

5.3. Punto di attenzione – Valutazione del sistema di misurazione delle *performance*, di incentivi e di *rewarding*

Il Consiglio di Amministrazione e il *management* assicurano l'allineamento dei premi e delle ricompense all'adempimento delle responsabilità sul controllo interno nel raggiungimento degli obiettivi.

La componente fissa e la componente variabile della remunerazione devono essere adeguatamente bilanciate in funzione del raggiungimento degli obiettivi strategici e della politica di gestione dei rischi della Società.

Affinché il piano di incentivazione e valutazione delle *performance* ottenga gli obiettivi previsti, il *management* tiene fede agli impegni assunti in fase di definizione degli obiettivi, comunicando in modo trasparente le logiche del sistema di *rewarding* e le tempistiche della valutazione.

5.4. Punto di attenzione – Considerare la complessità delle *performance* richieste

Il Consiglio di Amministrazione e il *management* valutano e ponderano la complessità e la fattibilità associate agli obiettivi in fase di assegnazione delle responsabilità, dello sviluppo, della misurazione delle *performance* e nella valutazione delle stesse.

5.5. Punto di attenzione – Valutazione della *performance* e conseguente premio o sanzione degli individui

Il Consiglio di Amministrazione e il *management* valutano la *performance* relativa alle responsabilità in materia di controllo interno, tenendo conto del rispetto degli standard di comportamento e dei livelli di competenza attesi e decidendo, di conseguenza, l'attribuzione di premi o l'adozione di misure disciplinari.

La *performance* è misurata in relazione al raggiungimento degli obiettivi aziendali ed alla capacità di assumere un livello di rischio all'interno del livello di tolleranza al rischio sia di breve periodo sia di lungo periodo.

La Società dovrebbe adottare pertanto un sistema disciplinare per sanzionare eventuali violazioni nonché la mancata osservanza delle procedure aziendali che recepiscono i presidi di controllo.

5.6. Strumenti applicativi

Si riportano di seguito, a titolo esemplificativo e non esaustivo, alcuni tra i principali elementi di concreta attuazione dei punti di attenzione del principio in esame:

- **Mandato all'*Internal Audit*** (*Audit Charter*), attraverso il quale il Consiglio di Amministrazione incarichi la funzione di effettuare il controllo del SCIGR;
- **Posizionamento organizzativo delle funzioni di controllo** per garantire la necessaria indipendenza e autonomia di giudizio;
- **Mansionari e *job description***, con cui siano formalmente individuate le responsabilità e i compiti delle funzioni di controllo;
- **Politiche di remunerazione e incentivazione,** attraverso le quali siano riconosciuti meccanismi di incentivazione al personale più rilevante delle funzioni di controllo, coerenti con i compiti e le responsabilità assegnati nello sviluppo di una cultura della conformità e gestione del rischio;
- **Sistema di valutazione delle prestazioni**, del potenziale professionale e delle risorse neo inserite;
- **Piano di successione del personale chiave delle funzioni di controllo**, idoneo a garantire la continuità.

CAPITOLO II

VALUTAZIONE DEL RISCHIO (*RISK ASSESSMENT*)

1. Principio n. 6 – L'organizzazione esplicita con sufficiente chiarezza i propri obiettivi, consentendo l'identificazione e la valutazione dei rischi ad essi legati - 2. Principio n. 7 – L'organizzazione identifica i rischi connessi al conseguimento degli obiettivi aziendali e ne determina le modalità di gestione - 3. Principio n. 8 – L'organizzazione prende in considerazione potenziali frodi nel valutare i rischi di conseguimento dei propri obiettivi aziendali - 4. Principio n. 9 – L'organizzazione identifica e valuta i cambiamenti che potrebbero avere impatti significativi sul Sistema di controllo interno

***

Il sistema di gestione del rischio (*Risk Assessment*) rappresenta un elemento fondamentale per una sana e prudente gestione aziendale.

La definizione delle strategie e degli obiettivi, nonché l'analisi relativa al monitoraggio sul perseguimento degli stessi, dovrebbe essere supportata dalla valutazione delle probabilità che i rischi a cui è esposta la Società si realizzino e degli impatti che la manifestazione dei rischi possa determinare.

Un approccio strutturato per la valutazione preventiva dei rischi rappresenta un supporto fondamentale per l'assunzione di scelte consapevoli e coerenti alla struttura, al dimensionamento, alla maturità, alla solidità patrimoniale, all'articolazione organizzativa, ecc., della Società.

La definizione dell'impostazione, degli obiettivi e delle linee guida del sistema di individuazione e valutazione del rischio rientrano tra le responsabilità del Consiglio di Amministrazione, come indicato nel capitolo precedente, mentre la relativa implementazione è realizzata a cura del *management* della Società.

Il sistema di gestione del rischio è composto da diverse fasi che ne determinano solidità ed affidabilità:

- Individuazione;
- Valutazione;
- Misurazione;
- Gestione;
- Mitigazione.

I rischi sono influenzati da fattori esogeni, relativi al contesto politico, economico, ambientale, regolamentare, competitivo in cui opera l'azienda, e da fattori endogeni, relativi alla propria organizzazione, alle risorse, ai sistemi.

I fattori esogeni possono determinare azioni di protezione, ma più spesso sono alla base della scelta di evitare un rischio o trasferirlo a terzi. I fattori endogeni sono quelli su cui la Società ha diretta influenza in termini di rafforzamento delle misure di prevenzione e mitigazione.

In base alla nuova impostazione *principle based* del COSO, tesa a favorire e facilitare la valutazione del SCIGR, il *Risk Assessment* è composto da 4 principi e 27 punti di attenzione, il cui disegno e la cui operatività sono il presupposto per la valutazione dell'adeguatezza dell'intera componente.

1. Principio n. 6 – L'organizzazione esplicita con sufficiente chiarezza i propri obiettivi, consentendo l'identificazione e la valutazione dei rischi ad essi legati

Il Principio 6 rappresenta il primo *step* per la costruzione di un adeguato modello di *Risk Assessment e* si focalizza sulla necessità di definire con sufficiente chiarezza gli obiettivi aziendali da parte del *management* e assegnarli ai vari livelli della struttura organizzativa.

Una chiara definizione degli obiettivi permette di individuare e valutare i rischi connessi al raggiungimento degli stessi. A tal fine, secondo il COSO, il *management* raggruppa gli obiettivi in tre categorie: operativi, di reporting e di conformità.

Il Principio si compone di 15 punti di attenzione che definiscono più in dettaglio l'ambito e le modalità di applicazione.

1.1. Punto di attenzione – Specificare con sufficiente chiarezza gli obiettivi

Specificare con sufficiente chiarezza gli obiettivi che si vogliono conseguire, identificando i rischi associati, rappresenta un presupposto fondamentale per perseguire una buona *performance*.

La condizione necessaria per garantire l'efficacia delle attività di *Risk Assessment* è rappresentata dalla definizione di un processo di pianificazione strategica, che, oltre a definire gli obiettivi da raggiungere, tenga in considerazione anche i rischi connessi alla strategia definita.

L'individuazione e la definizione degli obiettivi e dei rischi devono essere due momenti fortemente correlati che determinano la scelta dei *target* da raggiungere in funzione dei livelli di rischio sostenibili, a loro volta derivanti dalla filosofia di fondo dell'organizzazione e dalla relativa propensione al rischio.

Il COSO identifica le diverse categorie di obiettivi da perseguire:

- obiettivi operativi, relativi all'efficacia e all'efficienza delle operazioni aziendali, ivi inclusi obiettivi di *performance* operativi, finanziari e non finanziari nonché di salvaguardia del patrimonio aziendale;
- obiettivi di *reporting*, relativi all'efficacia del sistema di *reporting* aziendale, sia interno sia esterno, con riferimento all'informativa finanziaria e non finanziaria;
- obiettivi di conformità *(compliance)*, relativi alla conformità a leggi e regolamenti cui l'azienda è soggetta.

Gli obiettivi operativi, di *reporting* e di conformità, devono essere coerenti con la *vision* e la *mission* aziendale. È opportuno che insieme ad essi siano anche predisposti una serie di indicatori, normalmente denominati *key performance indicator*, in grado di verificare e monitorare quali obiettivi sono stati raggiunti e quali no.

La definizione degli obiettivi è inoltre condizionata da due altri elementi fondamentali all'interno di un'organizzazione: la propensione al rischio e la tolleranza del rischio.

Stabilendo gli obiettivi che si vogliono conseguire, si identificano di conseguenza i rischi associati, ma la propensione o meno ad accettarli dipende solitamente, oltre che da scelte strategiche, dalla filosofia di gestione. Di norma ad una maggiore propensione al rischio sono associabili maggiori ricavi, livelli di redditività, opportunità di crescita e sviluppo, mentre ad una minore propensione, anche i benefici potenzialmente conseguibili saranno minori. È quindi importante che nella scelta degli obiettivi il *management* abbia considerato questi aspetti e che i *target* individuati siano coerenti con la propensione e la tolleranza al rischio anch'essi definiti dai vertici aziendali.

La maggior parte degli obiettivi sono specifici per ciascuna Società, tuttavia ce ne sono alcuni ampiamente condivisibili da tutte le organizzazioni. Ad esempio, obiettivi comuni alla maggior parte delle organizzazioni riguardano il successo dell'organizzazione, le attività di *reporting* verso gli *stakeholder*, il personale competente e motivato, l'avere una reputazione positiva sul mercato, l'operare nel rispetto di leggi e regolamenti.

Il personale a tutti i livelli, deve acquisire una comprensione chiara e consapevole degli obiettivi dell'impresa e di quelli di cui è direttamente responsabile al fine di garantire una efficace gestione del rischio ad essi associato.

Obiettivi Operativi

I seguenti 4 punti di attenzione supportano il *management* nel determinare se il Principio è presente e funzionante. Gli obiettivi operativi:

- Riflettono le scelte del *management*;
- Tengono in considerazione la tolleranza di rischio;
- Includono gli obiettivi di *performance* operativa e finanziaria;
- Costituiscono la base per impegnare le risorse.

Gli obiettivi operativi riflettono le scelte del *management* rispetto al *business*, al settore e all'ambiente economico in cui l'organizzazione opera e il livello desiderato di *performance* operative e finanziarie. Un'impresa deve impostare le proprie azioni in modo da utilizzare le risorse disponibili in maniera efficiente, perseguendo quelli che sono gli obiettivi definiti, quali ad esempio la massimizzazione dei ricavi, dei profitti, della capitalizzazione, della riconoscibilità del brand sul mercato, della qualità dei servizi e/o prodotti offerti, ecc. Allo stesso modo, il gruppo di ricerca ritiene che anche con riferimento agli obiettivi di *performance* non finanziari, l'impresa deve definire le proprie politiche e indentificare le iniziative idonee a traguardare il livello di *performance* atteso, per esempio, per quanto attiene alle tematiche ambientali, sociali, di contrasto alla corruzione, sulla diversità, ecc.

Identificare quali sono gli obiettivi operativi, quindi definire un uso efficace delle risorse nonché una struttura di processi efficiente, permette di focalizzare l'attenzione dell'organizzazione su quei fattori che consentono di raggiungerli. Gli obiettivi operativi definiti e individuati in maniera chiara costituiscono una base per allocare le risorse in modo efficace ed efficiente; diversamente, se gli obiettivi di un'organizzazione non sono chiari o sono mal concepiti allora le risorse possono essere allocate ed utilizzate in modo non ottimale.

La definizione degli obiettivi operativi comporta anche che il *management* specifichi la tolleranza al rischio in relazione ai processi di *business*: la *risk tolerance* può essere espressa come devianza rispetto al livello di accettabilità del rischio facendo riferimento agli obiettivi da raggiungere. È importante che il livello di tolleranza del rischio sia stabilito contestualmente alla definizione degli obiettivi in modo da poter rappresentare un effettivo parametro nella gestione dei rischi e dell'azienda nel suo complesso.

Obiettivi di *Reporting*

Gli obiettivi di *reporting* riguardano la realizzazione di *report* validi con informazioni, verificate, tracciabili, tempestive e fruibili. Questo tipo di obiettivo può riguardare sia i documenti finanziari sia i documenti non finanziari e deve essere perseguito sia con riferimento alla reportistica indirizzata all'interno che a quella preparata per essere diffusa all'esterno.

Il raggiungimento degli obiettivi di ***reporting*** **finanziario rivolti all'esterno** deve essere valutato in relazione ai seguenti 3 punti di attenzione:

- Rispettare le norme/i principi contabili applicabili;
- Considerare la materialità nelle presentazioni delle dichiarazioni finanziarie e nelle esigenze dei destinatari;
- Riflettere le attività della Società.

Gli obiettivi di *reporting* finanziario rivolti all'esterno e che interessano soggetti terzi devono innanzitutto essere conformi alle norme, ai regolamenti e agli standard nazionali ed internazionali. Ai fini dell'accesso ai mercati regolamentati gli obiettivi di affidabilità della informativa finanziaria sono imprescindibili. Gli investitori, gli analisti e gli azionisti debbono disporre di dati finanziari affidabili per valutare e comparare le *performance* di un'impresa rispetto a quelle di un investimento alternativo.

Il *reporting* finanziario rivolto all'esterno include i bilanci pubblici, i rendiconti economici, le informazioni economiche specifiche, come i dati relativi ad una determinata *business unit*, anche solo distribuiti a determinate terze parti.

I bilanci pubblici includono informazioni selezionate ed aggregate dei risultati conseguiti durante un esercizio o durante un periodo più breve. Data la loro predisposizione ad essere resi disponibili al pubblico, la struttura dei dati è riconducibile agli standard imposti dai regolatori.

Le società quotate si avvalgono inoltre di un sistema normativo/documentale, composto da principi contabili, procedure amministrative contabili, linee guida, istruzioni operative, manuali contabili e piano dei conti, volto a garantire la *compliance* rispetto alle normative vigenti (i.e. Legge 262/2005, Sezione 404 del *Sarbanes-Oxley Act*, ecc., in funzione del mercato finanziario di riferimento) e a consentire così, al Dirigente Preposto/CFO di attestare, insieme agli organi amministrativi delegati, in generale e a titolo non esaustivo: (i) la corrispondenza dei documenti contabili societari alle risultanze documentali, ai libri ed alle scritture contabili; (ii) l'adeguatezza e l'effettiva applicazione del Sistema di controllo interno e di gestione del rischio sulla informativa finanziaria; (iii) l'idoneità dei documenti a fornire una rappresentazione veritiera e corretta della situazione patrimoniale, economica e finanziaria dell'emittente e dell'insieme delle imprese incluse nel consolidamento, così come specificato in maggior dettaglio dalle normative di riferimento.

I documenti consegnati esclusivamente a determinati fruitori, come banche, enti finanziatori o Pubblica Amministrazione, riguardano le informazioni che sono richieste dai relativi utilizzatori e pertanto l'attendibilità è tipicamente guidata dai relativi bandi (es. bandi per accedere a un finanziamento) o dagli standard richiesti, o da preesistenti contratti e/o accordi.

In sintesi, i *report* finanziari rivolti all'esterno devono possedere alcune caratteristiche, soprattutto qualitative, per rispettare le norme nazionali ed internazionali di volta in volta applicabili nonché le peculiari caratteristiche richieste da specifiche terze parti. Il termine affidabilità prevede che i *report* finanziari prodotti siano imparziali, obiettivi, esenti da errori significativi.

Gli **obiettivi di *reporting* non finanziario** rivolti all'interno devono essere raggiunti considerando i seguenti 3 punti di attenzione:

- Rispettare esistenti norme e *framework* esterni;
- Tenere in considerazione il livello di precisione richiesto;
- Riflettere le attività della Società.

I documenti rivolti all'esterno di natura non finanziaria, solitamente riguardano l'implementazione e l'adesione a determinati standard, come ad esempio lo Standard GRI, quelli ISO, o altri specifici standard.

Come quelli di tipo finanziario, devono classificare e sintetizzare, secondo il livello di dettaglio richiesto, le informazioni in maniera logica e strutturata, riportando i dati secondo i criteri previsti dai modelli esistenti.

Il raggiungimento degli **obiettivi di *reporting* interno** prevede i seguenti 3 punti di attenzione:

- Riflettere le scelte del *management*;
- Tenere in considerazione il livello di precisione richiesto;
- Riflettere le attività della Società.

I documenti prodotti e destinati ad un uso interno, sia di tipo finanziario che di tipo non finanziario, sono necessari al *management* come supporto al processo decisionale e per monitorare le *performance* aziendali. Esempi possono essere i risultati derivanti dalle campagne di *marketing*, la qualità della produzione o i risultati della soddisfazione dei dipendenti e dei clienti. Questi *report* sono sensibilmente diversi in base alla tipologia di organizzazione ed in relazione agli obiettivi prefissati. I documenti interni dipendono anche dalle esigenze del *management* ma, così come per i *report* rivolti all'esterno, è necessario che siano affidabili, adeguatamente dettagliati, verificati, tracciabili e fruibili per il destinatario delle informazioni. Altra qualità fondamentale è che i dati siano recenti ovvero che le informazioni salienti siano comunicate tempestivamente.

Obiettivi di Conformità

Gli obiettivi di *compliance* sono raggiunti se tutti o parte degli aspetti declinati nei seguenti 2 punti di attenzione risultino efficacemente applicati:

- Riflettere leggi e normative esterne;
- Tenere in considerazione la tolleranza al rischio.

Le organizzazioni devono condurre le loro attività rispettando le leggi e le normative applicabili anche in relazione al settore economico di appartenenza. All'interno di questo obiettivo l'impresa deve identificare e comprendere quali norme è tenuta ad applicare. In alcuni casi questa operazione può rivelarsi particolarmente complessa, in special modo per le aziende che hanno investito e operano in Paesi esteri con sistemi politici, giuridici e normativi radicalmente differenti.

Si tratta comunque di obiettivi importanti da perseguire per evitare ad esempio multe, sanzioni, interdizioni, annullamenti di contratti, danni di immagine e reputazionali.

1.2. Strumenti applicativi

Al fine di garantire che gli aspetti declinati nei punti di attenzione siano rispettati, le organizzazioni potrebbero adottare i seguenti strumenti, a titolo esemplificativo e non esaustivo:

- **Piano strategico**, che illustri, in termini qualitativi e quantitativi, le intenzioni del *management* relative alle strategie competitive dell'azienda, le azioni che saranno realizzate per il raggiungimento degli obiettivi strategici, la stima dei risultati attesi, compatibilmente al profilo di rischio assunto;
- **Processo strutturato di identificazione e valutazione dei rischi** (modelli di *Enterprise Risk Management*) associato agli obiettivi aziendali definiti che includa anche il processo di identificazione e valutazione del rischio nell'ambito della definizione del piano strategico/industriale;
- **Budget**, in cui vengano stabiliti gli obiettivi quantitativi delle diverse unità organizzative della Società in un arco temporale predefinito, al fine di conseguire un determinato risultato;

- **Reportistica periodica e strutturata supportata da strumenti informatici adeguati** che abbia l'obiettivo di monitorare e evidenziare nel continuo l'andamento del *business* e in particolare le variazioni tra i dati preventivati e quelli a consuntivo;
- **Politiche di remunerazione e incentivazione**:
  - attraverso le quali sia definito il sistema di incentivazione del *management* volto ad attrarre e motivare le risorse in possesso della capacità ed esperienza adeguata;
  - che colleghino la remunerazione dei dirigenti e del personale chiave ad una quota variabile della remunerazione (es. *MBO – Management by Objective*), in cui gli obiettivi dei diversi ruoli siano coerenti con gli obiettivi aziendali individuati in un orizzonte temporale di breve e lungo termine;
- **Monitoraggio dei *Key Performance Indicator*** *(KPI)*, grazie al quale l'organizzazione valuti l'andamento dei processi aziendali.

