ASSIREVI

MONOGRAFIE

COSO ERM:
guida alla lettura

n°3 - Novembre 2020

ASSIREVI
Associazione Italiana delle Società di Revisione Legale

Indice

PREMESSA

Lo scenario determinatosi a seguito della pandemia da COVID-19 ha definitivamente acclarato che lo sviluppo economico è caratterizzato da *shock* che periodicamente mettono a dura prova la tenuta del sistema economico e del tessuto delle imprese in esso operanti. Il XXI secolo ha già prodotto almeno tre grandi eventi di tale portata: l'attacco terroristico alle Torri Gemelle del 2001, la crisi finanziaria del 2008-2011 e, infine, la pandemia COVID-19. Le conseguenze sono state diverse ma di portata eccezionalmente rilevante e hanno richiesto cambiamenti delle regole di convivenza sociale e di gestione e controllo delle imprese.

La pandemia è attualmente in corso e le misure di contrasto del virus richiedono l'applicazione di misure di distanziamento sociale fino alla forma più drastica di chiusura delle attività economiche non indispensabili (*lock-down*) e l'attivazione di modalità di lavoro a distanza (*smart working*).

Le cause dell'evento pandemico sono, secondo alcuni, in buona parte ascrivibili al deterioramento delle condizioni sociali e ambientali, che ormai da molti anni viene registrato dai diversi osservatori internazionali, in special modo, per quanto attiene ai cambiamenti climatici. Tali fattori, cosiddetti ESG (*Environmental*, *Social*, *Governance*), stanno via via assumendo sempre maggiore rilevanza nei modelli di governo societario richiedendo alle imprese di assumere comportamenti sempre più sostenibili nel lungo periodo.

Nonostante la pandemia fosse un rischio conosciuto, la portata con cui si è manifestato ha messo a dura prova la capacità di attivare misure efficaci di contrasto della diffusione del virus e del mantenimento delle attività operative necessarie, sia da parte dei soggetti pubblici sia da parte delle imprese private.

Dal punto di vista delle imprese, la gestione corrente della crisi generata dal COVID-19 ha acclarato la necessità di implementare processi adeguati di *risk management* integrati nei processi decisionali ovvero che influenzino le scelte strategiche dell'impresa che non possono più basarsi su scenari stabili e tassi di crescita allineati al normale ciclo economico.

Difatti oltre all'instabilità, all'incertezza e alla volatilità dello scenario, con i quali abbiamo imparato a convivere, la nuova normalità richiede sistemi di governo ancora più resilienti, in grado di rispondere alle situazioni di stress con nuovi e differenti approcci che non necessariamente assumano carattere di temporaneità (come tipicamente avviene nel *crisis management*) ma diventino revisioni vere e proprie del modello operativo.

In questo contesto, il *Framework* "*Enterprise Risk Management – Aligning Risk with Strategy and Performance*" (di seguito anche "*Framework* COSO ERM" o semplicemente "*Framework*"), rappresenta un modello di riferimento e una guida per le imprese che intendono adottare processi robusti di gestione dei rischi in grado di orientare al meglio le strategie in base alle *performance* ma anche considerando le discontinuità che si possono originare da scenari particolarmente avversi ma plausibili.

Più recentemente, il *Framework* è stato integrato con una parte dedicata alla gestione dei rischi ESG ovvero quei rischi che possono pregiudicare il raggiungimento degli obiettivi di sostenibilità che le imprese stanno via via adottando anche attraverso le trasformazioni dei propri modelli di *business*.

È altresì essenziale registrare, nell'ambito dell'evoluzione dei modelli di *corporate governance*, che l'obiettivo del "successo sostenibile" sia stato definito e si sostanzi nella creazione di valore nel lungo termine a beneficio degli azionisti e degli altri stakeholder. In tale nuovo contesto, misurare la creazione di valore con il solo metro della *performance* finanziaria potrebbe risultare non più sufficiente mentre sarebbe opportuno valutare le altre attività immateriali ovvero la tecnologia e l'innovazione, la proprietà intellettuale, il capitale umano, le alleanze e le relazioni con le comunità, i clienti e i dipendenti.