2. Principio n. 7 – L'organizzazione identifica i rischi connessi al conseguimento degli obiettivi aziendali e ne determina le modalità di gestione

Il contesto economico, ambientale, politico e normativo in forte cambiamento e sempre più complesso, in cui si riscontrano forti interdipendenze e la necessità di gestire sempre più frequentemente rischi emergenti, crea l'esigenza per la Società di evolvere i propri processi di gestione del rischio verso modelli di *Enterprise Risk Management* (ERM) più esaurienti, in termini di ambito di applicazione, ed integrati, in termini di processi aziendali applicati.

Il Principio 7 rappresenta il principio cardine dei Sistemi di controllo interno e di gestione del rischio. È necessario procedere all'identificazione dei rischi cui l'impresa è sottoposta; il Consiglio di Amministrazione deve pertanto approvare un modello di riferimento ed un processo di analisi che consenta all'organizzazione di identificare gli eventi che possono compromettere il conseguimento degli obiettivi prefissati, analizzarli, valutarli ed infine implementare dei meccanismi con i quali i rischi possono essere monitorati e mitigati (rafforzando i presidi, modificando l'operatività, attuando misure per il loro trasferimento – si veda *infra* par. 2.5.).

Il percorso logico da seguire per l'applicazione di tale principio prevede che inizialmente vi sia la scelta degli obiettivi, (come indicato nel Principio 6 commentato nel precedente par. 1); in seguito devono essere individuati e analizzati i rischi; infine, deve essere sviluppata la risposta al rischio.

L'identificazione dei rischi consiste in un processo iterativo, integrato con il processo di pianificazione.

Il Principio si compone di 5 punti di attenzione che definiscono più in dettaglio l'ambito e le modalità di applicazione.

2.1. Punto di attenzione – Includere gruppo, divisione, Società, attività operative e livelli funzionali

L'organizzazione identifica e valuta i rischi a livello di gruppo, divisione, società, attività operativa e livelli funzionali rilevanti al raggiungimento degli obiettivi.

L'approccio *top-down* per l'individuazione dei rischi parte dagli obiettivi aziendali, definiti nel *business plan*, e identifica e valuta i rischi a livello *enterprise*, nonché nella loro articolazione a livello di divisione, società e attività operativa. Il *management*, in qualità di *process owner*, è chiamato a individuare i rischi riferiti al proprio perimetro di competenza.

2.2. Punto di attenzione – Analizzare fattori interni e esterni

L'organizzazione individua i rischi prendendo in considerazione tutti i livelli dell'organizzazione stessa nonché l'ambiente economico, politico e normativo in cui opera.

Al fine di identificare e analizzare i rischi è necessario creare una mappa di tutti i fattori/eventi che potrebbero avere un impatto sul raggiungimento degli obiettivi. I fattori individuati possono essere interni o esterni all'impresa. I primi derivano dalla struttura della Società (ad es. cambiamenti nella strategia o nelle aspettative del *management*, le risorse e l'insieme di fattori utilizzati); i secondi vanno individuati considerando il contesto in cui l'impresa e opera (ad es. eventi naturali, cambiamenti delle normative e regolamenti adottati nel paese in cui opera l'impresa, effetti economici esogeni quali livello dei prezzi, variazione dei tassi, del livello di inflazione, occupazione, innovazione tecnologica, ecc.).

2.3. Punto di attenzione – Coinvolgere appropriati livelli di *management*

L'organizzazione mette in atto meccanismi efficaci di valutazione del rischio che coinvolgono appropriati livelli di *management*. In particolare, i rischi vengono identificati e valutati a livelli sufficientemente elevati nell'organizzazione così da individuare appieno le loro implicazioni e considerare appropriati piani di azione.

Il perimetro di *Risk Assessment* ricomprende la prima linea manageriale e, in funzione della tipologia e del livello di complessità di processo, si estende a più livelli manageriali, al fine di ottenere un'analisi dei rischi ragionevolmente solida e ricomprendere tutti i rischi rilevanti.

2.4. Punto di attenzione – Stimare la significatività dei rischi identificati

Il processo di identificazione e valutazione dei rischi si pone come obiettivo la contestualizzazione dei rischi da gestire utilizzando un approccio sistematico e strutturato. Tale processo specifica cosa può accadere, dove e quando, come e perché.

L'attività non può prescindere dal coinvolgimento del *management* che presidia quotidianamente le operazioni aziendali e il *business* (v. *supra* cap.I).

I metodi utilizzati per identificare i fattori di rischio sono diversi e variano in base alle necessità delle imprese. I più utilizzati sono:

- *brainstorming*, attività di gruppo promossa dal vertice, dove i vari responsabili aziendali si confrontano apertamente, aiutandosi nell'identificazione di possibili fattori di rischio;
- questionari, che possono essere indirizzati sia a operatori esterni come clienti e fornitori, sia ai responsabili interni;
- analisi comparative di settore, che permettono di raffrontare il comportamento dei *competitor*, individuando delle linee guida comuni al settore in cui si opera;
- indagini su incidenti ed eventi avversi occorsi, per identificare le cause e le future probabilità di manifestazione;
- analisi di scenario, attraverso le quali l'impresa può simulare diverse situazioni ambientali e socio-politiche, per cogliere quali fattori potrebbero influenzarla positivamente o negativamente.

Dopo aver individuato i rischi, l'organizzazione deve assegnare un valore economico agli stessi. Il valore dipende dalla probabilità che il rischio si verifichi e dal suo potenziale impatto sulle *performance* aziendali adottando una metodologia chiara ed applicabile secondo modalità quanto più possibile omogenee ed uniformi.

Gli strumenti utilizzati dalle imprese per effettuare l'analisi dei rischi vengono suddivisi in due gruppi: i metodi qualitativi e i metodi quantitativi (che possono prevedere livelli diversi

di complessità) o, in alternativa, una combinazione di questi, a seconda delle circostanze.

Il processo di identificazione e valutazione dei rischi genera una matrice della rilevanza in grado di individuare i rischi prioritari, ovvero quei rischi che in termini di impatto, probabilità di accadimento nonché livello di adeguatezza del Sistema di controllo interno a presidio, vulnerabilità della Società, richiedono di essere maggiormente presidiati.

2.5. Punto di attenzione – Determinare la risposta ai rischi

La risposta ai rischi individuati non può prescindere dalla definizione del livello di rischio ritenuto accettabile per l'azienda (*risk appetite*) che può variare anche in considerazione della tipologia di rischio che si sta gestendo nonché dalla tipologia di impatto dello stesso.

La declinazione del *risk appetite* è un processo che, considerati gli obiettivi strategici e operativi, fornisce agli organi di governo supporto per la pianificazione e il controllo del complesso dei rischi che sussistono sul *business* aziendale.

In considerazione del livello di rischio ritenuto accettabile, a seguito del processo di valutazione, si individuano i rischi che presentano *gap* rilevanti rispetto alle soglie di tolleranza definite dalla Società. Il *management* deve determinare quale risposta dare ai rischi, ossia valutare quali interventi è opportuno mettere in atto, in un'ottica costi-benefici, per tutelarsi dall'eventuale verificarsi di tali rischi.

Queste scelte possono essere assunte dal *management* avvalendosi di quattro differenti approcci principali:

I. Accettare il rischio

Davanti ad un rischio, il *management* può decidere di non intervenire e di "correre" il rischio di un suo eventuale accadimento. Con questo approccio l'organizzazione decide di non prendere alcuna ulteriore misura cautelare; infatti, dopo aver comparato il livello di rischio esistente con la tolleranza al rischio dell'impresa, decide se è il caso o meno di correre quel determinato rischio e, nel caso in cui decida di assumerlo, ritiene che non sia necessario implementare nessun sistema ulteriore di protezione dallo stesso.

II. Evitare il rischio

La risposta in questo caso coincide con l'eliminazione a priori e alla radice delle cause dell'esposizione al rischio. L'utilizzo di questo approccio deriva solitamente dalla filosofia e dalle esperienze passate del *management* che può giungere alla determinazione di non svolgere l'attività che comporterebbe l'assunzione di quel dato rischio.

III. Condividere/Trasferire i rischi

Questo approccio consiste nel trasferire il rischio verso terze parti esterne all'azienda. In questo caso i rischi vengono addossati, in tutto o in parte, a parti esterne in corrispondenza solitamente del pagamento di un premio.

La stipulazione di polizze di assicurazione, l'esternalizzazione di un'attività[1] in determinati ambiti, permette di condividere e/o di trasferire completamente lo specifico rischio. La tendenza è di trasferire i rischi difficilmente gestibili ovvero quelli il cui impatto è importante, ma la probabilità di evento bassa e quindi nei casi in cui non si disponga di sufficienti conoscenze dell'evento o si ritenga non efficiente attivare contromisure che possano gravare sulle modalità di esecuzione delle attività.

[1] Si noti che l'esternalizzazione non comporta sempre un totale trasferimento, in quanto la responsabilità ultima può rimanere all'interno dell'azienda.

IV. Mitigare il rischio

La risposta in questo caso consiste nell'adozione di provvedimenti e accortezze finalizzati a ridurre l'esposizione ai rischi. Le tecniche più utilizzate sono quelle riferibili al potenziamento dei sistemi di controllo e monitoraggio, ma anche azioni specifiche, quali la diversificazione dei portafogli di investimento, la diversificazione dei prodotti, ecc. possono concorrere a tale obiettivo. In aggiunta, è anche possibile mitigare il rischio attraverso la costituzione di accantonamenti specifici (ad esempio: accantonamenti per rischi legali).

2.6. Strumenti applicativi

Al fine di garantire che gli aspetti declinati nei punti di attenzione siano rispettati, le organizzazioni potrebbero adottare i seguenti strumenti, a titolo esemplificativo e non esaustivo:

- **Definizione del *risk appetite*** ovvero la propensione dell'organizzazione ad accettare e gestire i rischi;
- **Definizione di un modello integrato *Enterprise Risk Management* (ERM)**, ovvero di un modello volto a predisporre una metodologia di individuazione, valutazione e gestione integrata dei rischi. Il Modello, come specificato negli strumenti applicativi 2.5, oltre a definire un processo strutturato di identificazione e valutazione dei rischi associato agli obiettivi aziendali che includa anche il processo di identificazione e valutazione del rischio anche nell'ambito della definizione del piano strategico/industriale, dovrebbe avere lo scopo di mettere in atto una strategia di gestione del rischio della Società focalizzata sulla opportunità di rafforzare la capacità aziendale di creare, preservare e generare valore.
- **Definizione, implementazione e aggiornamento del SCIGR**, attraverso il quale l'azienda individui, valuti, monitori e misuri tutti i rischi d'impresa, coerentemente con il livello di rischio scelto/accettato dal vertice aziendale;
- ***Corpus* procedurale** (politiche, linee guida e procedure), in grado di definire l'integrazione e il funzionamento complessivo del SCIGR;
- **Monitoraggio *dei Key Risk Indicator* (KRI)**, ovvero un set di indicatori sintetici in grado di monitorare i rischi identificati in un preciso momento basandosi sull'elaborazione di dati quantitativi e comunicando lo stato di criticità del rischio identificato;
- **Analisi del contesto**, attraverso strumenti quali la *balanced scorecard*, l'analisi della concorrenza allargata (Porter) e l'analisi *Strengths, Weaknesses, Opportunities and Threats* (SWOT), finalizzati alla valutazione dei punti di forza/debolezza e delle opportunità/minacce alla competitività aziendale;
- **Analisi quantitative**, finalizzate alla stima della volatilità dei risultati di piano riconducibile ai rischi/opportunità identificati, calcolata attraverso modelli deterministici (*base, worst, best analysis*) ovvero stocastici (simulazione Montecarlo);
- **Implementazione di strumenti di *Governance Risk e Compliance* (GRC)**, ovvero di *tool* informatici a supporto dei modelli di gestione dei rischi e controlli che facilitano la gestione integrata del modello nonché la produzione di reportistica affidabile, tempestiva e fruibile per il *management*;
- **Piano di *Internal Audit Risk Based***, ovvero il piano di verifiche della funzione *Internal Audit* deve essere definito anche in base alle risultanze del processo di *Risk Assessment*.

3. Principio n. 8 – L'organizzazione prende in considerazione potenziali frodi nel valutare i rischi di conseguimento dei propri obiettivi aziendali

Il COSO include esplicitamente la considerazione del rischio di frode in sede di valutazione dei rischi. Il Principio 8 spiega che, come parte del processo di valutazione del rischio, l'organizzazione deve identificare le possibili modalità in cui le differenti tipologie di frode possono verificarsi (cd. schemi di frode).

La frode rappresenta il comportamento posto in essere da colui che elude le norme di legge, i regolamenti e le procedure aziendali per procurare a sé o ad altri un ingiusto profitto. Tale comportamento si può concretizzare nell'appropriazione indebita di beni, nella falsificazione di documenti, nella simulazione e/o dissimulazione di comportamenti, ecc.

La frode, in ambito aziendale, può comportare un rilevante danno economico e di immagine.

Questo principio esamina come la frode potrebbe impedire alla Società di raggiungere gli obiettivi individuati nel Principio 6.

Il Principio si compone di 4 punti di attenzione che definiscono più in dettaglio l'ambito e le modalità di applicazione.

3.1. Punto di attenzione – Considerare le varie tipologie di frode

L'organizzazione considera le diverse modalità di commissione di una frode che possono realizzarsi tramite diffusione di *report* (finanziari e non) deliberatamente omissivi, appropriazione indebita di beni, condotte illegali (es. violazione di leggi o regolamenti, ecc.).

L'implementazione di *fraud risk assessment* come processi di *risk management* verticali fornisce maggiore garanzia che l'*assessment* si focalizzi sulle debolezze del Sistema di Controllo Interno causate da atti intenzionali.

3.2. Punto di attenzione – Valutare gli incentivi e le pressioni

L'organizzazione considera incentivi e pressioni che potrebbero spingere i soggetti a commettere una frode.

Il Consiglio di Amministrazione, nel ruolo di *oversight*, definisce politiche e procedure, così come le aspettative sull'integrità e sui valori etici, sulla trasparenza e sulla responsabilità per l'attuazione e il funzionamento dei processi di gestione dei rischi di frodi.

3.3. Punto di attenzione – Valutare il rischio di frode

La Società considera i rischi di commettere frodi generate da un debole Sistema di controllo, da una scarsa supervisione del *management*, ecc.. La valutazione dei rischi di frode tiene conto, infatti, delle situazioni di non autorizzate acquisizioni, usi o cessioni di *asset*, dell'alterazione di registri e rendicontazioni o della commissione di altre condotte inappropriate.

3.4. Punto di attenzione – Valutare i comportamenti e le realizzazioni

L'organizzazione considera i motivi, personali o di contesto, che potrebbero spingere il *management* e il personale a intraprendere o giustificare azioni inappropriate.

Una adeguata attività di prevenzione delle frodi può consentire il risparmio di grosse somme di denaro riducendo al minimo i costi associati a eventi non previsti che possono minacciare

il perseguimento degli obiettivi, nonché salvaguardare il patrimonio e la reputazione aziendale.

Nella fase di prevenzione l'azienda analizza i propri processi per capire quali siano quelli maggiormente esposti al rischio di eventi fraudolenti e definisce la propria posizione rispetto al fenomeno fraudolento identificato. In tale contesto la Società conduce anche opportune attività di formazione e sensibilizzazione per trasmettere alle proprie risorse un'adeguata conoscenza delle iniziative in corso, pone in essere attività di *fraud risk assessment* specifici, ed emana un codice di condotta contenente i principi di comportamento da adottare a prevenzione di fenomeni fraudolenti.

La probabilità di accadimento di una frode può essere ridotta attraverso l'implementazione di un efficace programma antifrode e di un piano di prevenzione che contempli le seguenti attività:

- accertare l'esistenza di un adeguato Ambiente di Controllo Interno orientato a:
  - creare e mantenere una cultura di onestà, elevati standard etici e comportamentali;
  - prevedere sanzioni disciplinari per la violazione del codice etico;
  - definire un'adeguata sensibilità dell'organizzazione verso la frode e la sua prevenzione;
  - promuovere controlli preventivi, con finalità deterrenti, e di individuazione delle frodi;
- verificare l'esistenza di norme/istruzioni/procedure aziendali idonee a fornire i principi di riferimento generali in materia di prevenzione, individuazione e segnalazione delle frodi;
- verificare l'esistenza di bilanciati meccanismi di remunerazione ed incentivazione ed i relativi criteri applicativi;
- verificare l'esistenza di procedure di comunicazione interne volte a diffondere consapevolezza a livello aziendale in merito al rischio di frode ed atte a consentire la tempestiva segnalazione di quelle eventualmente individuate;
- identificare i fattori di rischio di frode (risorse, processi, sistemi) in grado di favorire la commissione di frodi e indagare così sui motivi che potrebbero spingere il personale ad intraprendere azioni inappropriate;
- individuare gli ambiti di operatività potenzialmente esposti al rischio di frodi e individuare i possibili controlli a presidio.

La sola prevenzione non assicura una totale difesa contro le frodi, ma rappresenta un primo fondamentale passo.

Successivamente, al fine di identificare tempestivamente la frode sarà necessario implementare un sistema di controllo che permetta di minimizzare il danno provocato, intervenendo in maniera quanto più possibilmente ravvicinata rispetto al momento di perpetrazione della frode.

L'esistenza di sistemi di rilevazione (*detection*) della frode, ovvero le attività che consentono di individuare prontamente se una frode è avvenuta, o stia avvenendo, costituisce il maggiore deterrente contro il rischio di frode.

Nella fase di rilevazione, un efficace supporto è fornito dalle tecniche di analisi delle transazioni e dell'operatività.

Queste tecniche hanno visto un rapido sviluppo che è avvenuto in concomitanza con quello degli strumenti di *data analytics* in grado di gestire ed elaborare tempestivamente grandi quantità di dati.

3.5. Strumenti applicativi

Al fine di garantire che gli aspetti declinati nei punti di attenzione siano rispettati, le organizzazioni potrebbero adottare i seguenti strumenti, a titolo esemplificativo e non esaustivo:

- **Modello di Organizzazione, Gestione e Controllo *ex* D.Lgs. 231/2001** e istituzione di un Organismo di Vigilanza, al fine di orientare il SCIGR all'identificazione, valutazione e gestione dei rischi che potrebbero compromettere il raggiungimento degli obiettivi aziendali;
- **Codice Etico (e/o di Condotta e/o di Comportamento)**, che definisca il complesso di norme etiche e sociali condivise e promosse dall'azienda e al quale i dipendenti e gli esponenti aziendali devono attenersi e proibisca, senza eccezioni, pratiche e attitudini riconducibili al compimento o alla partecipazione al compimento di frodi;
- **Definizione degli schemi di frode** seguendo anche i suggerimenti forniti dalla *Association of Certified Fraud Examiners* (ACFE);
- ***Programmi di Fraud Risk Assessment and Prevention***: la Società dovrebbe eseguire una valutazione complessiva del rischio di frode, per identificare specifici schemi e rischi di frode, in termini di probabilità e impatto, e delle Attività di Controllo delle frodi esistenti e attua azioni volte a mitigare i rischi residui di frode;
- **Politiche di remunerazione e incentivazione**, che chiarifichino il sistema degli incentivi e delle remunerazioni, agganciando la remunerazione dei dirigenti e del personale chiave ad una quota variabile della remunerazione, basata su meccanismi di determinazione oggettivi, trasparenti e verificabili;
- **Sistema sanzionatorio,** che preveda i diversi livelli di sanzioni e le relative modalità di applicazione in relazione a differenti tipologie di violazioni (di norme o procedure aziendali interne, norme di legge, comportamenti contrari all'etica, ecc.) effettuate da parte degli organi sociali, del personale aziendale e di terze parti**;**
- **Sistema di segnalazione delle violazioni (*whistleblowing*)**, volto a permettere la segnalazione, anche in forma anonima, di potenziali fenomeni fraudolenti e, in generale, situazioni pericolose che possano arrecare, in modo diretto o indiretto, un danno economico-patrimoniale e/o di immagine all'azienda/ente. Il sistema di segnalazione dovrebbe coinvolgere clienti, *partner* commerciali, cittadini e, in generale, parti terze in grado di dare il loro contributo**.**

4. Principio n. 9 – L'organizzazione identifica e valuta i cambiamenti che potrebbero avere impatti significativi sul Sistema di controllo interno

Il Principio 9 prevede che l'organizzazione identifichi e valuti i cambiamenti che potrebbero avere un impatto significativo sul SCIGR. Ciò significa che nell'ambito del processo di valutazione dei rischi, il *management* deve considerare i cambiamenti che possono compromettere il raggiungimento degli obiettivi.

In particolare occorre tenere in considerazione i seguenti cambiamenti:

- dell'ambiente esterno;
- nel modello di *business*;
- nella *leadership*.

L'organizzazione gestisce i cambiamenti significativi con un processo analogo a quello di *Risk Assessment*. Le modalità per identificare i cambiamenti influenti sono molteplici e devono essere incentrati sulle previsioni future in modo da poter anticipare e pianificare in modo ottimale le risposte. Nel caso di cambiamenti significativi dovrebbero essere previsti dei

sistemi di *alert* in grado segnalare tempestivamente eventuali nuovi rischi.

Il Principio si compone di 3 punti di attenzione che definiscono più in dettaglio l'ambito e le modalità di applicazione.

4.1. Punto di attenzione – Valutare i cambiamenti dell'ambiente esterno

Nel valutare i cambiamenti nel contesto esterno il *management* deve prendere in considerazione possibili impatti di breve, medio, ma anche lungo termine. A titolo esemplificativo bisogna accuratamente valutare l'eventuale introduzione di una nuova regolamentazione o gli impatti sui prezzi delle materie prime nonché sulla effettiva disponibilità delle stesse derivanti da guerre, importanti conflitti diplomatici o catastrofi naturali; in generale debbono essere considerati gli impatti derivanti dal verificarsi di eventi eccezionali. Un'organizzazione deve inoltre considerare l'eventualità di definire un processo di *business continuity* che includa anche lo spostamento delle sedi produttive e il reperimento di risorse alternative o da fornitori alternativi.

4.2. Punto di attenzione – Valutare i cambiamenti nel modello di *business*

I cambiamenti al modello di *business* possono riguardare il lancio di una nuova linea produttiva o variazioni nella logistica, operazioni di *Merger & Acquisition* e disinvestimenti, accrescimento/ridimensionamento dell'organizzazione, operazioni con Paesi esteri e nuove tecnologie. Tutti questi cambiamenti possono modificare l'equilibrio esistente e pertanto rendono necessaria una rivalutazione dei rischi.

4.3. Punto di attenzione – Valutare i cambiamenti nella *leadership*

Le organizzazioni devono inoltre valutare l'impatto sul SCIGR di un cambio dei vertici aziendali che può riflettere una variazione nella filosofia di conduzione aziendale anche associabile ad una diversa concezione dei rischi e della propensione al rischio che può determinare diverse scelte di investimento, di avvio di nuove iniziative, in sintesi diverse modalità di gestione aziendale.

4.4. Strumenti applicativi

Al fine di garantire che gli aspetti declinati nei punti di attenzione siano rispettati, le organizzazioni potrebbero adottare i seguenti strumenti, a titolo esemplificativo e non esaustivo:

- **Analisi *SWOT (Strengths, Weaknesses, Opportunities, Threats*)** ovvero individuare, analizzare e confrontare i punti di forza e di debolezza interni all'azienda nonché le minacce e opportunità che caratterizzano l'idea di impresa;
- **Analisi dei *competitor,*** attraverso la quale vengano esaminate le principali imprese che operano nello stesso mercato/settore in cui opera l'impresa al fine di valutarne i vantaggi competitivi;
- **Analisi dei prodotti/servizi**, che consenta di definire la loro combinazione ottimale e che dovranno quindi essere valorizzati in chiave economica;
- **Analisi della clientela**, ovvero l'individuazione dei bisogni dei potenziali clienti per la conseguente calibrazione dell'offerta;
- **Analisi degli effetti nel cambiamento di *leadership*** che evidenzi l'importanza della formazione e della valutazione della *leadership* sulla base di variegate dimensioni comportamentali: manageriale, relazionale, ecc.;

- **Analisi scenario normativo che monitori l'evoluzione delle normative di riferimento** ovvero delle normative che potrebbero avere un impatto sull'andamento del *business* e sulla gestione della Società;
- ***Business Impact Analysis*** **e Piano di** ***Business Continuity*** ovvero valutazione dei potenziali impatti finanziari e operativi in caso di discontinuità di una o più funzioni aziendali e definizione di un piano che assicuri la continuità aziendale in caso di crisi/eventi straordinari.

CAPITOLO III

ATTIVITÀ DI CONTROLLO (*CONTROL ACTIVITIES*)

1. Principio n. 10 – L'organizzazione definisce e implementa Attività di Controllo che contribuiscano a ridurre i rischi entro livelli accettabili - 2. Principio n. 11 – L'organizzazione definisce e implementa attività di controllo sulla tecnologia, per supportare il raggiungimento degli obiettivi aziendali - 3. Principio n. 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

***

Le Attività di Controllo sono azioni e misure stabilite attraverso linee guida (*policy*) e procedure finalizzate ad assicurare l'attuazione delle direttive del *managemen*t per mitigare i rischi di mancato raggiungimento degli obiettivi aziendali (strategici, correlati all'informativa interna e verso l'esterno, di *compliance, ecc.*).

Queste attività vanno identificate a tutti i livelli dell'organizzazione, nelle differenti fasi dei processi aziendali, anche con riferimento alla gestione complessiva dei sistemi informativi.

Possono essere di **natura manuale** o **automatica** e si identificano tipicamente in autorizzazioni ed approvazioni, verifiche, riconciliazioni, controlli fisici, ma anche in misure di più ampio respiro come analisi degli scostamenti e *business performance review*.

E' in ogni caso opportuno che, ove percorribile, l'identificazione e lo sviluppo delle Attività di Controllo avvengano in ottica di separazione dei compiti (cd. *segregation of duties*), al fine di evitare che si gestisca in autonomia un intero processo o che si attribuiscano al medesimo soggetto attività tra loro potenzialmente incompatibili ovvero, nel caso in cui questo non sia possibile, siano individuati idonei meccanismi compensativi.

È possibile distinguere Attività di Controllo di **natura preventiva** (*preventive*) o **successiva** (*detective*) in relazione alla loro capacità di prevenire o rilevare a posteriori eventuali errori non intenzionali o frodi.

Riguardo alle altre componenti del SCIGR, le Attività di Controllo dovrebbero essere strettamente correlate alla valutazione dei rischi (*Risk Assessment*), già descritta nel capitolo II: l'identificazione delle Attività di Controllo nell'ambito dei processi aziendali, il loro sviluppo nella gestione dei sistemi informativi e la loro collocazione ai differenti livelli dell'organizzazione dovrebbero infatti essere funzionali ad impedire che eventi negativi possano pregiudicare il raggiungimento degli obiettivi aziendali, attraverso la loro identificazione preventiva o la rilevazione tempestiva di eventuali malfunzionamenti (v. *supra* cap. II, par.2.5).

Le caratteristiche delle Attività di Controllo (pervasività, collocazione nella struttura organizzativa, ecc.) sono peraltro inevitabilmente influenzate dall'Ambiente di controllo (*Control environment*) e dunque dalla cultura aziendale (v. *supra* cap. I).

I risultati del funzionamento di tali attività (anche derivanti da Attività di Monitoraggio, continuo o periodico), inoltre, specie avendo riguardo ad eventuali anomalie e malfunzionamenti, dovrebbero costituire oggetto di adeguati flussi di comunicazione verso le strutture aziendali interessate, al fine di disporre di informazioni utili al processo decisionale per:

- valutare la solidità dei processi aziendali;
- intraprendere con tempestività eventuali azioni correttive necessarie.

Il COSO identifica 3 principi che dovrebbero essere sempre rispettati per il corretto disegno delle Attività di Controllo. Affinché le stesse siano costruite in maniera efficace e

contribuiscano in maniera ottimale al raggiungimento degli obiettivi aziendali, è utile che tali Principi siano riflessi in modalità operative che tengano conto dei correlati 16 elementi di attenzione, come di seguito approfondito.

1. Principio n. 10 – L'organizzazione definisce e implementa Attività di Controllo che contribuiscono a ridurre i rischi entro livelli accettabili

Il Principio 10 sottolinea la necessità che l'identificazione delle Attività di Controllo da implementare (e successivamente da monitorare) sia strettamente correlata con i rischi che potrebbero pregiudicare il raggiungimento degli obiettivi aziendali e con i relativi livelli di accettazione/tolleranza, facendo riferimento ai processi aziendali rilevanti.

Ciò determina il fatto che organizzazioni che svolgono *business* anche similari possano richiedere l'implementazione di Attività di controllo sensibilmente differenti, per effetto di diversi obiettivi da perseguire e di differente propensione al rischio.

Il Principio si compone di 6 punti di attenzione che definiscono più in dettaglio l'ambito e le modalità di applicazione.

1.1. Punto di attenzione – Integrazione con le attività di identificazione e valutazione dei rischi (*Risk Assessment*): le Attività di Controllo devono aiutare ad assicurare che le risposte ai rischi siano attuate

L'identificazione e la selezione delle Attività di Controllo dovrebbero essere **strettamente correlate all'individuazione dei rischi aziendali** (v. *supra* cap. II), con l'obiettivo di prevedere misure finalizzate alla loro prevenzione ed al loro contenimento, tenendo conto delle relative priorità e della propensione e tolleranza al rischio.

L'implementazione di Attività di Controllo ha infatti la finalità primaria di assicurare che le risposte ai rischi aziendali siano adeguate e abbiano effettiva attuazione, in linea con le direttive del *management* in merito all'accettabilità o meno degli stessi e più in generale alla propensione al rischio dell'organizzazione.

Nel caso in cui l'organizzazione intenda accettare o evitare i rischi, potrebbero non risultare necessarie risposte al rischio specifiche e conseguentemente l'implementazione delle correlate Attività di Controllo.

Di particolare rilevanza risulta pertanto la rilevazione e rappresentazione dei rischi, in modo da consentire, tra l'altro, il corretto disegno delle Attività di Controllo (ossia la loro teorica capacità di prevenire/mitigare i rischi per mantenersi entro i livelli di accettabilità definiti, ma anche le loro eventuali ridondanze o carenze) ed insieme l'individuazione di eventuali *gap* da colmare con opportune azioni correttive.

Le Attività di Controllo dovranno, peraltro, essere **tanto più stringenti quanto più è limitato il livello di tolleranza al rischio**; per questo motivo risulta di fondamentale importanza che esso sia conosciuto e diffuso nell'organizzazione.

È opportuno che il *management* definisca con attenzione il loro perimetro di intervento: nell'identificazione delle azioni da porre in essere per mitigare i rischi identificati, dovranno essere considerati tutti gli ambiti entro cui le operazioni aziendali si svolgono e pertanto le misure potranno interessare anche le attività affidate in *outsourcing*.

1.2. Punto di attenzione – Identificazione dei fattori aziendali rilevanti che impattano sulle Attività di Controllo da implementare

Per la piena efficacia delle Attività di Controllo, è opportuno che nella loro identificazione e nel disegno delle caratteristiche attese si tengano in adeguata considerazione gli elementi peculiari dell'organizzazione e delle attività aziendali.

Tra essi possono assumere rilevanza, a titolo esemplificativo, le caratteristiche e la complessità del modello organizzativo e di *business*, la propensione aziendale al rischio, la cultura aziendale, il livello di informatizzazione dei processi, il complesso regolamentare da osservare, anche su base internazionale, ecc.

1.3. Punto di attenzione – Identificazione dei processi di *business* rilevanti che richiedono Attività di Controllo

Al fine di garantire un adeguato disegno delle Attività di Controllo, è necessario identificare in via preliminare **i processi di *business* rilevanti**, individuando gli aspetti che - sulla base dei rischi che possono manifestarsi – necessitano di misure di prevenzione, tenendo anche in considerazione eventuali attività gestite da terzi.

In tale contesto, oltre alle attività svolte manualmente, assumono particolare rilevanza i sistemi informativi utilizzati per lo svolgimento delle attività, al fine di identificare i rischi correlati ma anche le verifiche e i controlli basati sugli stessi.

Parimenti, come osservato (v. *supra* par.1.1), è opportuno assicurare adeguate misure di prevenzione anche su eventuali processi o parti degli stessi affidati all'esterno, sia nelle interazioni con gli *outsourcer* (controlli sulla contrattualistica, sugli *input* forniti e sugli *output* ricevuti), ma anche sulle misure di controllo da questi adottate.

Nell'identificazione delle misure di controllo da implementare (e nella valutazione del loro corretto disegno) è opportuno assicurarsi che siano indirizzati (con appropriate misure finalizzate a garantirne il raggiungimento) anche gli **obiettivi di completezza, accuratezza e validità delle informazioni** (cd. "*information-processing objective*"), al fine di consentire che le operazioni aziendali:

- siano debitamente registrate,
- siano registrate tempestivamente, per il loro corretto ammontare e nei conti opportuni,
- rappresentino eventi effettivamente accaduti e gestiti secondo le procedure attese, autorizzate nelle forme previste e dai soggetti identificati, anche per effetto di un'appropriata restrizione degli accessi.

1.4. Punto di attenzione – Identificazione del *mix* delle Attività di Controllo

Le Attività di Controllo dovrebbero insistere in prima battuta sulle transazioni aziendali per cui assicurare completezza, accuratezza e validità e dovrebbero garantire che le stesse siano gestite solo da persone debitamente autorizzate.

Ne sono esempi:

- autorizzazioni ed approvazioni;
- *check* e verifiche comparative;
- conte fisiche;
- controlli sulla completezza/correttezza dei dati (incluse verifiche sulle anagrafiche, riconciliazioni, attività di supervisione finalizzate ad assicurare che i controlli attesi

siano stati svolti correttamente e tempestivamente ed eventuali anomalie siano state debitamente indirizzate).

Oltre ai controlli sulle specifiche transazioni, è importante assicurare che siano altresì implementate misure di controllo più ampie, finalizzate ad intercettare ed indagare eventuali anomalie sulla loro complessità e le relative cause.

Ne sono tipici esempi:

- le analisi di scostamenti tra dati previsionali e consuntivi;
- le *business performance review*.

Occorre in ogni caso che nell'identificazione delle Attività di Controllo sia assicurato un **giusto equilibrio** con riferimento alla loro natura, attraverso un *mix* di controlli automatici, semiautomatici e manuali, preventivi e successivi, che siano in grado sia di prevenire, sia di intercettare gli errori non intenzionali e le frodi. A questo riguardo, anche in relazione alla presenza sempre più pervasiva della tecnologia nella conduzione dei processi aziendali, assumono un'importanza crescente i controlli che insistono nei sistemi informatici, che di norma garantiscono una maggiore affidabilità di esecuzione.

Nella loro configurazione (disegno dei controlli), è fondamentale:

- considerare i rischi che si intende prevenire;
- prevedere che i controlli implementati siano debitamente documentati e ripercorribili, nelle verifiche fatte e negli esiti raggiunti.

1.5. Punto di attenzione – Identificazione della collocazione dei controlli

Parimenti, risulta di fondamentale rilevanza che nell'identificazione delle Attività di Controllo sia prestata adeguata attenzione alla loro collocazione nel processo e che le stesse siano **poste in essere ai vari livelli dell'organizzazione**, specificando eventuali soglie che determinano lo svolgimento dei controlli stessi.

1.6. Punto di attenzione – *Segregation of Duties*

Particolare attenzione deve essere dedicata alla separazione delle attività che è opportuno affidare a soggetti diversi (attività cd. "incompatibili") o comunque all'identificazione di contromisure in grado di prevenirne i rischi correlati.

La separazione delle attività o compiti (anche detta *segregation of duties*, abbreviato SoD) consente di indirizzare e mitigare rischi significativi correlati all'aggiramento dei controlli da parte del *management* (*management override)* e alla frode, limitando la possibilità che un soggetto agisca da solo; parimenti, in relazione all'intervento di più persone nell'esecuzione di attività e controlli, contribuisce a contenere rischi di errori non intenzionali.

Tuttavia, in alcuni casi la separazione dei compiti non è pratica, economica o perseguibile in relazione alle caratteristiche e alle dimensioni dell'organizzazione; in tali circostanze è necessario istituire controlli alternativi.

1.7. Strumenti applicativi

Si riportano di seguito, a titolo esemplificativo e non esaustivo, alcuni elementi di concreta attuazione dei punti di attenzione del principio in esame:

- **rappresentazione della catena del valore aziendale**, con identificazione dei processi "*core*" e di supporto;
- **rappresentazione dei controlli all'interno delle matrici dei rischi** prodotte nell'ambito delle attività di *Risk Assessment*: inserimento nella mappatura dei processi aziendali rilevanti, e delle matrici dei rischi, dei controlli (manuali ed

automatici, di natura preventiva e successiva), in grado di indirizzare completezza, accuratezza e validità delle informazioni processate e restrizione degli accessi (*information-processing objective)*, eventualmente accompagnate da note descrittive (*narrative*) e diagrammi di flusso (*flow chart*);

- **identificazione degli *outsourcer* significativi per i processi rilevanti** e delle correlate tipologie di controlli da assicurare (controlli sugli *input* forniti e sugli *output* ricevuti, controlli sulla contrattualistica, attività di *Third Party Assurance* ed acquisizione di report sui controlli della *service organization*, di tipo I o II). Le analisi preventive alla stipula dei contratti consentiranno peraltro di prevedere adeguati *Service Level Agreement* e *Operational Level Agreement* all'interno degli stessi contratti;
- **predisposizione di documenti di *Gap Analysis*** (rischi vs. controlli), inclusivi della valutazione delle eventuali carenze individuate e delle relative azioni correttive, con identificazione di responsabilità e scadenze;
- **lista dei principi di SoD da assicurare**;
- **svolgimento di analisi SoD** (organizzativa e sistemica);
- **svolgimento di analisi del "transato"** e identificazione di controlli compensativi in caso di principi SoD non rispettati;
- ***Corpus* procedurale** (politiche, linee guida e procedure), contenenti i controlli da assicurare, completi di responsabilità di esecuzione, tempistiche, modalità, strumenti da utilizzare idonei a garantire l'efficacia e l'efficienza del Sistema di Controllo Interno e Gestione dei Rischi nel tempo e a prevenire e individuare irregolarità e/o atti fraudolenti.