Obiettivo del Gruppo di Ricerca, con la pubblicazione della presente Monografia, è stato quello di contribuire alla diffusione dei principi di *leading practice* del *Framework* che, in quanto tali, costituiscono un'utile guida per le imprese che intendano implementare o rafforzare i processi di *risk management* per affrontare le sfide che lo scenario economico impone loro di affrontare.

Nel prosieguo di questa premessa, in sintesi, e nei successivi capitoli del documento, in maggior dettaglio, sono descritte le caratteristiche del *Framework* e le sue componenti attraverso un approccio basato su 20 principi di *leading practice*.

1. Il *Framework Enterprise Risk Management*

Integrare il processo di *risk management* in tutte le componenti e le attività di una azienda significa rafforzare la capacità di *prendere decisioni* in materia di *governance*, strategia, definizione degli obiettivi e operatività. L'integrazione del *risk management* nei processi aziendali consente di migliorarne le *performance* ottenendo come risultato la definizione di un chiaro percorso per creare e preservare *valore*.

La riflessione sull'*Enterprise Risk Management* (ERM) deve partire da queste premesse:

- ogni entità, sia essa *profit, no profit* o pubblica, ha come fine la creazione del valore per tutti gli *stakeholder*;
- per creare valore ogni entità deve affrontare dei rischi.

Una prima sfida che il *management* deve affrontare è la quantificazione del livello di rischio che l'organizzazione è in grado di accettare (*risk appetite*) in coerenza con gli elementi fondanti dell'organizzazione stessa *(mission, vision e core value)*.

Il *Framework* sposta il focus sui principali requisiti necessari a far funzionare e rendere effettivo l'ERM all'interno di un'organizzazione. Il *Framework* propone una struttura concettuale secondo la quale un'organizzazione dovrebbe integrare i processi di *risk management* nella gestione del proprio *business* con l'obiettivo di realizzare la *strategia*, migliorare la misurazione dei risultati (*performance*) e creare valore nel tempo.

Riconoscendo perciò la crescente rilevanza della relazione "Rischio - Strategia - *Performance* aziendali", il *Framework* rafforza alcune componenti fondamentali caratterizzanti la vita aziendale:

- **Valore**

Il *valore* in una organizzazione è determinato dalle scelte del *management*, dalla definizione delle strategie alle decisioni operative. Il valore si intende:

- *creato:* quando i benefici superano le risorse impiegate in termini di costo;
- *preservato:* quando le risorse impiegate consentono il mantenimento del valore creato;
- *eroso:* quando il *management* implementa una strategia che non produce i risultati attesi;
- *realizzato:* quando il valore viene distribuito agli *stakeholder*.

Il valore può avere carattere monetario o non monetario a seconda del tipo di entità: le società lucrative producono valore quando realizzano con successo delle strategie che bilanciano opportunità e rischi economici. Le società non lucrative e le società pubbliche realizzano valore distribuendo beni e servizi che bilanciano l'opportunità di servire la comunità rispetto ai rischi afferenti.

- ***Mission*, *vision* e *core value***

La *mission*, la *vision* ed i *core value* definiscono cosa una entità vuole essere e come vuole condurre il proprio *business*. Comunicano agli *stakeholder* il fine dell'organizzazione.

In linea generale *mission, vision* e *core value* rimangono stabili nel tempo e vengono riaffermati nella definizione della strategia. Potrebbero però anche subire dei cambiamenti per adattarsi al mutamento delle aspettative degli *stakeholder* o per decisione degli amministratori.

- **Strategia**

Con il termine "strategia" si fa riferimento ai piani che una società adotta per il conseguimento della propria *mission*, *vision* e *core value*.

L'ERM non definisce la strategia di una entità, ma influenza il suo sviluppo.

L'ERM supporta un'organizzazione nel comprendere con maggior chiarezza come definire strategia e obiettivi coerenti con la tipologia ed il livello dei rischi ritenuti accettabili rispetto alla propria *mission*, alla *vision* ed ai *core value*, elementi originari e fondanti dell'azione aziendale.

Aziende in cui *mission*, *vision* e *core value* siano ispirati ad una forte spinta all'innovazione o alla qualità dei propri prodotti definiranno strategie, obiettivi di *performance* e livelli accettabili di rischio in modo sostanzialmente diverso da aziende volte invece alla commercializzazione a prezzi competitivi di prodotti di qualità.

Fig. 1 – Integrazione di strategia, gestione del rischio e performance

Fonte: COSO – Enterprise Risk Management Integrating with strategy and performance

L'ERM supporta l'organizzazione nell'identificazione dei rischi associati alla strategia adottata ed, eventualmente, a strategie alternative. Nel valutare i rischi potenziali che possono derivare da una determinata strategia, il *management* considera anche le assunzioni critiche sottostanti. Il processo di *risk management* monitora e fornisce informazioni preziose sui cambiamenti nelle assunzioni e sui loro effetti sulla realizzazione della strategia.

Il perseguimento di ogni strategia comporta dei rischi che possono variare in funzione delle dinamiche di contesto. A volte il rischio diventa così rilevante che un'organizzazione potrebbe voler rivedere la strategia scelta o, eventualmente, sostituirla con un'altra connotata da un profilo di rischio più adatto.

Il rischio può anche essere esaminato in correlazione agli obiettivi caratterizzanti la strategia aziendale. Un'organizzazione può utilizzare più tecniche per valutare i rischi. Per quanto possibile, l'organizzazione dovrebbe utilizzare unità di misura dei rischi simili per ogni tipologia di obiettivo. Così facendo sarà possibile allineare la valutazione della gravità del rischio alla misurazione delle *performance* ed effettuare una corretta prioritizzazione.

- ***Business***

L'ERM deve essere integrato in tutti gli aspetti del *business*, dalla *governance* alla gestione delle *performance* ed al *controllo interno*.

Governance

La *governance* rappresenta un concetto ampio e fa riferimento alla distribuzione di ruoli, poteri e responsabilità tra gli *stakeholder*, il Consiglio di Amministrazione e il *management*. Alcuni aspetti della *governance* esorbitano dalla gestione del rischio, ad esempio la selezione dei membri del Consiglio di Amministrazione nonché la definizione della *mission*, della *vision* e dei *core value*.

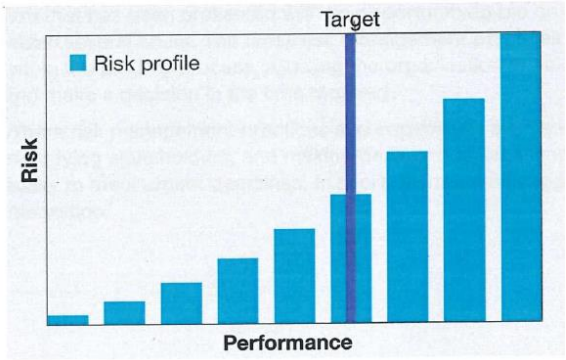
Performance

Valutare il rischio associato ad una strategia e agli obiettivi di *business*, richiede che un'organizzazione sia in grado di capire il legame tra rischio e *performance*, inteso

come "profilo di rischio". Il profilo di rischio di un'organizzazione fornisce una visione composita del rischio a un determinato livello organizzativo (ad es. una visione complessiva, di *business unit* o di funzione) oppure per area di *business* (ad es. prodotti, servizi, area geografica, ecc.). Questa visione permette al *management* di considerare la tipologia, la gravità e l'interdipendenza dei rischi e come questi abbiano impatto sulla *performance*. L'organizzazione dovrebbe comprendere il profilo di rischio potenziale già quando valuta strategie alternative. Scelta la strategia, il *focus* si sposta verso la comprensione del relativo profilo di rischio attuale.

Il rapporto tra rischio e *performance* è raramente lineare. Un eventuale miglioramento di *performance* non necessariamente si traduce in un cambiamento di pari effetto dei livelli di rischio e viceversa.

Nella figura a lato, ogni barra rappresenta l'ammontare aggregato del rischio per ogni specifico livello di *performance* associato a un obiettivo di *business*. La linea *target* rappresenta il livello di *performance* scelto dall'organizzazione nell'ambito della definizione della strategia, che viene comunicato attraverso un obiettivo e un *target* di *business*. Le organizzazioni possono sviluppare diversi approcci per concettualizzare e rappresentare il profilo di rischio dell'entità.