2. Principio n. 11 – L'organizzazione definisce e implementa Attività di Controllo sulla tecnologia, per supportare il raggiungimento degli obiettivi aziendali

Il Principio 11 si riferisce al ruolo rilevante che i processi IT rivestono nel SCIGR. Un numero crescente di dati ed informazioni dell'azienda risiede nei sistemi informativi. Per garantirne l'integrità e l'affidabilità, ma anche per poterli proficuamente utilizzare a supporto del raggiungimento degli obiettivi aziendali, è necessario garantire l'implementazione di adeguate misure di prevenzione.

La tecnologia rappresenta, infatti, di per sé, un rischio da mitigare in relazione al crescente volume di attività gestite per via informatica, ma al contempo può essere uno strumento efficace per svolgere i controlli.

In conseguenza della crescente pervasività della tecnologia nella vita aziendale (processi, flussi informativi, ecc.), il principio sottolinea la necessità di implementare (e monitorare) i controlli generali sui sistemi informativi aziendali.

Anche al fine di poter fare affidamento sui controlli automatici implementati nei processi aziendali rilevanti, è importante assicurare che sui relativi sistemi informativi insistano dei controlli generali finalizzati ad assicurare l'adeguatezza della loro gestione. A tale riguardo è necessario identificare in via preliminare le applicazioni e l'infrastruttura interessati da tali Attività di Controllo. La configurazione dei sistemi IT deve conseguentemente supportare i controlli attesi.

Nel panorama dei controlli da assicurare, particolare rilievo assumono i controlli a garanzia della sicurezza e dell'integrità delle informazioni, che non possono prescindere da una precisa identificazione dei soggetti abilitati ad accedere ai sistemi e dei relativi diritti di accesso (visualizzazione, modifica, ecc.). Ugualmente, specifica attenzione deve essere garantita con riferimento all'acquisto, allo sviluppo e al mantenimento dell'infrastruttura

tecnologica.

Conseguentemente, risulta imprescindibile assicurare l'affidabilità dei sistemi attraverso l'implementazione di controlli pervasivi in relazione all'infrastruttura tecnologica, alla sicurezza logica e fisica, ai processi di acquisizione, allo sviluppo e al mantenimento (*maintenance*) dei sistemi.

Il Principio si compone di 4 punti di attenzione che definiscono più in dettaglio l'ambito e le modalità di applicazione.

2.1. Punto di attenzione – Correlazione tra uso della tecnologia nei processi di *business* e controlli generali sulla tecnologia

Affinché l'uso della tecnologia nei processi di *business*, compresi i controlli automatici implementati nei processi aziendali rilevanti, sia affidabile, è necessario che siano individuate e implementate specifiche Attività di Controllo sui sistemi informativi ("controlli generali sui sistemi informativi").

Come per gli altri processi aziendali, è infatti opportuno prevedere Attività di Controllo in merito all'acquisizione, allo sviluppo, alla *maintenance* e all'accesso alla tecnologia al fine di prevenire e mitigare i rischi correlati.

I controlli generali sui sistemi informativi contribuiscono ad assicurare che i controlli automatici operino correttamente sin dall'origine in quanto correttamente disegnati e operino con efficacia nel continuo una volta implementati.

L'organizzazione è chiamata a mantenere traccia del collegamento tra la tecnologia utilizzata e le correlate Attività di Controllo mediante lista/mappatura delle applicazioni aziendali, matrici di controllo, diagrammi di flusso (*flow chart*) e descrizione dei processi (*narrative*).

In questo modo è possibile comprendere quali aspetti della tecnologia (infrastruttura, sicurezza, sviluppo, *maintenance*) sono indispensabili per la continuità del servizio e quali aspetti sono specificamente legati al disegno ed al funzionamento dei controlli automatici.

2.2. Punto di attenzione – Identificazione delle Attività di Controllo sull'infrastruttura tecnologica

I controlli generali sui sistemi informativi coinvolgono la gestione della sicurezza, l'acquisto, lo sviluppo e il mantenimento dell'infrastruttura tecnologica.

L'estensione e la profondità delle Attività di Controllo che afferiscono questi ambiti dipendono dalla complessità della tecnologia e dai rischi dei processi di *business* sottostanti che vengono supportati.

Così come i controlli sui processi e sulle transazioni, anche i controlli sulla tecnologia possono includere sia controlli manuali che automatici.

L'infrastruttura tecnologica può essere complessa, ad esempio può essere condivisa da diverse unità di *business*, o può essere gestita da terze parti o ancora può avere una collocazione di servizio indipendente (*cloud computing*).

L'organizzazione deve far fronte a tale complessità attraverso appropriate misure e rispondere tempestivamente ai nuovi rischi che si presentano con l'evoluzione della tecnologia, anche prevedendo e implementando procedure di *backup* e *disaster recovery* adattate al contesto di riferimento.

2.3. Punto di attenzione – Identificazione dei controlli rilevanti sulla sicurezza informatica

La gestione della sicurezza deve prevedere Attività di Controllo sugli accessi (rete, applicazioni, locali, ecc.) per garantire che solo il personale autorizzato possa accedere ai sistemi informativi, al fine di ridurre il rischio che i dati possano essere modificati o manomessi da personale non autorizzato.

I controlli di sicurezza sugli accessi (in linea con le *policy* e le procedure dell'organizzazione) proteggono da accessi non autorizzati e dall'utilizzo non autorizzato dei dati e delle informazioni presenti nei sistemi e supportano anche la *segregation of duties*. Prevenendo l'utilizzo improprio ed eventuali modifiche non autorizzate, l'integrità dei dati e dei sistemi può essere protetta da intenti fraudolenti o da semplici errori.

Le minacce alla sicurezza dei dati possono essere sia di origine interna che esterna:

- le minacce esterne si verificano con maggior frequenza negli ambienti interconnessi, che peraltro contraddistinguono l'operatività dell'attuale contesto di *business*. E' pertanto necessario tenere il passo con l'evoluzione della tecnologia per fronteggiare i nuovi rischi correlati;
- le minacce interne provengono tipicamente da *ex* dipendenti o dipendenti insoddisfatti o disonesti, che, attraverso le loro conoscenze sia dei processi che dei sistemi di sicurezza, possono essere motivati a commettere atti dolosi a discapito dell'organizzazione.

L'accesso ai sistemi dovrebbe essere limitato a soli utenti autorizzati, come sopra indicato; sono pertanto attese Attività di Controllo sulle procedure di autenticazione. A tal proposito, i sistemi dovrebbero essere configurati in modo tale da riconoscere solo le utenze autorizzate e approvate dal *management* e prevedere modalità apposite per autenticare gli utenti, come ad esempio parametri chiave, lunghezza minima e durata della *password*.

Le Attività di Controllo dovrebbero peraltro essere orientate a verificare che gli accessi:

- avvengano solo da parte di utenti autorizzati;
- siano attribuiti, nel rispetto del principio di *segregation of duties*, a ruoli/funzioni dalle responsabilità assegnate coerenti con l'utilizzo atteso delle informazioni e dei dati sottese;
- siano revocati in caso di cambiamenti nelle responsabilità assegnate, ove non più coerenti con l'utilizzo atteso dei dati e delle informazioni sottese.

A tale riguardo, dovrebbero essere attivate misure che contemplino tra l'altro:

- la previsione di procedure che evidenzino formalmente la richiesta, la sospensione, la disattivazione, il cambio di utenze attive;
- standard di autenticazione che prevedano una lunghezza minima dei caratteri della *password* ed un numero definito di possibili tentativi di accesso;
- l'utilizzo limitato di utenze privilegiate *(*c.d. *"super user")* responsabili della sicurezza delle informazioni, monitorate dal *management* per prevenire usi impropri;
- lo svolgimento di periodiche *review* degli accessi al fine di monitorare eventuali violazioni, da riportare tempestivamente al *management* per l'identificazione di appropriate azioni correttive;
- *log* di sicurezza generati dagli applicativi e dai sistemi, che consentano di monitorare da chi sono svolte le attività e cosa viene effettivamente fatto.

2.4. Punto di attenzione – Sviluppo di Attività di Controllo sull'acquisizione, sviluppo e *maintenance* della tecnologia

I controlli generali sulla tecnologia supportano l'acquisto, lo sviluppo e mantenimento dell'infrastruttura tecnologica. Le metodologie di sviluppo tecnologico ("*system development life cycle*") dovrebbero fornire una struttura per il disegno e l'implementazione del sistema, che delinei le fasi specifiche, la documentazione, i requisiti, le approvazioni e diversi controlli in merito ad acquisizione, lo sviluppo e la manutenzione dell'infrastruttura tecnologica.

Prima di procedere ad una modifica dei sistemi informativi, tali processi dovrebbero prevedere una specifica richiesta di autorizzazione alla modifica, appropriate approvazioni, *test* di prova e protocolli per determinare se le modifiche sono state apportate correttamente. In particolare:

- le modifiche dovrebbero essere apportate solo a seguito di una specifica richiesta di sviluppo. Tutte le fasi della modifica dovrebbero essere autorizzate, tracciate e monitorate;
- gli standard di programmazione dovrebbero essere seguiti durante tutte le fasi di disegno e dovrebbero essere messe in atto procedure che prevedano i nuovi controlli da porre in essere;
- dovrebbero essere effettuati opportuni test prima del "*go live*", per verificare che le modifiche siano state apportate in modo corretto e non abbiano impattato negativamente i sistemi già esistenti (i *test* tipicamente variano a seconda del tipo di cambiamento effettuato);
- dovrebbero essere effettuate verifiche finalizzate ad assicurare la completezza, l'accuratezza e la validità dei dati presenti nei vecchi sistemi e riversati nei nuovi;
- prima della definitiva implementazione delle modifiche/nuovi sistemi, i cambiamenti dovrebbero essere approvati dagli *stakeholder*;
- gli utenti finali dovrebbero essere formati mediante apposite sezioni di *training*.

Alcune realtà prevedono stesse procedure e modalità di esecuzione sia per grandi che per piccole modifiche, altre invece prevedono metodologie distinte per lo sviluppo e per il *change management*. In ogni caso, i controlli da assicurare dovrebbero essere strettamente correlati con il livello di rischio dell'iniziativa.

Un'alternativa allo sviluppo *in-house* è l'utilizzo di pacchetti *software*. I produttori forniscono sistemi integrati e flessibili, che possono essere personalizzati a seconda delle esigenze di *business*. In tal caso, i controlli da assicurare dovrebbero insistere sia sul processo di acquisizione che su quello di implementazione e *maintenance*.

Altra alternativa è *l'outsourcing*: nel caso in cui un sistema sia gestito dall'*outsourcer*, l'organizzazione deve verificare la completezza, l'accuratezza e la validità delle informazioni fornite e ricevute dal fornitore del servizio in *outsourcing*.

2.5. Strumenti applicativi

Si riportano di seguito, a titolo esemplificativo e non esaustivo, alcuni elementi di concreta attuazione dei punti di attenzione del principio in esame:

- **Lista/mappatura delle applicazioni aziendali** (con identificazione di quelle rilevanti per le attività di analisi specifiche);
- ***Information Technology General Control*** (ambiti da considerare: sviluppo e manutenzione dei sistemi applicativi, operatività dei sistemi informatici, gestione dei database, gestione delle reti di comunicazione, gestione dei *software* di sistema, sicurezza delle informazioni);

- Identificazione dei **profili di accesso ai sistemi** e relativi diritti e verifica periodica dell'effettivo rispetto dei requisiti identificati;
- Matrice funzionale dei profili attivati;
- Procedura per l'abilitazione ai sistemi informatici aziendali;
- ***Vulnerability assessment*** e piani anti-intrusione;
- Mappatura dei fogli di calcolo e controlli attesi;
- Documentazione della configurazione dei sistemi IT.

3. Principio n. 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

Il Principio 12 enfatizza l'importanza di definire e diffondere, attraverso strumenti di adeguato livello di dettaglio, i comportamenti attesi, le responsabilità ed i compiti assegnati, le attività da svolgere, i controlli da assicurare e le relative modalità attuative.

E' opportuno che il *management* indirizzi, attraverso appropriate linee guida, i principi di comportamento e le attività da porre in essere per implementare i controlli da assicurare. Tali *policy* dovrebbero essere documentate, anche attraverso apposite comunicazioni.

Le procedure si traducono nelle azioni necessarie per implementare le linee guida (o *policy*), individuando le Attività di Controllo da assicurare.

Al fine di garantire un appropriato coinvolgimento (*commitment)*, è importante che le *policy* e le procedure di maggiore rilievo siano approvate direttamente dal Consiglio di Amministrazione.

Policy e procedure sono talora comunicate oralmente: *policy* non scritte sono comuni laddove esista una prassi consolidata, soprattutto nelle piccole realtà, in cui i canali comunicativi prevedono una stretta interazione con il personale. Anche se tale circostanza può apparire un'alternativa conveniente, regole non scritte rappresentano un pericolo, dal momento che possono essere facilmente aggirate, riducono il senso di responsabilità da parte dei destinatari e possono risultare fonte di costi ulteriori in casi di alto *turnover* di personale.

La loro formalizzazione, al contrario, presuppone più chiare e precise responsabilità del personale nell'esecuzione delle Attività di Controllo.

In ogni caso, *policy* e procedure devono essere rese disponibili in maniera tempestiva al personale, cui deve essere ribadito il dovere di rispettarle con sistematicità e diligenza.

Il Principio si compone di 6 punti di attenzione che definiscono più in dettaglio l'ambito e le modalità di applicazione.

3.1. Punto di attenzione – Sviluppo di *policy* e procedure per l'implementazione delle direttive del *management*

I comportamenti del personale dovrebbero essere indirizzati da apposite linee guida.

Le correlate procedure attuative possono essere documentate in differenti formati, quali note descrittive, diagrammi di flusso, matrici dei rischi e dei controlli *(risks & controls matrix*).

Al fine di assicurare che le direttive del *management* siano attuate in maniera appropriata e coerente, le *policy* e le procedure dovrebbero prevedere, di norma, la regolamentazione dei

seguenti aspetti:

- finalità della loro redazione, inclusi i rischi da indirizzare,
- ambito di applicazione (operazioni, *business unit*, ecc.),
- responsabilità di emissione e aggiornamento,
- comportamenti da osservare e da evitare,
- controlli da attuare in relazione alle attività da svolgere, indicandone le responsabilità, nonché le modalità di svolgimento e documentazione,
- azioni correttive da mettere in atto e procedure di *escalation* nello svolgimento delle Attività di Controllo in caso di eccezioni,
- rimando tra *policy* e procedure attuative,
- competenze/conoscenze eventualmente richieste per lo svolgimento delle attività,
- tempistiche di entrata in vigore,
- data di emissione.

3.2. Punto di attenzione – Responsabilità nello svolgimento delle Attività di Controllo

È fondamentale che le responsabilità di svolgimento delle Attività di Controllo siano espressamente e univocamente identificate.

Tali responsabilità dovrebbero essere esplicitate nelle *policy* e procedure di riferimento e richiamate in maniera coerente nella documentazione relativa all'attribuzione di ruoli, compiti e responsabilità (funzionigrammi, mansionari, *job description*).

3.3. Punto di attenzione – Tempestività delle Attività di Controllo

Le procedure dovrebbero esplicitare le tempistiche entro cui le Attività di Controllo ed eventuali azioni correttive devono essere effettuate. La mancanza di tale previsione può ridurre significativamente l'utilità dell'Attività di Controllo.

Ad esempio, una *review* periodica delle utenze e degli accessi è efficace se viene eseguita in maniera tempestiva per evitare rischi di accessi non autorizzati.

3.4. Punto di attenzione – Messa in atto di azioni correttive

Nel condurre un'Attività di Controllo, è necessario identificare i casi per cui effettuare *follow-up* e prevedere le correlate azioni correttive da attuare.

E' il caso ad esempio di una riconciliazione di cassa in cui si rilevi una discrepanza in uno dei conti: chi esegue le riconciliazioni dovrà individuare quali operazioni non siano state registrate correttamente e da parte di chi, fornendo istruzioni per le correlate azioni correttive.

3.5. Punto di attenzione – Impiego di personale competente

Un'Attività di Controllo adeguata generalmente non può prescindere dal fatto di essere condotta con diligenza da personale competente, con un livello di *seniority* adeguato per il suo svolgimento. Il livello di competenza richiesto dipende da diversi fattori, quali la complessità del controllo da eseguire e il volume delle operazioni sottostanti.

Nello svolgimento delle Attività di Controllo è pertanto importante:

- avere piena consapevolezza dei rischi da prevenire,

- avere conoscenze adeguate per comprendere gli effetti derivanti da eventuali non conformità,
- avere autorità adeguata per intraprendere eventuali azioni correttive necessarie.

3.6. Punto di attenzione – *Review* di *policy* e procedure

L'organizzazione dovrebbe regolarmente e periodicamente rivedere le proprie *policy* e procedure e le correlate Attività di Controllo per garantirne la continua efficacia.

In particolare, nell'ambito dei processi di identificazione e valutazione dei rischi, dovrebbero essere adeguatamente valutate le implicazioni correlate ad eventuali cambiamenti significativi.

I cambiamenti inerenti il personale, i processi e/o la tecnologia potrebbero infatti ridurre significativamente l'efficacia dei controlli, renderli ridondanti o obsoleti. Quando si verificano tali cambiamenti, dovrebbe essere sempre valutata l'adeguatezza dei controlli al fine di individuare eventuali azioni correttive. Ad esempio, l'aggiornamento di un modulo di un sistema informativo aziendale (es. ERP) che preveda l'introduzione di alcuni controlli automatici potrebbe rendere obsoleti gli eventuali controlli manuali previsti.

3.7. Strumenti applicativi

Si riportano di seguito, a titolo esemplificativo e non esaustivo, alcuni elementi di concreta attuazione dei punti di attenzione del principio in esame:

- **Identificazione, valutazione e documentazione dei controlli relativi ai rischi aziendali rilevanti**;
- ***Corpus* procedurale** (politiche, linee guida e procedure), con identificazione:
  - dei principi di comportamento da osservare;
  - delle attività e dei controlli da porre in essere, delle relative responsabilità (comprendendo sia le funzioni operative sia le funzioni di controllo), tempistiche, modalità operative, documentazione;
- **Funzionigrammi, mansionari e *job description***, con indicazione delle responsabilità assegnate (coerenti con quanto indicato nelle *policy* e nelle procedure aziendali di riferimento);
- ***Check list* e standard di controllo**;
- **Verifiche periodiche del disegno dei controlli**;
- ***Gap Analysis* e piani di attuazione delle azioni correttive**, con identificazione di responsabilità, contenuti e tempistiche.

CAPITOLO IV

INFORMAZIONI E COMUNICAZIONE (*INFORMATION & COMMUNICATION*)

1. Principio n. 13 – L'organizzazione ottiene o genera e utilizza informazioni rilevanti e di qualità a supporto del funzionamento del Sistema di controllo interno e di gestione dei rischi - 2. Principio n. 14 – L'organizzazione comunica internamente le informazioni, compresi gli obiettivi e le responsabilità di controllo interno, necessarie a supportare il funzionamento del Sistema di controllo interno e di gestione dei rischi nel suo complesso - 3. Principio n. 15 - L'organizzazione comunica con parti terze relativamente a questioni che interessano il funzionamento del Sistema di controllo interno e di gestione dei rischi

***

Il Sistema di controllo interno e di gestione dei rischi è costituito da informazioni.