Controllo interno

L'ERM incorpora alcuni concetti del controllo interno inteso come il processo messo in atto dalla società per raggiungere una ragionevole *assurance* che gli obiettivi aziendali verranno conseguiti.

Il controllo interno supporta l'organizzazione nell'identificare e analizzare i rischi connessi al raggiungimento di quegli obiettivi e di come gestirli. Consente al *management* di restare focalizzato sul *business* e conseguire gli obiettivi rimanendo *compliant* alle leggi e regolamenti di riferimento. Si nota, comunque, che alcuni concetti relativi al *risk management* non sono considerati nell'ambito del controllo interno. Per esempio, i concetti di *risk appetite* e *risk tolerance*, strategia e obiettivi sono parte del *risk management*, ma sono considerati come precondizioni del controllo interno.

Per evitare ridondanze, alcuni concetti relativi al controllo interno che sono comuni a questa pubblicazione e all' "*Internal Control - Integrated Framework*" non sono qui ripetuti (ad esempio i rischi di frode relativi agli obiettivi della reportistica finanziaria, le attività di controllo riferite agli obiettivi di *compliance* e le valutazioni relative agli obiettivi operativi). Ad ogni modo alcuni concetti comuni al controllo interno sono ulteriormente sviluppati nella relativa sezione del presente *Framework* (per esempio il concetto di *governance*) e si raccomanda di considerare l'"*Internal Control - Integrated Framework*" come parte applicativa del presente *Framework*.

1.1 I benefici dell'*Enterprise Risk Management*

Integrare il *risk management* nella gestione del *business* consente il potenziamento della capacità di:

- aumentare le opportunità: questo beneficio sarà tanto più evidente quanto più il processo di gestione dei rischi interagirà con la definizione delle strategie;
- aumentare i risultati positivi riducendo gli imprevisti negativi: l'ERM migliora la capacità di anticipare l'identificazione dei rischi e di stabilire le risposte più adeguate;
- identificare e gestire i rischi dell'azienda nel suo complesso: a volte un rischio può originarsi in una parte dell'azienda, ma avere un impatto su un'altra parte. In quanto processo trasversale, l'ERM consente di veicolare le informazioni nella struttura aziendale e attivare il coordinamento delle azioni di mitigazione e monitoraggio;
- ridurre gli scostamenti nelle *performance*: la variabilità delle *performance* può rappresentare una minaccia significativa tanto quanto le potenziali perdite. L'ERM permette alle organizzazioni di anticipare i rischi che potrebbero avere un impatto sulle *performance* e le mette in grado di adottare azioni per minimizzare le inefficienze e i momenti di crisi;
- migliorare l'utilizzo delle risorse: disporre di informazioni documentate sui rischi permette al *management* di valutare le necessità complessive di risorse e di ottimizzarne l'allocazione;
- migliorare la capacità di adattarsi al cambiamento: in ambienti economici in evoluzione, l'identificazione tempestiva dei rischi e delle azioni di mitigazione consente al *management* di adattare la gestione del *business* ai cambiamenti del contesto, stimolando la ridefinizione della strategia.

Gestione integrata dell'ERM

Il successo di un'organizzazione è il risultato delle innumerevoli decisioni adottate dal *management* in un contesto dinamico di *business* e come *trade off* tra soluzioni alternative. Per questa ragione il *Framework* propone di integrare il *Risk Management* in ogni aspetto dell'operatività non potendo essere inteso come una sovrastruttura rispetto ai processi di *business*.

Punto di partenza per la realizzazione dell'integrazione dell'ERM nella strategia e nella *performance* aziendale potrebbe essere rappresentato dalla revisione di aspetti di *governance* quali la cultura, le competenze e le procedure aziendali.

Cultura

Per diffondere maggior trasparenza e consapevolezza del rischio all'interno dell'azienda, si richiedono azioni come:

- definire meccanismi utili per la condivisione di informazioni;
- stimolare le persone a superare le problematiche senza paura di ritorsioni;

- individuare e comunicare ai destinatari il proprio ruolo e le proprie responsabilità per il raggiungimento di strategie e obiettivi di *business*, incluse le responsabilità nella gestione del rischio;
- allineare *core value*, comportamenti e scelte agli incentivi e remunerazioni;
- sviluppare e diffondere una forte comprensione del contesto aziendale e dei *driver* di creazione di valore.