Le modalità di gestione, condivisione e comunicazione delle stesse sono pertanto aspetti cruciali per l'organizzazione.

Tale componente del SCIGR è costituita da due macro-elementi, strettamente interconnessi: le informazioni e la comunicazione aziendale.

Con il termine "Informazioni" si fa riferimento agli elementi che il *management* deve ottenere, generare sia da fonti interne che esterne, e utilizzare per supportare il funzionamento delle altre componenti del SCIGR. La criticità riguardante le informazioni che costituiscono il SCIGR, o che gravitano attorno allo stesso, è quella di identificare quali siano rilevanti e adeguate per il funzionamento e il raggiungimento degli obiettivi del SCIGR, all'interno del più ampio sistema informativo aziendale. È inoltre necessario che tali informazioni siano affidabili, tempestive e accessibili.

La "Comunicazione" è invece il processo continuo e iterativo finalizzato a fornire, condividere e ottenere le informazioni necessarie al funzionamento del SCIGR. In tale contesto, la "Comunicazione Interna" è il mezzo attraverso cui le informazioni sono diffuse nelle varie direzioni dell'organizzazione aziendale, dal basso verso l'alto o con modalità *Top-Down* oppure orizzontalmente (all'interno dei processi o tra diverse funzioni e divisioni).

Il COSO identifica 3 principi che dovrebbero essere sempre rispettati per il corretto disegno dell'Informazione e Comunicazione. Affinché le stesse siano costruite in maniera efficace e contribuiscano in maniera ottimale al raggiungimento degli obiettivi aziendali, è utile che tali Principi siano riflessi in modalità operative che tengano conto dei correlati 14 elementi di attenzione, come di seguito approfondito.

1. Principio n. 13 – L'organizzazione ottiene o genera e utilizza informazioni rilevanti e di qualità a supporto del funzionamento del Sistema di controllo interno e di gestione dei rischi

L'efficacia delle Attività di Controllo è strettamente correlata all'affidabilità e alla tempestività delle informazioni necessarie al raggiungimento degli obiettivi di controllo (*report*, analisi, approvazioni, riconciliazioni, ecc.).

Il Principio si compone di 5 punti di attenzione che definiscono più in dettaglio l'ambito e le modalità di applicazione.

1.1. Punto di attenzione – Identificare il fabbisogno informativo

Il "punto di attenzione" riguarda il tipo di informazioni da ottenere per un corretto funzionamento del SCIGR.

L'identificazione di misure finalizzate a garantire informazioni coerenti con le aspettative degli attori coinvolti nel SCIGR e necessarie per il funzionamento delle altre componenti è un'importante sfida per il *management*.

Il fabbisogno informativo è condizionato:

- dalle fonti che è necessario consultare per reperire le informazioni: l'identificazione delle fonti da cui è possibile acquisire le informazioni necessarie per l'operatività del SCIGR è un fattore determinante per il suo adeguato funzionamento man mano che si procede nel flusso logico dell'implementazione del SCIGR;
- dal formato delle informazioni: l'informazione può essere trasferita in forma di *report*, moduli, comunicazioni, dati utilizzati nelle analisi e diagrammi che consentano di fornire una visione complessiva del rischio, dell'Attività di Controllo o del *test*;
- dal livello di dettaglio delle informazioni: in linea generale, man mano che si procede nel flusso logico dell'implementazione dello SCIGR, il livello di dettaglio delle informazioni da identificarsi come "adeguato" diventa sempre maggiore (nella definizione dell'Ambiente di Controllo sono necessarie informazioni di alto livello, mentre il livello di dettaglio appropriato è maggiore per il *Risk Assessment* e aumenta ulteriormente nell'esecuzione delle Attività di Controllo e di monitoraggio, si vedano in proposito i capitoli precedenti).

Una soluzione per gestire con adeguata efficacia l'identificazione delle fonti informative è quella di definire una mappa delle stesse in relazione alle diverse componenti dello SCIGR, categorie di obiettivi e livelli organizzativi del ERM.

1.2. Punto di attenzione – Acquisire fonti di dati interni ed esterni

Il punto di attenzione sottolinea l'importanza di un'appropriata identificazione delle informazioni da acquisire per il buon funzionamento del SCIGR.

Ogni fonte di dati può fornire informazioni (quantitative o qualitative). Le criticità possono quindi essere legate all'identificazione di informazioni rilevanti ed adeguate in riferimento agli obiettivi del SCIGR, piuttosto che all'acquisizione di dati.

Esempi di fonti di dati che possono incidere sul SCIGR sono:

- Partner commerciali: condivisione di rischi e Attività di Controllo;
- Organismi Pubblici: provvedimenti, norme, regolamenti e linee guida;
- Clienti: manifestazione di esigenze relative a prodotti e servizi differenti da quelli commercializzati dalla Società, reclami, resi;
- Concorrenti: lancio di nuovi prodotti o di nuove strategie commerciali, acquisizione di altri *competitor*;
- Funzione legale: esposizione al rischio di contenzioso;
- Funzione *Compliance*: aggiornamenti derivanti da norme e regolamenti;
- *Data provider* esterni: dati relativi al *sentiment* degli *stakeholder* (es. clienti) desumibili dai *social network*.

I primi 4 punti dell'elenco rappresentano fonti informative comuni per tutte le società, a prescindere dalla loro dimensione, mentre le organizzazioni che non dispongono di una funzione legale o di una funzione *Compliance* potranno ricorrere al supporto di professionisti esterni.

Quanto più ci si sposta verso il basso nell'organizzazione, e ancora di più quando le fonti informative sono esterne, tanto più importante è la verifica preventiva della disponibilità delle informazioni presso una determinata fonte. In considerazione di tale *driver* è fondamentale muoversi con tanto più anticipo per l'ottenimento dei dati da una determinata fonte, quanto più complesso è il processo di acquisizione degli stessi e quanto più critiche sono le informazioni rispetto agli obiettivi di controllo.

1.3. Punto di attenzione – Elaborare i dati rilevanti al fine di generare informazioni

L'elaborazione di un'informativa riguarda l'individuazione dell'informativa rilevante che rappresenta un'attività cardine per il SCIGR.

Se correttamente analizzati e valutati, i dati del sistema informativo aziendale possono avere finalità plurime. Le informazioni economico-finanziarie, ad esempio, sono utilizzate sia per redigere il bilancio che per attivare decisioni operative per il monitoraggio delle *performance* e l'allocazione delle risorse. Parimenti, le informazioni riguardanti le attività operative sono fondamentali per l'elaborazione dei bilanci e dell'informativa economico-finanziaria.

In particolare, i dati riguardanti l'attività operativa (acquisti, vendite, trasporti, prezzi e modalità di lancio di prodotti e servizi, ecc.) devono essere elaborati per ottenere informazioni adeguate all'identificazione e mitigazione dei rischi, nonché allo svolgimento e al monitoraggio delle Attività di Controllo.

Il processo che, dall'acquisizione del dato, consente di formalizzare e trasferire un'informazione prevede i seguenti *step*:

a) reperire i dati;

b) raccogliere e organizzare i dati;

c) elaborare i dati;

d) analizzare e strutturare i dati;

e) predisporre il *report*/relazione o determinare gli indici di sintesi.

1.4. Punto di attenzione – Mantenere un adeguato livello di qualità durante l'elaborazione delle informazioni

Il punto di attenzione richiama l'importanza del mantenimento di un adeguato livello di qualità delle informazioni.

Affinché ciò avvenga, durante l'elaborazione delle informazioni l'organizzazione dovrebbe implementare un sistema informativo in grado di produrre e rendere disponibili informazioni:

- Tempestive e Aggiornate: i dati dovrebbero essere generati da fonti correnti e con la frequenza necessaria per un adeguato monitoraggio dei rischi;
- Accurate: il sistema informativo dovrebbe includere controlli di validità che attestano l'accuratezza e completezza dei dati, prevedendo azioni correttive in caso di anomalie o eccezioni;
- Complete: dovrebbero essere presenti informazioni sufficienti ad un adeguato livello di dettaglio. I dati non rilevanti dovrebbero essere eliminati per evitare inefficienze, utilizzi impropri di informazioni e errate interpretazioni;

- Accessibili: l'informazione dovrebbe essere facile da ottenere da coloro che ne hanno necessità. Gli utenti dovrebbero conoscere quali informazioni sono disponibili e dove sono collocate all'interno del Sistema informativo;
- Protette: l'accesso ad informazioni strategiche o confidenziali dovrebbe essere limitato a personale autorizzato. La classificazione dei dati (es. confidenziale/riservato) dovrebbe supportare la protezione delle informazioni maggiormente critiche;
- Valide: le informazioni dovrebbero essere ottenute da fonti autorizzate, raccolte nel rispetto di procedure predefinite e rappresentare eventi correnti;
- Verificabili: le informazioni dovrebbero essere supportate da evidenze sulla fonte di provenienza. Il *management* dovrebbe definire *policy* di gestione delle informazioni, che prevedano specifiche responsabilità in merito alla qualità delle informazioni;
- Adeguatamente archiviate e conservate: le informazioni dovrebbero essere disponibili per un periodo adeguatamente esteso per supportare eventuali verifiche e ispezioni da parte di Funzioni deputate a controlli di terzo livello o terze parti.

La progettazione di un'architettura dei sistemi informativi e l'acquisizione di tecnologie che consentano l'integrazione dei *database*, la tracciabilità delle modifiche e la protezione di dati e informazioni dovrebbero essere aspetti rilevanti della strategia aziendale.

Inoltre, la condivisione di procedure e regole comuni con gli *stakeholder* che abbiano l'obiettivo di mantenere elevati *standard* di qualità delle informazioni consente di ottenere elevati livelli qualitativi dei dati in entrata e delle informazioni elaborate da soggetti terzi.

1.5. Punto di attenzione – Considerare i costi e benefici

Un'informativa dettagliata e rilevante dovrebbe sempre tenere in considerazione il *trade-off* costi e benefici.

Di seguito si riportano le implicazioni correlate a scelte da effettuare per disporre di un patrimonio informativo adeguato:

Adozione di soluzioni manuali:

- Vantaggi: nessun costo di implementazione, flessibilità dei controlli, assenza di vincoli tecnologici.
- Svantaggi: rischio di errori manuali, inefficienze legati ai tempi di archiviazione e alla predisposizione di *report*, costo in caso di produzione di documenti cartacei.

Utilizzo di *database* interni:

- Vantaggi: flessibilità delle informazioni, nessun vincolo di servizio, verificabilità dello specifico autore.
- Svantaggi: costi legati ai tempi di produzione delle informazioni, difficoltà di reperimento delle fonti.

Accentramento delle informazioni:

- Vantaggi: chiara identificazione dell'*owner* di dati/informazioni e/o del referente a cui richiederle, possibilità di analizzare i dati in modo aggregato, maggiore specializzazione.
- Svantaggi: tempi connessi alla richiesta/invio di documenti e informazioni, rischi di *business continuity* in assenza delle risorse.

Adozione di soluzioni automatizzate:

- Vantaggi: riduzione dei tempi di elaborazione, tracciabilità delle modifiche, archiviazione automatica, flussi approvativi e meccanismi SoD configurabili, riduzione del margine di errore.

- Svantaggi: costi e tempi di implementazione, rischi di *business continuity* in caso di interruzione del servizio, resistenze al cambiamento.

Utilizzo di *database* esterni:

- Vantaggi: informazioni disponibili in tempi rapidi, maggiore oggettività del dato, maggiore specializzazione del personale che ha elaborato l'informazione.
- Svantaggi: difficoltà nell'identificazione della fonte originaria, vincoli e costi legati al servizio, mancata esclusività dell'informazione.

Cloud solution:

- Vantaggi: possibilità di reperire il dato ovunque, facilità di *knowledge sharing*, eliminazione dei tempi connessi alla richiesta/consegna dei documenti.
- Svantaggi**:** investimenti per lo sviluppo di una cultura alla condivisione delle informazioni (*change management*), possibile difficoltà di identificare la collocazione dell'informazione, maggiori varchi esposti a rischi di accesso esterno.

1.6. Strumenti applicativi

Si riportano di seguito, a titolo esemplificativo e non esaustivo, alcuni tra i principali elementi di concreta attuazione dei punti di attenzione del principio in esame:

- **Sistemi contabili e gestionali** (in alcune aziende integrati nei cosiddetti sistemi ERP) da cui utilizzare i dati generati dai processi aziendali a supporto delle attività di *assessment* e monitoraggio dei controlli interni;
- **Sistemi di *business intelligence*** (cosiddetti sistemi di BI) da cui utilizzare indicatori sintetici (kpi, kpri, kci, ecc) a supporto delle attività di *assessment* e monitoraggio dei controlli interni;
- ***Software* per la raccolta delle informazioni** (*customer relationship management* o CRM, *customer service management* o CSM, i *software* adottati per il monitoraggio degli impianti, dei macchinari, dei mezzi di trasporto e del magazzino);
- **Applicativi per la gestione del SCIGR** (cosiddetti *governance, risk & compliance tool* o GRC tool), per la mappatura dei processi, il *Risk Assessment,* l'esecuzione dei test e l'acquisizione dei dati e della documentazione di supporto.
- **Sistema di segnalazione delle violazioni (*whistleblowing*)**, che definisca i canali specifici, indipendenti e autonomi messi a disposizione del segnalante per la denuncia di presunte anomalie o violazioni delle procedure aziendali o della normativa effettuate da dipendenti, membri degli organi sociali o terzi;
- **Funzione *Investor Relations***, per comunicare efficacemente e in modo strutturato con gli investitori e gli analisti finanziari proteggendo al tempo stesso le informazioni riservate e *price sensitive*;
- **Sezioni dedicate dei siti *web*** quali, ad esempio, quella sulla *Corporate Governance* nella quale vengono rese disponibili molte informazioni relative anche al SCIGR;
- **Partecipazione delle funzioni di controllo ai *management meeting* ed ai comitati di direzione**;
- ***Reporting* alle funzioni di controllo** sull'andamento aziendale e sui dati di periodo (ad es. *report* sulla produzione, sulla qualità e sul personale);
- ***Data Analytics*** su base dati interni ed esterni finalizzati a calcolare indicatori di rischi e di controllo nonché di acquisire informazioni utili al processo decisionale;
- **Scambio di informazioni tra le funzioni di controllo** (secondo e terzo livello) al fine di assicurare maggiore efficienza nelle Attività di Monitoraggio e al tempo stesso una più ampia copertura dei rischi (*risk coverage*).

2. Principio n. 14 – L'organizzazione comunica internamente le informazioni, compresi gli obiettivi e le responsabilità di controllo interno, necessarie a supportare il funzionamento del Sistema di controllo interno e di gestione dei rischi nel suo complesso

Il Principio 14 prevede che l'organizzazione comunichi internamente le informazioni, inclusi gli obiettivi e le responsabilità del controllo interno, necessarie per supportarne il funzionamento.

Il processo di comunicazione delle informazioni rilevanti per il SCIGR deve produrre il risultato di "attivare" il personale incaricato di svolgere le Attività di Controllo, trasmettendo ad ognuno le specifiche responsabilità.

Il Principio si compone di 4 punti di attenzione che definiscono più in dettaglio l'ambito e le modalità di applicazione.

2.1. Punto di attenzione – Comunicare le informazioni del Controllo Interno

Il punto di attenzione riguarda la scelta delle informazioni da comunicare all'organizzazione per il buon funzionamento del SCIGR.

La Società dovrebbe infatti implementare un processo finalizzato a comunicare con efficacia e tempestività le informazioni necessarie per consentire al personale di comprendere e svolgere le loro responsabilità in riferimento al SCIGR.

Ogni componente del SCIGR fornisce un *set* di informazioni alle altre componenti:

1) Attraverso la definizione dell'Ambiente di Controllo (v. *supra* cap. I) si comunicano all'organizzazione:
   - la cultura della gestione del rischio (principi etici, *sustainability*, ecc.);
   - le linee guida aziendali;
   - l'impegno inerente il SCIGR;
   - le indicazioni sulla struttura organizzativa, con particolare riferimento ai limiti autorizzativi e le responsabilità;
   - le misure di *performance* e il sistema incentivante.
2) Attraverso il *Risk Assessment* (v. supra cap. II) si comunicano all'organizzazione:
   - il catalogo dei rischi;
   - gli obiettivi del SCIGR;
   - la valutazione del rischio, inerente e residuo;
   - la valutazione del Sistema di Controllo esistente (AS-IS) e le sue necessità di adeguamento.
3) Attraverso l'Ambiente di Controllo e il *Risk Assessment* si definiscono la propensione e la tolleranza al rischio.
4) Attraverso le Attività di Controllo e monitoraggio si comunicano (v. *supra* cap. III) all'organizzazione:
   - le misure/i presidi da adottare;
   - i risultati delle attività di verifica inerenti il SCIGR;
   - gli indicatori di performance;
   - la Reportistica aziendale.

2.2. Punto di attenzione – Comunicare con il Consiglio di Amministrazione

Il punto di attenzione sottolinea l'importanza della comunicazione con il *management* e il Consiglio di Amministrazione.

E' necessario che sia implementato un flusso comunicativo tra il *management* e il Consiglio di Amministrazione affinché quest'ultimo disponga delle informazioni necessarie per svolgere il proprio ruolo.

Il *management* deve essere adeguatamente informato dei rischi a cui la Società è sottoposta e delle azioni di rimedio implementate attraverso documenti di sintesi (*Risk Assessment, gap analysis*, stato delle azioni di rimedio, indicatori di sintesi).

Gli obiettivi del SCIGR e i ruoli a cui attribuirne le responsabilità possono variare notevolmente a seconda della dimensione e della complessità organizzativa, dei mercati a cui è esposta la Società e dal ciclo di vita della stessa.

2.3. Punto di attenzione – Definire linee di comunicazione separate

Il punto di attenzione sottolinea la necessità di separare le linee informative per il corretto funzionamento del SCIGR.

Al fine di garantire l'efficacia del SCIGR è necessario che le informazioni rilevanti siano diffuse a tutti i livelli dell'organizzazione, in modo che ognuno possa identificare, valutare e rispondere ai rischi.

E' opportuno che l'organizzazione implementi flussi di comunicazione separati (es. canale di *whistleblowing* o comunicazioni all'organismo di vigilanza), che fungano da meccanismi di sicurezza per attivare comunicazioni anonime o confidenziali quando i normali canali di comunicazione siano non operativi o inefficaci.

Per ottenere un elevato livello di efficacia del SCIGR è necessario provvedere a comunicazioni che agiscono a differenti livelli nell'organizzazione:

- *Entity Level* - Flussi informativi destinati al Consiglio di Amministrazione/Amministratore Delegato: comunicazioni periodiche sugli obiettivi di *Risk Management*, Relazione sulla *Corporate Governance*;
- *Division* – Flussi informativi destinati al *Senior Management*: comunicazioni dei KRI (*Risk Key Indicator*), comunicazioni sui Modelli di Organizzazione, Gestione e Controllo e sulle *policy*, comunicazioni sulle tempistiche di funzionamento del Sistema di Controllo, variazioni dell'*Internal Control Handbook*;
- *Operation Unit* – Flussi informativi rivolti a Responsabili di Funzione: comunicazioni inerenti i Piani di Lavoro, *Risk Control Matrix*, Procedure, variazioni dei *Risk Assessment*;
- *Function* - Flussi informativi provenienti da, o rivolto a, ciascun membro dell'organizzazione: comunicazione dei risultati dei test/controlli svolti, segnalazione di eventuali anomalie.

2.4. Punto di attenzione – Selezionare metodi di comunicazione adeguati

La selezione dei metodi di comunicazione maggiormente rilevanti è fondamentale per il corretto funzionamento del SCIGR.

La Società identifica i metodi di comunicazione maggiormente efficaci in considerazione delle tempistiche, dei destinatari dell'*audience* e della natura delle informazioni.

L'invio di email che definiscono chiaramente le tempistiche di svolgimento delle attività previste dal SCIGR sono certamente un elemento essenziale per il suo funzionamento.

Tuttavia, sempre più spesso le società si dotano di soluzioni automatizzate e canali specifici per trasferire le informazioni.

2.5. Strumenti applicativi

Si riportano di seguito, a titolo esemplificativo e non esaustivo, alcuni tra i principali elementi di concreta attuazione dei punti di attenzione del principio in esame:

- **Relazione periodica dell'Organismo di Vigilanza** al CdA e l'informativa su fatti ed eventi specifici di particolare rilevanza;
- **Comunicazione dell'amministratore indipendente** al CdA sulla perdita dei requisiti di indipendenza;
- **Indicazioni del Comitato Controllo e Rischi**, in virtù delle proprie funzioni consultive e propositive, e la relazione semestrale sull'adeguatezza del Sistema di controllo interno e di gestione dei rischi;
- **Relazione annuale del Collegio Sindacale** su tutti gli aspetti di vigilanza previsti dalla legge, tra cui l'indipendenza della Società di revisione, l'assetto organizzativo, i processi di *risk management*, l'*Internal Auditing*, l'applicazione dei principi contabili, ecc.
- **Relazioni rilasciate dal revisore** in caso di specifiche disposizioni regolamentari;
- **Relazioni e verbali sul SCIGR** predisposti dai comitati manageriali e consiliari nonché dalla funzione *Internal Audit*;
- Comunicazione sull'adozione e sul funzionamento del **Modello di Organizzazione Gestione e Controllo ex D.Lgs. 231/2001** e Codice Etico**,** modulati in base ai destinatari;
- **Comunicazione su strumenti normativi e organizzativi** quali *policy* e procedure, poteri autorizzativi, linee di dipendenza gerarchica, flussi informativi ecc.;
- **Ordini di servizio o mandati** delle funzioni preposte ad Attività di Controllo Interno;
- **Risultati del *Risk Assessment*** con l'indicazione del profilo di rischio aziendale costituito dai rischi più rilevanti;
- ***Risks & Controls Matrix,*** con la conseguente identificazione del *Process Owner*, *Control Owner* e degli incaricati delle Attività di Controllo;
- **Piano di *Internal Audit risk-based*,** per informazione/approvazione da parte del CdA (almeno annualmente);
- **Evidenze ed esiti dei test** e dei controlli svolti da parte delle funzioni di controllo (es. *Internal Audit*, *compliance*, ecc.);
- ***Report* dell'*Internal Audit*** quali ad esempio verbali degli interventi effettuati, *action plan*, *follow-up* sul completamento delle azioni del *management*, ecc..

3. Principio n. 15 – L'organizzazione comunica con parti terze relativamente a questioni che interessano il funzionamento del Sistema di controllo interno e di gestione dei rischi

Il Principio 15 prevede che l'organizzazione comunichi con soggetti esterni in merito al funzionamento del SCIGR.

L'obiettivo della Comunicazione esterna deve essere quello di attivare le "comunicazioni in entrata" necessarie per valutare il rischio, condurre le Attività di Controllo e monitorare sia i rischi, che i controlli.

Inoltre, la Comunicazione esterna deve provvedere a fornire ai soggetti esterni le

informazioni sul SCIGR in applicazione di requisiti normativi o regolamentari anche al fine di rispondere alle aspettative degli *stakeholder*.

Il Principio si compone di 5 punti di attenzione che definiscono più in dettaglio l'ambito e le modalità di applicazione.

3.1. Punto di attenzione – Comunicare le informazioni del Controllo Interno

Il punto di attenzione enfatizza l'importanza di implementare un processo finalizzato a comunicare tempestivamente informazioni rilevanti ai soggetti terzi, inclusi gli azionisti o le controllanti, i *partner* commerciali, le Autorità, gli analisti finanziari e ogni ulteriore parte terza verso cui la Società è tenuta a trasmettere le informazioni riguardanti il SCIGR (per motivi normativi o regolamentari) o ritiene strategicamente di diffondere determinate informazioni sul Sistema di Controllo.

In ogni caso, le comunicazioni da effettuare nei confronti di soggetti esterni (in particolare in riferimento ai rischi di *compliance*) sono quanto meno considerevoli.

A tal fine, un ruolo fondamentale lo riveste la funzione *compliance* che è tenuta a svolgere un continuo aggiornamento (*scouting*) normativo per verificare eventuali nuove comunicazioni da effettuare nei confronti delle autorità, nonché eventuali variazioni nelle modalità di tali comunicazioni.

Una soluzione auspicabile è la mappatura degli obblighi normativi e della relativa autorità di riferimento.

3.2. Punto di attenzione – Attivare le comunicazioni in entrata

E' importante che la Società implementi canali di comunicazione "aperti" che consentano a clienti, fornitori, *auditor*, Autorità, analisti finanziari e altri soggetti terzi di fornire al *management* e al Consiglio di Amministrazione le informazioni rilevanti per il corretto funzionamento del SCIGR.

Ne sono esempi:

- linee apposite per i reclami;
- linee apposite per le segnalazioni di non conformità da parte dei fornitori;
- la comunicazione di *hotline* di *whistleblowing* per i tentativi di frode o comportamenti inappropriati.

3.3. Punto di attenzione – Comunicare con il Consiglio di Amministrazione

E' fondamentale che sia implementato un flusso comunicativo tra il *management* e il Consiglio di Amministrazione al fine che quest'ultimo disponga tempestivamente delle informazioni risultanti da *Assessment* e *Audit* condotte da soggetti esterni.

3.4. Punto di attenzione - Definire linee di comunicazione separate

E' auspicabile che la Società implementi flussi di comunicazione separati (es. canale di *whistleblowing*), che fungano da meccanismi di sicurezza per attivare comunicazioni anonime o confidenziali quando i normali canali di comunicazione siano non operativi o inefficaci.

Fermi restando gli obblighi normativi, è fondamentale definire cosa è strategicamente opportuno comunicare verso l'esterno.

Le evidenze del *Risk Assessment* e delle *gap analysis* non vengono solitamente divulgate verso l'esterno, in particolare nei casi in cui un determinato rischio considerato rilevante e in

riferimento a cui è stato identificato una carenza del sistema possa essere visto come un punto di debolezza da parte di clienti, concorrenti o altri *stakeholder*.

Viceversa altri elementi del SCIGR come il codice etico, i documenti di *corporate social responsibility* e i risultati del Sistema di controllo interno e di gestione dei rischi possono essere strategicamente diffusi verso l'esterno generando un potenziale ritorno di immagine.

Il comportamento in caso di eventi di rischio (c.d. *crisis management*) comporta invece scelte particolarmente delicate, sulle modalità (e le tempistiche) con cui diffondere le informazioni. Una rapida presa di posizione verso gli *stakeholder* del *management* potrebbe essere considerata come un atteggiamento proattivo da parte della Società, ma di contro essere interpretato come una conferma di responsabilità.

3.5. Punto di attenzione – Selezionare metodi di comunicazione adeguati

La selezione dei metodi di comunicazione verso l'esterno è fondamentale per il corretto funzionamento del SCIGR.

In aggiunta alle tempistiche, ai destinatari, all'*audience* e alla natura delle informazioni, per ciò che concerne i metodi di comunicazione nei confronti dei soggetti terzi, la Società è tenuta a considerare eventuali specifici aspetti legali o regolatori, nonché le aspettative del soggetto terzo.

Per gestire efficacemente le tempistiche e le modalità di comunicazione verso l'esterno, una soluzione auspicabile è quella di dotarsi di scadenzari e di soluzioni automatizzate per la predisposizione dei dati da trasmettere all'esterno, attraverso il quale siano già preimpostate le categorie e il *format* delle informazioni da rilasciare.

3.6. Strumenti applicativi

Si riportano di seguito, a titolo esemplificativo e non esaustivo, alcuni tra i principali elementi di concreta attuazione dei punti di attenzione del principio in esame:

- **Relazioni finanziarie annuali e periodiche** (bilanci, relazioni infrannuali, relazioni sulla gestione, ecc.). Tali informative variano a seconda delle caratteristiche (es. società quotate) e della forma societaria.
- **Specifiche comunicazioni di settore** da trasmettere agli enti incaricati di verificare il rispetto della normativa di settore. Esempi tipici sono gli istituti bancari, assicurativi, gli intermediari finanziari e le Società farmaceutiche. Particolari comunicazioni sono inoltre previste per le società tenute al rispetto di disciplinari relativi ai prodotti commercializzati.
- **Comunicazioni di *non financial information***, ad es. Bilancio Sociale, Dichiarazione di Informazioni Non Finanziarie e/o comunicazioni su specifiche tematiche quali ad es. quelle ambientali.
- **Comunicazione di specifiche *policy*** (*market abuse*, rapporti con le parti correlate, ecc.) e dei principi etico-comportamentali attesi dai terzi (tramite presa visione del Modello 231, Codice Etico, ecc.);
- **Relazione sulla *corporate governance*** derivante dagli obblighi del TUF per gli emittenti titoli quotati in mercati regolamentati;
- **Informazioni regolamentate** comunicate al mercato ed agli investitori attraverso i canali e gli strumenti dedicati.

CAPITOLO V

ATTIVITÀ DI MONITORAGGIO (*MONITORING ACTIVITIES*)

1. Principio n. 16 – L'organizzazione definisce, sviluppa ed esegue valutazioni continuative (*ongoing*) e obiettive (*separate*) per accertare che le componenti del Sistema di controllo interno siano presenti e funzionanti - 2. Principio n. 17 – L'organizzazione valuta e comunica tempestivamente le carenze del Sistema di controllo interno ai soggetti responsabili di intraprendere le necessarie azioni correttive, incluso il *senior management* e il Consiglio di Amministrazione per quanto necessario e di competenza

***

Le Attività di Monitoraggio consistono principalmente nella verifica continuativa o periodica dell'efficacia del disegno dei controlli interni e della reale operatività degli stessi, resa necessaria dalla dinamicità del contesto nel quale il sistema dei controlli è inserito.

Se le Attività di Controllo mitigano i rischi, le Attività di Monitoraggio hanno un obiettivo più vasto e permettono di verificare che il SCIGR sia sempre in grado di operare adeguatamente, sia abbastanza flessibile da poter rispondere ai cambiamenti delle condizioni in cui opera l'azienda e sia in grado di far fronte all'emergere di nuove tematiche di rischio. Le Attività di Monitoraggio dovrebbero quindi garantire che il *management* riconsideri il disegno del SCIGR ogniqualvolta vi siano cambiamenti significativi dei rischi aziendali ed inoltre che i controlli definiti per ridurre i rischi ad un livello accettabile siano effettivamente operativi nel periodo di osservazione.

Un ulteriore punto di fondamentale importanza per quanto riguarda l'attività di *Monitoring* ricade nell'individuazione, all'interno delle compagine aziendale, dei soggetti cui affidare la gestione del processo di monitoraggio e la presentazione dei risultati emersi. Considerando che questi soggetti hanno un ruolo sostanziale nella valutazione del funzionamento del SCIGR è indispensabile che posseggano principalmente due requisiti: competenza e obiettività. La competenza si configura nella comprensione del funzionamento dei processi, dei controlli connessi e dei rischi associati, caratteristiche senza le quali non sarebbe possibile né identificare le carenze del SCIGR né gli elementi che le hanno originate. L'obiettività invece riguarda la necessità che i soggetti responsabili del processo di monitoraggio non siano interessati da tematiche di conflitto di interessi e che non si debbano preoccupare di eventuali conseguenze legate allo svolgimento delle attività loro attribuite.

Si rende, infine, necessario precisare che le Attività di Monitoraggio, così come descritte dal COSO, vanno ben al di là della semplice raccolta documentale di informazioni e della predisposizione di *dashboard* di sintesi. Affinché il monitoraggio si possa considerare adeguatamente strutturato devono essere assicurate le seguenti condizioni:

- deve consentire la verifica del funzionamento dei controlli sui principali rischi della Società;
- deve portare all'identificazione delle carenze dei controlli analizzati e alla correzione delle stesse;
- deve garantire il miglioramento nell'efficacia e nell'efficienza dei processi di controllo interno;
- deve assicurare l'effettivo funzionamento del Sistema di Controllo e di gestione dei rischi ad una determinata data o per un determinato periodo di tempo;

- deve supportare chi ne è responsabile nell'esprimere, in modo efficace ed efficiente, le proprie conclusioni circa il funzionamento del sistema dei controlli interni.

Il monitoraggio è strettamente connesso a tutte le componenti del COSO per varie ragioni.

Le Attività di Monitoraggio risentono del funzionamento di tutte le altre componenti definite all'interno del COSO: eventuali carenze in elementi quali, ad esempio, i sistemi informativi, le competenze, le responsabilità, le deleghe ed i comportamenti possono influenzare l'efficacia, l'efficienza e in generale l'andamento degli strumenti di misurazione e monitoraggio.

In secondo luogo, lo scopo delle Attività di Monitoraggio è proprio quello di verificare la presenza e il corretto funzionamento nel tempo di ognuna delle altre componenti di controllo interno definite dal COSO. In questo contesto le componenti non interagiscono direttamente con le attività di *Monitoring;* piuttosto, essendo oggetto di verifica, ne subiscono gli effetti dello svolgimento delle varie attività.

Infine, le mancanze e i malfunzionamenti eventualmente presenti nelle Attività di Monitoraggio possono compromettere l'efficacia delle altre componenti previste dal COSO; può infatti accadere che, un Sistema di controllo e di gestione dei rischi, inizialmente funzionante, diventi inefficace nel tempo per l'incapacità del processo di monitoraggio di individuare gli elementi e i segnali di criticità emergenti presenti all'interno delle varie componenti.

In base alla nuova impostazione *principle based* del COSO, tesa a favorire e facilitare la valutazione del SCIGR, la componente *Monitoring Activities* è composta da 2 principi e 10 punti di attenzione, di seguito riportati.

1. Principio n. 16 – L'organizzazione definisce, sviluppa ed esegue valutazioni continuative (*ongoing*) e obiettive (*separate*) per accertare che le componenti del controllo interno siano presenti e funzionanti

Il Principio 16 prevede che le Attività di Monitoraggio si compongano di due tipi di valutazioni: valutazioni continuative (*ongoing*) e valutazioni obiettive (*separate*), a seconda che la competenza per lo svolgimento di tali attività sia assegnata a funzioni aziendali che svolgono l'Attività di Monitoraggio all'interno o al di fuori del processo in esame e pertanto tipicamente operanti nel secondo o nel terzo livello di controllo oppure soggetti esterni alla Società. Le valutazioni *ongoing* e *separate* consentono di valutare le altre componenti del SCIGR definite dal COSO e di verificarne continuativamente il corretto funzionamento.

Il Principio si compone di 7 punti di attenzione che definiscono più in dettaglio l'ambito e le modalità di applicazione.

1.1. Punto di attenzione – *Mix* di valutazioni *ongoing* e *separate*

Il *management* prevede un insieme bilanciato di valutazioni continuative (*ongoing*) e valutazioni obiettive (*separate*). La distinzione tra queste due fattispecie è insita nel soggetto aziendale cui è affidata la responsabilità di esecuzione e nel *timing*.

Le valutazioni continue sono generalmente definite come operazioni routinarie, integrate nei processi, condotte in tempo reale e che reagiscono alle condizioni di cambiamento (interne/esterne).

Per le valutazioni *separate* è possibile utilizzare le stesse tecniche adottate per le valutazioni *ongoing*; la differenza è legata però alla periodicità delle valutazioni e alla mancata integrazione all'interno delle *operation*. Questo tipo di valutazione viene, inoltre, svolto da

funzioni che sono fuori dal processo su cui si sta svolgendo il monitoraggio in modo da assicurare obiettività di giudizio. Soggetti deputati allo svolgimento di valutazioni *separate* potrebbero essere: *Compliance Officer/HSE Manager/Finance Risk Manager/Security Manager/Credit Manager/*ecc.

La scelta del giusto *mix* di valutazioni *ongoing* e *separate* ricade su più livelli dell'organizzazione e dipende principalmente da fattori quali la portata e la natura delle operazioni della Società, il cambiamento di fattori esterni ed interni e i rischi associati alle diverse tipologie di valutazioni. Molto spesso le valutazioni *separate* vengono utilizzate al fine di confermare quanto emerso da valutazioni *ongoing*; un'organizzazione che però ricorre molto frequentemente al tipo di valutazione *separate* potrebbe dover riconsiderare la validità dei suoi controlli *ongoing*.

1.2. Punto di attenzione – Frequenza di cambiamento

Il *management*, nella scelta del giusto *mix* di valutazioni, deve sempre tener conto delle variazioni che coinvolgono l'organizzazione stessa o il suo settore/contesto di riferimento.

Questo interessa il monitoraggio da due punti di vista: da un lato si riscontra la necessità di adattare il *mix* di valutazioni in base ai cambiamenti che possono intercorrere, dall'altro il monitoraggio ha un ruolo di primaria importanza nella comprensione della *baseline* dell'organizzazione (si veda par. 1.3) in quanto permette di evidenziare eventuali fattori di cambiamento dell'organizzazione, come anche del settore e del contesto di riferimento che, in assenza di monitoraggio, non sarebbe possibile individuare.

1.3. Punto di attenzione – Comprensione della struttura (o *baseline*)

La comprensione del funzionamento di un SCIGR è un passo imprescindibile per la scelta di quali Attività di Monitoraggio implementare.

La *baseline* è costituita dall'insieme dei controlli interni individuati nelle 5 componenti definite nel COSO. La sua comprensione è pertanto legata a tutte le componenti e varia al variare di ognuna di queste. Si rende quindi necessario aggiornare costantemente le Attività di Monitoraggio in seguito ad una modifica avvenuta su una delle altre componenti dei controlli interni.

Questo punto è strettamente connesso con il precedente punto di attenzione par. 1.2: il continuo monitoraggio dei cambiamenti permette di avere sempre una visione chiara della *baseline* dei controlli interni, elemento determinante nella scelta del giusto *mix* di valutazioni *separate/ongoing*.

1.4. Punto di attenzione – Utilizzo di personale competente

Per assicurarsi che il processo implementato fornisca una garanzia ragionevole del raggiungimento degli obiettivi prefissati dal *management*, chi effettua le valutazioni conduce un'analisi partendo dagli standard che il *management* ha definito per ogni singola componente del COSO. Benché lo stesso discorso valga anche per le valutazioni *ongoing*, si consideri che le valutazioni *separate* vengono svolte periodicamente da *manager* e altro personale obiettivo ed esterno rispetto al processo in esame, revisori esterni e *Internal Auditors*, e che è sempre necessario che questi soggetti abbiano una conoscenza del funzionamento dei processi aziendali, del sistema di monitoraggio, delle attività oggetto di valutazione nonché altre conoscenze specifiche legate al *business*.

1.5. Punto di attenzione – Integrazione con i processi di *business*

La valutazione *ongoing* è integrata e viene svolta all'interno delle funzioni e dei processi

aziendali e necessita di essere modificata di pari passo con i cambiamenti che intercorrono nei processi.

La valutazione *separate*, di contro, è esterna alle funzioni monitorate, obiettiva nel giudizio e permette di ottenere una ulteriore garanzia dell'esistenza e del corretto funzionamento del SCIGR.

Per quanto riguarda proprio le valutazioni *separate* è possibile garantire diversi gradi d'indipendenza del ruolo di monitoraggio.

1.6. Punto di attenzione – Frequenza e ambito

Il *management* modifica la portata e la frequenza delle valutazioni *separate* sulla base dei rischi. La frequenza e la portata dipendono da diversi elementi: significatività del rischio, risultati delle valutazioni *ongoing* e impatto atteso sulle componenti dei controlli nella gestione dei rischi stessi. Un rischio con una priorità maggiore, determinata dalla probabilità di accadimento o dal suo impatto, necessita di un approfondimento maggiore rispetto ad un rischio con bassa priorità. Per rischi con alta priorità si possono utilizzare entrambe le tipologie di valutazione in quanto la valutazione *separate* può fornire un *feedback* rispetto ai risultati della valutazione *ongoing*.

1.7. Punto di attenzione – Valutazione obiettiva

La presenza di un certo numero di valutazioni *separate* è opportuna al fine di fornire un *feedback* obiettivo ovvero autonomo nel giudizio e depurato dal rischio di *self-review* sul funzionamento del Sistema di controllo interno e di gestione dei rischi.

L'obiettività e l'autonomia di giudizio richiesta dal Principio 16 del COSO può essere fornita attraverso: le valutazioni condotte dall'*Internal Audit*, altre valutazioni obiettive (*compliance officer*, *risk specialist*, consulenti esterni), le valutazioni di *benchmarking/peer*, le valutazioni funzionali o di *cross operating unit* e il *self-assessment* (in questo caso saranno i soggetti destinatari del *report* a valutare l'affidabilità da porre sui risultati in considerazione delle limitazioni all'obiettività).

1.8. Strumenti applicativi

Si riportano di seguito, a titolo esemplificativo e non esaustivo, alcuni tra i principali elementi di concreta attuazione dei punti di attenzione del principio in esame:

- **Risk Assessment** del Chief Risk Officer per la definizione del Corporate Risk Profile (separate evaluation);
- ***Business Review*** del Controllo di Gestione che analizzino gli scostamenti dei risultati consuntivi e dei *forecast* rispetto al budget (*separate evaluation*);
- Svolgimento di attività di *Audit* previste nel **Piano di *Internal Audit Risk Based*** (*separate evaluation*);
- **Attività di *benchmarking*** di processi o controlli rispetto a quelli di altre Società comparabili (*separate evaluation*);
- ***Quality Assurance Review*** delle attività di *Internal Audit* per verificare che siano organizzate e vengano svolte secondo gli standard professionali *dell'Institute of Internal Auditors*;
- **Certificazione ISO** per il sistema di gestione della qualità, ambientale, salute e sicurezza, anti-corruzione, ecc.;
- **Controllo qualità** delle materie prime e dei prodotti finiti svolti dalla Funzione Controllo Qualità;

- **Conta fisica delle scorte di magazzino** effettuata dalla Logistica per verificare l'allineamento dei saldi contabili con le rimanenze fisiche (*on-going evaluation*);
- **Verifica delle riconciliazioni bancarie** svolta dalla Funzione Tesoreria per verificare l'allineamento tra i saldi contabili e la cassa (*on-going evaluation*);
- **Controlli di produzione** da parte delle Funzioni di Produzione per verificare la qualità dei lotti di produzione (*on-going evaluation*);
- **Conta fisica in fase di ricevimento merci** da parte del magazzino per verificare la congruità dei prodotti rispetto ai documenti di trasporto e agli ordini di acquisto (*on-going evaluation*);
- **Verifica dell'*ageing* del credito** da parte della Funzione Amministrazione per sollecitare l'incasso delle partite insolute (*on-going evaluation*);
- **Verifica delle giacenze di magazzino** (*slow moving*) da parte della Funzione Logistica per avviare iniziative di vendita dei prodotti obsoleti (*on-going evaluation*);
- **Verifica degli accessi fisici** da parte della Funzione Security ai locali aziendali (*on-going evaluation).*

2. Principio n. 17 – L'organizzazione valuta e comunica tempestivamente le carenze del Sistema di controllo interno ai soggetti responsabili di intraprendere le necessarie azioni correttive, incluso il *senior management* e il Consiglio di Amministrazione per quanto necessario e di competenza

Il Principio 17 evidenzia che eventuali carenze riscontrate nella valutazione della presenza, funzionamento e operatività integrata del Sistema di controllo, andranno comunicate ai soggetti responsabili affinché vengano implementate determinate azioni correttive. Qualora durante il monitoraggio si riscontrino gravi carenze del SCIGR (esistenza di componenti con inadeguato funzionamento piuttosto che totale assenza delle componenti stesse), queste saranno comunicate al *management* e al Consiglio di Amministrazione. La valutazione delle carenze riscontrate deve sempre tener conto dei criteri stabiliti internamente, per esempio dal *management* e dal Consiglio di Amministrazione ed esternamente, per esempio dagli enti preposti all'emanazione di standard nazionali/internazionali.

Attività imprescindibile e immediatamente successiva a quella appena indicata è la previsione delle azioni correttive in grado di porre rimedio alle problematiche emerse. Tale attività si sostanzia principalmente nelle seguenti fasi: valutazione e *reporting* delle carenze, monitoraggio delle azioni correttive e sviluppo delle linee guida per il *reporting*.

Il Principio si compone di 3 punti di attenzione che definiscono più in dettaglio l'ambito e le modalità di applicazione.

2.1. Punto di attenzione – Valutazione dei risultati

La valutazione dei risultati *ongoing e separate evaluation* spetta al *management* e al Consiglio di Amministrazione. Per valutare se quanto riscontrato rappresenti o meno una minaccia potenziale/reale al raggiungimento degli obiettivi aziendali serve una metodologia definita in anticipo per la corretta valutazione delle carenze riscontrate. L'esame dei risultati delle valutazioni può avvenire secondo logiche quali-quantitative in un'ottica di *risk management* sempre tenendo conto del *company risk profile* (definito dall'insieme dei rischi aziendali rilevanti ai fini del raggiungimento degli obiettivi).

2.2. Punto di attenzione – Comunicazione delle carenze riscontrate

Le eventuali carenze riscontrate dovrebbero essere comunicate ai soggetti responsabili per la realizzazione degli interventi correttivi, al *management* e al Consiglio di Amministrazione. Le caratteristiche del *reporting* variano a seconda dei principi stabiliti dalla legge, dagli organismi regolatori, dal *management* e dal Consiglio di Amministrazione. Per raggiungere gli obiettivi aziendali, le carenze riscontrate devono sempre essere comunicate a due soggetti:

a) coloro che effettuano la valutazione complessiva del SCIGR;

b) coloro che sono responsabili per la realizzazione delle azioni di miglioramento.

Un ulteriore coinvolgimento è quello del *management* e del Consiglio di Amministrazione; la condivisione con questi due soggetti assicura supporto, supervisione e integrazione.

Qualora le carenze riscontrate riguardino più livelli organizzativi è necessario riportare il risultato ad un livello sufficientemente elevato affinché sia definito l'opportuno piano di azione.

Qualora siano rilevate delle non conformità sarà necessario identificare e definire delle azioni correttive appropriate ai fini di eliminare le cause che le hanno provocate. Si definirà, quindi, un "piano di azioni correttive/miglioramento" che comprenda:

a) le azioni che verranno intraprese;

b) i responsabili della realizzazione di tali azioni;

c) le tempistiche di completamento di tali azioni.

2.3. Punto di attenzione – Monitoraggio delle azioni correttive

Periodicamente, il *management* dovrebbe controllare l'avvenuta implementazione delle azioni correttive e quindi la rimozione delle carenze riscontrate in fase di *ongoing/separate evaluation*. La responsabilità di monitorare le azioni correttive ricadrà su un soggetto differente da quello responsabile della relativa implementazione.

Qualora le azioni correttive non siano implementate nelle tempistiche previste e condivise, sarà necessario riportare questa tematica nuovamente all'attenzione del *management* ad un livello che sia superiore rispetto a quello responsabile per il piano di miglioramento.

2.4. Strumenti applicativi

Si riportano di seguito, a titolo esemplificativo e non esaustivo, alcuni tra i principali elementi di concreta attuazione dei punti di attenzione del principio in esame:

- **Valutazione da parte dei soggetti responsabili dei risultati delle Attività di Monitoraggio svolte**: ad esempio, al termine delle Attività di Monitoraggio condotte sull'*ageing* del credito, il *credit manager* responsabile per l'attività riferisce al Comitato Crediti (Comitato manageriale) gli esiti delle valutazioni svolte in modo che possano essere valutate eventuali carenze e che si definisca un piano di azioni correttive condivise per sopperire alle mancanze rilevate;
- ***Report* dell'*Internal Auditing*,** che riportino la valutazione di sintesi del Sistema di Controllo Interno e di gestione dei rischi riferito alle aree/processi oggetto di verifica, la descrizione dei rilievi riscontrati e delle limitazioni incontrate inviati dal Responsabile della funzione *Internal Audit* al Presidente del Consiglio di Amministrazione, all'Amministratore Delegato, al Comitato Controllo e Rischi nonché al Collegio Sindacale e al *Chief Financial Officer,* ove individuato quale

Dirigente Preposto alla redazione dei documenti contabili societari (per quest'ultimo, per gli aspetti di relativa competenza);

- **Informativa data dal Responsabile della funzione *Internal Audit*** verso il Presidente del Consiglio di Amministrazione, l'Amministratore Delegato, il Comitato Controllo e Rischi nonché il Collegio Sindacale e il *Chief Financial Officer* (se individuato quale Dirigente Preposto) circa eventuali rilievi nel sistema di prevenzione delle irregolarità e atti fraudolenti oppure irregolarità commesse da dipendenti che ricoprono un ruolo importante nel disegno o nel funzionamento del SCIGR;
- **Monitoraggio delle azioni correttive**: il Responsabile della funzione *Internal Audit* sulla base dell'eventuale piano delle azioni correttive dovrebbe monitorare periodicamente l'avvenuta realizzazione delle azioni di miglioramento ed in seguito procede all'aggiornamento periodico del relativo stato di attuazione con riferimento alle valutazioni interne ed esterne effettuate;
- **Valutazione da parte della Funzione di *Risk Management*** in merito alla corretta identificazione, valutazione, gestione e monitoraggio dei principali rischi rispetto agli obiettivi aziendali;
- **Valutazione da parte della Funzione di *Compliance*** rispetto all'identificazione delle norme e dei relativi impatti sui processi aziendali nonché sul recepimento dei requisiti in esse previsti.

Tabella 1 - Riepilogo degli esempi di strumenti applicativi per componente/principio del COSO

La Tabella 1 riporta, per ogni Componente del COSO *Framework,* i relativi Principi e tutti gli Strumenti Applicativi identificati nel corpo del documento. Essa vuole costituire una sintesi efficace per favorire l'interpretazione dei Principi del COSO *Framework*, esemplificandone la concreta attuazione all'interno del contesto aziendale.

Componente COSO	Principio	Strumento Applicativo
1. Ambiente di Controllo	Principio n. 1 – L'organizzazione dimostra il proprio impegno rispetto ai valori etici e all'integrità	Statuto societario
		Sistema di deleghe e procure
		Linee guida in materia di governo societario
		Codice Etico (e/o di Condotta e/o di Comportamento)
		Modello di Organizzazione, Gestione e Controllo *ex* D.Lgs. 231/2001
		Linee guida sul SCIGR (in particolare per le società quotate)
		Sistema sanzionatorio
		Norme in materia di anticorruzione
		Sistema di segnalazione delle violazioni (*whistleblowing*)
		Politiche di remunerazione e incentivazione
		Piani di formazione e comunicazione
		Verifiche periodiche sul clima aziendale
	Principio n. 2 – Il Consiglio di Amministrazione è indipendente rispetto al *management* ed esercita la propria supervisione sullo sviluppo e sull'implementazione del Sistema di controllo interno e di gestione dei rischi	Piano strategico
		Programma di *assessment* e di formazione del Consiglio di Amministrazione
		Relazione sulla *corporate governance*
		Regolamento del Comitato Controllo e Rischi e di altri eventuali Comitati all'interno del Consiglio di Amministrazione
		Policy di *Enterprise Risk Management* (ERM) e profilo di rischio
		Procedura sulle operazioni con parti correlate
		Corpus procedurale
		Piano di *Internal Audit risk-based*
	Principio n. 3 – Il *management* definisce, sotto la supervisione del Consiglio di Amministrazione, la struttura organizzativa, le linee di riporto, i livelli autorizzativi e le responsabilità funzionali al fine di perseguire gli obiettivi aziendali	Partecipogramma societario
		Policy/direttive di Gruppo
		Modelli di controllo implementati a fronte di specifiche norme e *leading practice* (es. L. 262/2005, sistema di gestione della qualità, sistema di gestione HSE, *privacy*, informativa non finanziaria, ecc.)
		Organigramma societario
		Mansionari e *job description*
		Sistema di deleghe e procure
		Comunicazioni organizzative
		Corpus procedurale

Componente COSO	Principio	Strumento Applicativo
	Principio n. 4 – L'organizzazione dimostra il proprio impegno ad attrarre, sviluppare e trattenere risorse competenti, in linea con il conseguimento degli obiettivi aziendali	Piano strategico
		Corpus procedurale
		Mappa della competenze
		Politiche di *recruiting*
		Processi di formazione e sviluppo del personale
		Politiche di remunerazione e incentivazione
		Piano di successione
		Processo strutturato di definizione degli obiettivi e valutazione della *performance*
	Principio n. 5 – L'organizzazione, nel raggiungimento degli obiettivi aziendali, ritiene i singoli individui responsabili per la parte del Sistema di controllo interno di propria competenza	Mandato all'*Internal Audit (Audit Charter)*
		Posizionamento organizzativo delle funzioni di controllo
		Mansionari e *job description*
		Politiche di remunerazione e incentivazione
		Sistema di valutazione delle prestazioni
		Piano di successione del personale chiave delle funzioni di controllo
2. *Risk Assessment*	Principio n. 6 – L'organizzazione esplicita con sufficiente chiarezza i propri obiettivi, consentendo l'identificazione e la valutazione dei rischi ad essi legati	Piano strategico
		Processo strutturato di identificazione e valutazione dei rischi
		Budget
		Reportistica periodica e strutturata supportata da strumenti informatici adeguati
		Politiche di remunerazione e incentivazione
		Monitoraggio dei *Key Performance Indicator*
	Principio n. 7 – L'organizzazione identifica i rischi connessi al conseguimento degli obiettivi aziendali e ne determina le modalità di gestione	Definizione del *risk appetite*
		Definizione di un modello integrato di gestione dei rischi aziendali, cd. *Enterprise Risk Management* (ERM)
		Definizione, implementazione e aggiornamento del SCIGR
		Corpus procedurale
		Monitoraggio dei *Key Risk Indicator* (KRI)
		Analisi del contesto
		Analisi quantitative
		Implementazione di strumenti di *Governance Risk e Compliance* (GRC)
		Piano di *Internal Audit risk-based*
	Principio n. 8 – L'organizzazione prende in considerazione potenziali frodi nel valutare i rischi di conseguimento dei propri obiettivi aziendali	Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001
		Codice Etico (e/o di Condotta e/o di Comportamento)
		Definizione degli schemi di frode
		Programmi di *Fraud Risk Assessment and Prevention*
		Politiche di remunerazione e incentivazione
		Sistema sanzionatorio
		Sistema di segnalazione delle violazioni (*whistleblowing*)

Componente COSO	Principio	Strumento Applicativo
	Principio n. 9 – L'organizzazione identifica e valuta i cambiamenti che potrebbero avere impatti significativi sul Sistema di controllo interno	Analisi SWOT (*Strengths, Weaknesses, Opportunities, Threats*)
		Analisi dei *competitor*
		Analisi dei prodotti/servizi
		Analisi della clientela
		Analisi degli effetti nel cambiamento di leadership
		Analisi scenario normativo che monitori l'evoluzione delle normative di riferimento
		Business Impact Analysis e Piano di *Business Continuity*
3. Attività di Controllo	Principio n. 10 – L'organizzazione definisce e implementa attività di controllo che contribuiscono a ridurre i rischi entro livelli accettabili	Rappresentazione della catena del valore aziendale
		Rappresentazione dei controlli all'interno delle matrici dei rischi
		Identificazione degli *outsourcer* significativi per i processi rilevanti
		Predisposizione di documenti di *Gap Analysis*
		Lista dei principi di SoD
		Svolgimento di analisi SoD
		Svolgimento di analisi del "transato"
		Corpus procedurale
	Principio n. 11 – L'organizzazione definisce e implementa attività di controllo sulla tecnologia, per supportare il raggiungimento degli obiettivi aziendali	Lista/mappatura delle applicazioni aziendali
		Information Technology General Controls
		Identificazione dei profili di accesso ai sistemi
		Matrice funzionale dei profili attivati
		Procedura per l'abilitazione ai sistemi informatici
		Vulnerability assessment e piani antiintrusione
		Mappatura dei fogli di calcolo e controlli attesi
		Documentazione della configurazione dei sistemi IT
	Principio n. 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	Identificazione, valutazione e documentazione dei controlli relativi ai rischi aziendali rilevanti
		Corpus procedurale
		Funzionigrammi, mansionari e *job description*
		Check list e *standard* di controllo
		Verifiche periodiche del disegno dei controlli
		Gap Analysis e piani di attuazione delle azioni correttive
4. Informazione e Comunicazione	Principio n. 13 – L'organizzazione ottiene o genera e utilizza informazioni rilevanti e di qualità a supporto del funzionamento del Sistema di controllo interno e di gestione dei rischi	Sistemi contabili e gestionali
		Sistemi di *business intelligence*
		Software per la raccolta delle informazioni
		Applicativi per la gestione del SCIGR
		Sistema di segnalazione delle violazioni (*whistleblowing*)
		Funzione *Investor Relations*
		Sezioni dedicate dei siti web

Componente COSO	Principio	Strumento Applicativo
		Partecipazione, da parte dalle funzioni di controllo, ai *management meeting*
		Reporting alle funzioni di controllo
		Scambio informazioni tra le funzioni di controllo
	Principio n. 14 – L'organizzazione comunica internamente le informazioni, compresi gli obiettivi e le responsabilità di controllo interno, necessarie a supportare il funzionamento del Sistema di controllo interno e di gestione dei rischi nel suo complesso	Relazione periodica dell'Organismo di Vigilanza
		Comunicazione degli amministratori indipendenti al CdA
		Indicazioni del Comitato Controllo e Rischi
		Relazione annuale del Collegio Sindacale
		Relazioni rilasciate dal revisore
		Relazioni e verbali sul SCIGR
		Modello di Organizzazione, Gestione e Controllo *ex* D.Lgs. 231/2001
		Comunicazione su strumenti normativi e organizzativi
		Ordini di servizio o mandati delle funzioni preposte ad attività di Controllo Interno
		Risultati del *Risk Assessment*
		Risk Control Matrix
		Piano di I*nternal Audit risk-based*
		Evidenze ed esiti dei test e dei controlli svolti
		Report dell'*Internal Audit*
	Principio n. 15 – L'organizzazione comunica con parti terze relativamente a questioni che interessano il funzionamento del Sistema di controllo interno e di gestione dei rischi	Relazioni finanziarie annuali e periodiche
		Specifiche comunicazioni di settore
		Comunicazioni/dichiarazioni di *non financial* information
		Comunicazione di specifiche *policy*
		Relazione sulla *corporate governance* (per le società quotate, come previsto dal TUF)
		Informazioni regolamentate
5. Attività di monitoraggio	Principio n. 16 – L'organizzazione definisce, sviluppa ed esegue valutazioni continuative (*ongoing*) e obiettive (*separate*) per accertare che le componenti del controllo interno siano presenti e funzionanti.	*Risk Assessment* per la definizione del *Corporate Risk Profile*
		Business Review del Controllo di Gestione
		Piano di *Internal Audit risk-based*
		Attività di *benchmarking* di processi o controlli rispetto a quelli di altre società comparabili
		Quality Assurance Review delle attività di *Internal Audit*
		Certificazione ISO per il sistema di gestione della qualità, ambientale, salute e sicurezza, anti-corruzione, ecc.
		Controllo qualità delle materie prime e dei prodotti finiti
		Conta fisica delle scorte di magazzino
		Verifica delle riconciliazioni bancarie
		Controlli di produzione
		Conta fisica in fase di ricevimento merci
		Verifica dell'*ageing* del credito
		Verifica della giacenze di magazzino
		Verifica degli accessi fisici

Componente COSO	Principio	Strumento Applicativo
	Principio n. 17 – L'organizzazione valuta e comunica tempestivamente le carenze del Sistema di controllo interno ai soggetti responsabili di intraprendere le necessarie azioni correttive, incluso il *senior management* e il Consiglio di Amministrazione per quanto necessario e di competenza.	Valutazione da parte dei soggetti responsabili dei risultati delle Attività di Monitoraggio svolte
		Report dell'*Internal Audit*
		Informativa data dal Responsabile della funzione *Internal Audit*
		Monitoraggio delle azioni correttive
		Valutazione da parte della Funzione di *Risk Management*
		Valutazione da parte della Funzione di *Compliance*

Tabella 2 – Riepilogo degli esempi di strumenti applicativi per Ambito

La Tabella 2 introduce il concetto di "Ambito" inteso come macroarea o tematica rilevante nella costituzione e funzionamento di efficaci e funzionali sistemi di gestione dei rischi e di controllo interno. L'Ambito è immediatamente riconducibile, da parte di qualunque società, alle attività aziendali ed alle responsabilità di singole funzioni interne. A ciascun Ambito sono ricondotti, senza duplicazioni, tutti gli Strumenti Applicativi (con l'evidenza dei Componenti COSO e dei relativi Principi) identificati nel corpo del documento.

Conseguentemente, una Società, mediante la verifica degli Strumenti Applicativi effettivamente implementati nei diversi Ambiti, potrà più facilmente valutare il proprio livello di allineamento ai Principi del COSO *Framework* e attraverso quali eventuali interventi contribuire al miglioramento del processo di gestione dei rischi nonché all'attivazione dei sistemi a presidio degli stessi.

Ambito	Strumento Applicativo	Componente COSO	Principio
Pianificazione, budget e controllo	Analisi degli effetti nel cambiamento di *leadership*	Attività di controllo	Principio n. 9
	Analisi dei *competitor*	Attività di controllo	Principio n. 9
	Analisi dei prodotti/servizi	Attività di controllo	Principio n. 9
	Analisi del contesto	*Risk Assessment*	Principio n. 7
	Analisi della clientela	Attività di controllo	Principio n. 9
	Analisi quantitative	*Risk Assessment*	Principio n. 7
	Analisi scenario normativo che monitori l'evoluzione delle normative di riferimento	Attività di controllo	Principio n. 9
	Analisi SWOT (*Strengths, Weaknesses, Opportunities, Threats*)	Attività di controllo	Principio n. 9
	Piano strategico	Ambiente di Controllo, *Risk Assessment*	Principi n. 2, 4, 6
	Budget	*Risk Assessment*	Principio n. 6
	Business Review del Controllo di Gestione	Attività di monitoraggio	Principio n. 16
	Mappatura dei fogli di calcolo e controlli attesi	Attività di controllo	Principio n. 11
	Monitoraggio dei *Key Performance Indicator*	*Risk Assessment*	Principio n. 6
	Processo strutturato di definizione degli obiettivi e valutazione della performance	Ambiente di Controllo	Principio n. 4
***Governance*, assetti organizzativi ed impianto normativo interno**	Statuto societario	Ambiente di Controllo	Principio n. 1
	Organigramma societario	Ambiente di Controllo	Principio n. 3
	Programma di *assessment* e di formazione del Consiglio di Amministrazione	Ambiente di Controllo	Principio n. 2
	Regolamento Comitato Controllo e Rischi e di altri eventuali Comitati all'interno del Consiglio di Amministrazione	Ambiente di Controllo	Principio n. 2
	Partecipazione, da parte dalle funzioni di controllo, ai *management meeting*	Informazione e Comunicazione	Principio n. 13
	Partecipogramma societario	Ambiente di Controllo	Principio n. 3
	Lista dei principi di SoD	Attività di controllo	Principio n. 10
	Svolgimento di analisi SoD	Attività di controllo	Principio n. 10
	Sistema di deleghe e procure	Ambiente di Controllo	Principi n. 1, 3
	Comunicazioni organizzative	Ambiente di Controllo	Principio n. 3

Ambito	Strumento Applicativo	Componente COSO	Principio
	Corpus procedurale	Ambiente di Controllo, *Risk Assessment*, Attività di Controllo	Principi n. 3, 4, 7, 10, 12
	Funzionigrammi, mansionari e *job description*	Attività di controllo	Principio n. 12
	Mansionari e *job description*	Ambiente di Controllo	Principi n. 3, 5
	Policy/direttive di Gruppo	Ambiente di Controllo	Principio n. 3
	Comunicazione di specifiche *policy*	Informazione e Comunicazione	Principio n. 15
	Comunicazione su strumenti normativi e organizzativi	Informazione e Comunicazione	Principio n. 14
	Rappresentazione della catena del valore aziendale	Attività di controllo	Principio n. 10
	Attività di *benchmarking* di processi o controlli rispetto a quelli di altre Società comparabili	Attività di monitoraggio	Principio n. 16
Sistema di gestione dei rischi	Definizione del *risk appetite*	*Risk Assessment*	Principio n. 7
	Definizione di un modello integrato di gestione dei rischi, cd. *Enterprise Risk Management* (ERM)	*Risk Assessment*	Principio n. 7
	Policy di *Enterprise Risk Management* (ERM) e profilo di rischio	Ambiente di Controllo	Principio n. 2
	Implementazione di strumenti di *Governance Risk e Compliance* (GRC)	*Risk Assessment*	Principio n. 7
	Processo strutturato di identificazione e valutazione dei rischi	*Risk Assessment*	Principio n. 6
	Valutazione da parte della Funzione di *Risk Management*	Attività di monitoraggio	Principio n. 17
	Risk Assessment del *Chief Risk Officer* per la definizione del *Corporate Risk Profile*	Attività di monitoraggio	Principio n. 16
	Identificazione, valutazione e documentazione dei controlli relativi ai rischi aziendali rilevanti	Attività di controllo	Principio n. 12
	Risultati del *Risk Assessment*	Informazione e Comunicazione	Principio n. 14
	Indicazioni del Comitato Controllo e Rischi	Informazione e Comunicazione	Principio n. 14
	Linee guida sul SCIGR (in particolare per le società quotate)	Ambiente di Controllo	Principio n. 1
	Monitoraggio dei *Key Risk Indicator* (KRI)	*Risk Assessment*	Principio n. 7
Sistema di controllo interno e *compliance*	*Business Impact Analysis* e Piano di *Business Continuity*	Attività di controllo	Principio n. 9
	Mandato all'*Internal Audit (Audit Charter)*	Ambiente di Controllo	Principio n. 5
	Piano di *Internal Audit risk-based*	Ambiente di Controllo, *Risk Assessment*, Informazione e Comunicazione, Attività di Monitoraggio	Principi n. 2, 7, 14, 16
	Definizione, implementazione e aggiornamento del SCIGR	*Risk Assessment*	Principio n. 7
	Applicativi per la gestione del SCIGR	Informazione e Comunicazione	Principio n. 13
	Evidenze ed esiti dei test e dei controlli svolti	Informazione e Comunicazione	Principio n. 14
	Predisposizione di documenti di *Gap Analysis*	Attività di controllo	Principio n. 10
	Gap Analysis e piani di attuazione delle azioni correttive	Attività di controllo	Principio n. 12
	Monitoraggio delle azioni correttive	Attività di monitoraggio	Principio n. 17

Ambito	Strumento Applicativo	Componente COSO	Principio
	Rappresentazione dei controlli all'interno delle matrici dei rischi	Attività di controllo	Principio n. 10
	Report dell'*Internal Audit*	Informazione e Comunicazione, Attività di monitoraggio	Principi n. 14, 17
	Informativa data dal Responsabile della funzione *Internal Audit*	Attività di monitoraggio	Principio n. 17
	Posizionamento organizzativo delle funzioni di controllo	Ambiente di Controllo	Principio n. 5
	Reporting alle funzioni di controllo	Informazione e Comunicazione	Principio n. 13
	Scambio informazioni tra le funzioni di controllo	Informazione e Comunicazione	Principio n. 13
	Risk Control Matrix	Informazione e Comunicazione	Principio n. 14
	Quality Assurance Review delle attività di *Internal Audit*	Attività di monitoraggio	Principio n. 16
	Certificazione ISO per il sistema di gestione della qualità, ambientale, salute e sicurezza, anti-corruzione, ecc.	Attività di monitoraggio	Principio n. 16
	Check list e *standard* di controllo	Attività di controllo	Principio n. 12
	Identificazione degli *outsourcer* significativi per i processi rilevanti	Attività di controllo	Principio n. 10
	Modelli di controllo implementati a fronte di specifiche norme e *leading practice* (es. L.262/2005, sistema di gestione della qualità, sistema di gestione HSE, *privacy*, informativa non finanziaria, ecc.)	Ambiente di Controllo	Principio n. 3
	Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001	Ambiente di Controllo, *Risk Assessment*, Informazione e Comunicazione	Principi n. 1, 8, 14
	Ordini di servizio o mandati delle funzioni preposte ad attività di Controllo Interno	Informazione e Comunicazione	Principio n. 14
	Valutazione da parte dei soggetti responsabili dei risultati delle Attività di Monitoraggio svolte	Attività di monitoraggio	Principio n. 17
	Valutazione da parte della Funzione di *Compliance*	Attività di monitoraggio	Principio n. 17
	Verifica degli accessi fisici	Attività di monitoraggio	Principio n. 16
	Verifica dell'*ageing* del credito	Attività di monitoraggio	Principio n. 16
	Verifica delle riconciliazioni bancarie	Attività di monitoraggio	Principio n. 16
	Conta fisica in fase di ricevimento merci	Attività di monitoraggio	Principio n. 16
	Conta fisica delle scorte di magazzino	Attività di monitoraggio	Principio n. 16
	Verifica della giacenze di magazzino	Attività di monitoraggio	Principio n. 16
	Controllo qualità delle materie prime e dei prodotti finiti	Attività di monitoraggio	Principio n. 16
	Verifiche periodiche del disegno dei controlli	Attività di controllo	Principio n. 12
	Verifiche periodiche sul clima aziendale	Ambiente di Controllo	Principio n. 1
	Controlli di produzione	Attività di monitoraggio	Principio n. 16
	Svolgimento di analisi del "transato"	Attività di controllo	Principio n. 10

Ambito	Strumento Applicativo	Componente COSO	Principio
Antifrode, anticorruzione e gestione dei conflitti di interesse	Sistema di segnalazione delle violazioni (*whistleblowing*)	Ambiente di Controllo, *Risk Assessment*, Informazione e Comunicazione	Principi n. 1, 8, 13
	Definizione degli schemi di frode	*Risk Assessment*	Principio n. 8
	Norme in materia di anticorruzione	Ambiente di Controllo	Principio n. 1
	Corpus procedurale	Ambiente di Controllo	Principio n. 2
	Codice Etico (e/o di Condotta e/o di Comportamento)	Ambiente di Controllo, *Risk Assessment*	Principi n. 1, 8
	Procedura sulle operazioni con parti correlate	Ambiente di Controllo	Principio n. 2
	Programmi di *Fraud Risk Assessment and Prevention*	*Risk Assessment*	Principio n. 8
	Sistema sanzionatorio	Ambiente di Controllo, *Risk Assessment*	Principi n. 1, 8
Sistemi informativi e *cyber risk*	Documentazione della configurazione dei sistemi IT	Attività di controllo	Principio n. 11
	Identificazione dei profili di accesso ai sistemi	Attività di controllo	Principio n. 11
	Information Technology General Controls	Attività di controllo	Principio n. 11
	Lista/mappatura delle applicazioni aziendali	Attività di controllo	Principio n. 11
	Matrice funzionale dei profili attivati	Attività di controllo	Principio n. 11
	Procedura per l'abilitazione ai sistemi informatici	Attività di controllo	Principio n. 11
	Vulnerability assessment e piani antiintrusione	Attività di controllo	Principio n. 11
Gestione e valorizzazione delle risorse umane	Piani di formazione e comunicazione	Ambiente di Controllo	Principio n. 1
	Processi di formazione e sviluppo del personale	Ambiente di Controllo	Principio n. 4
	Mappa della competenze	Ambiente di Controllo	Principio n. 4
	Piano di successione	Ambiente di Controllo	Principio n. 4
	Piano di successione del personale chiave delle funzioni di controllo	Ambiente di Controllo	Principio n. 5
	Politiche di *recruiting*	Ambiente di Controllo	Principio n. 4
	Sistema di valutazione delle prestazioni	Ambiente di Controllo	Principio n. 5
Remunerazione ed incentivazione	Politiche di remunerazione e incentivazione	Ambiente di Controllo, *Risk Assessment*	Principi n. 1, 4, 5, 6, 8
Produzione dell'informativa interna ed esterna	Informazioni regolamentate	Informazione e Comunicazione	Principio n. 15
	Linee guida in materia di governo societario	Ambiente di Controllo	Principio n. 1
	Relazione annuale del Collegio Sindacale	Informazione e Comunicazione	Principio n. 14
	Relazione periodica dell'Organismo di Vigilanza	Informazione e Comunicazione	Principio n. 14
	Relazione sulla corporate *governance*	Ambiente di Controllo, Informazione e Comunicazione	Principi n. 2, 15
	Relazioni e verbali sul SCIGR	Informazione e Comunicazione	Principio n. 14
	Relazioni finanziarie annuali e periodiche	Informazione e Comunicazione	Principio n. 15
	Funzione *Investor Relations*	Informazione e Comunicazione	Principio n. 13
	Reportistica periodica e strutturata supportata da strumenti informatici adeguati	*Risk Assessment*	Principio n. 6

Ambito	Strumento Applicativo	Componente COSO	Principio
	Relazioni rilasciate dal revisore	Informazione e Comunicazione	Principio n. 14
	Sezioni dedicate dei siti web	Informazione e Comunicazione	Principio n. 13
	Specifiche comunicazioni di settore	Informazione e Comunicazione	Principio n. 15
	Comunicazioni degli amministratori indipendenti al CdA	Informazione e Comunicazione	Principio n. 14
	Comunicazioni di *non financial information*	Informazione e Comunicazione	Principio n. 15
	Sistemi contabili e gestionali	Informazione e Comunicazione	Principio n. 13
	Sistemi di *business intelligence*	Informazione e Comunicazione	Principio n. 13
	Software per la raccolta delle informazioni	Informazione e Comunicazione	Principio n. 13

AUTORI

La presente monografia è stata realizzata dal Gruppo di Ricerca Governance, che è così composto:

Zanghi Nicolò	(KPMG S.p.A.)
Lorenzoni Adele	(ASSIREVI)
Marcucci Fabrizio	(Deloitte & Touche S.p.A.)
Fortunato Stefano	(KPMG S.p.A.)
Gallistru Alfredo	(PricewaterhouseCoopers S.p.A.)
Damiano Cinzia	(PricewaterhouseCoopers S.p.A.)
De Romanis Ginevra	(EY S.p.A.)
Girardi Alberto	(EY S.p.A.)
Carnesecchi Giuseppe	(BDO Italia S.p.A.)
Gnocchi Stefano	(Mazars Italia S.p.A.)
Dellatorre Enrica	(Mazars Italia S.p.A.)
Cattaneo Laura	(Audirevi S.p.A.)
Losa Manuela	(Audirevi S.p.A.)

ORGANI SOCIALI
ASSIREVI

Assemblea delle Associate

AGKNSERCA S.n.c.
Audirevi S.p.A.
Axis S.r.l.
Baker Tilly Revisa S.p.A.
BDO Italia S.p.A.
Deloitte & Touche S.p.A.
EY S.p.A.
KPMG S.p.A.
Mazars Italia S.p.A.
PKF Italia S.p.A.
PricewaterhouseCoopers S.p.A.
Prorevi Auditing S.r.l.
Re.Bi.S. S.r.l.
RIA Grant Thornton S.p.A.
Trevor S.r.l.
UHY Bompani S.r.l.

Componenti del Consiglio Direttivo

CONSIGLIERE	VICE CONSIGLIERE
Mario Boella (P)	Luca Ferranti
Simone Scettri (VP)	Massimo Antonelli
Simone Del Bianco (VP e T)	Rosanna Vicari
Anna Baldini	Alfonso Laratta
Gianmario Crescentino	Stefano Dell'Orto
Sandro Gherardini	Maurizio Finicelli
Umberto Giacometti	Maria Luisa Delcaldo
Maurizio Lonati	Giorgio Greco
Olivier Rombaut	Marco Lumeridi
Davide Trinchero	Bruno Piazza

(P) Presidente
(VP) Vice Presidente
(T) Tesoriere

ASSIREVI

ASSIREVI (Associazione Italiana Revisori Contabili) è un'associazione privata senza scopo di lucro fondata nel 1980. L'Associazione è iscritta nel Registro delle persone giuridiche della Prefettura di Milano con il n. 1261.

Possono aderire all'Associazione le società di revisione operanti in Italia iscritte al Registro di cui all'art. 6 e ss. D.Lgs. 39/2010 e relative disposizioni attuative.

ASSIREVI riunisce oggi 16 società di revisione, che costituiscono attualmente la maggior parte delle società che svolgono la revisione degli Enti di Interesse Pubblico. Attualmente i professionisti che operano nell'ambito dell'attività di revisione svolta dalle Associate sono circa 6.000, con una presenza distribuita su tutto il territorio nazionale.

ASSIREVI promuove e realizza l'analisi scientifica di supporto all'adozione dei principi di revisione (norme etico professionali, norme tecniche di svolgimento della revisione contabile e norme di stesura della relazione di revisione) e dei principi di *assurance*, nonché lo studio dell'evoluzione della legislazione e della regolamentazione. Inoltre, è impegnata nella risoluzione di problematiche professionali, giuridiche e fiscali di comune interesse delle Associate.

In tale contesto, collabora con le Istituzioni e le Autorità Pubbliche, con gli organismi professionali, e con altri organismi ed enti nella determinazione e nell'aggiornamento dei principi di revisione, di *assurance* e dei principi contabili.

ASSIREVI

www.assirevi.it

Milano, Gennaio 2019
Provider: register.it