Competenze

Le competenze nella gestione del rischio aziendale sono integrate nell'organizzazione quando:

- il *management* è in grado di prendere decisioni appropriate in considerazione della propensione al rischio, del profilo di rischio e delle sue variazioni nel tempo;
- l'organizzazione assume abitualmente persone capaci e di esperienza che possono esercitare il giudizio e la supervisione in base alle loro responsabilità e a supporto del processo decisionale;
- si effettuano gli investimenti necessari in tecnologia o altre infrastrutture e la direzione considera gli strumenti necessari per attivare le responsabilità di gestione del rischio aziendale;
- fornitori, appaltatori e altre terze parti sono presi in considerazione nelle valutazioni su rischio e *performance*.

Procedure

Le procedure dell'ERM sono integrate quando:

- nella definizione delle strategie sono considerati i rischi associati alle diverse opzioni;
- il *management* indirizza attivamente il rischio nel perseguimento dei propri obiettivi di *performance*;
- le attività sono sviluppate per monitorare regolarmente e costantemente le *performance* e le variazioni del profilo di rischio;
- il *management* è in grado di prendere decisioni in linea con la velocità e la portata dei cambiamenti nell'organizzazione.

2. Componenti e principi dell'ERM

Il *Framework* COSO ERM introduce cinque componenti tra loro interconnesse ed esplicita i principi rilevanti di ciascuna. La figura 3.1 illustra le componenti e la loro relazione con la *mission*, la *vision* e i *core value*. Le componenti rappresentate nel nastro a tre colori (*Strategia e Definizione degli obiettivi*, *Performance* e *Review and Revision*) rappresentano i processi traversali che attraversano l'intera organizzazione. Le componenti rappresentate nel nastro a due colori (*Governance* e Cultura e

Informazione /Comunicazione e Reporting) rappresentano gli elementi di supporto alla gestione del rischio aziendale.

La figura illustra inoltre come il valore aumenti quando la gestione del rischio aziendale è integrata nello sviluppo della strategia, nella formulazione degli obiettivi di *business*, nell'operatività e nella *performance*. L'ERM non è statico, ma interagisce fortemente con le dinamiche del *business*.

Fig.2- Componenti dell'Enterprise Risk Management

Fonte: COSO – Enterprise Risk Management Integrating with strategy and performance

Le cinque componenti dell'ERM sono:

- *Governance & Culture (Governance e cultura)*: sono gli elementi portanti dell'ERM. La *governance* definisce il carattere dell'organizzazione, rafforzando l'importanza dell'ERM e stabilendo le responsabilità della sua supervisione. La cultura si riflette nel processo decisionale.
- *Strategy & Objective-setting (Strategia e definizione degli obiettivi)*: l'ERM è integrato nella definizione del piano strategico dell'azienda. Con la comprensione del contesto aziendale, l'organizzazione può acquisire una visione d'insieme dei fattori interni ed esterni e del loro effetto sul rischio. Un'organizzazione stabilisce la sua propensione al rischio in combinazione con la definizione della strategia. Gli obiettivi di *business* permettono di mettere in pratica la strategia e modellare le operazioni e le priorità quotidiane della società.
- *Performance*: un'organizzazione identifica e valuta i rischi che possono influenzare la sua capacità di raggiungere la strategia e gli obiettivi di *business*. Dà la priorità ai rischi in base alla loro gravità e in considerazione della sua propensione al rischio. L'organizzazione seleziona quindi le risposte al rischio e ne misura l'efficacia.
- *Review & Revision (Riesame e revisione)*: rivedendo le competenze e le procedure della gestione dei rischi e le *performance* conseguite rispetto agli obiettivi, un'organizzazione può valutare quanto l'ERM abbia contribuito ad aumentare il valore nel tempo.
- *Information, communication & reporting* (Informazione, comunicazione e rendicontazione)**:** la comunicazione è il processo continuo e iterativo per ottenere informazioni e condividerle in tutta l'organizzazione. Il *management*

utilizza informazioni rilevanti provenienti da fonti interne ed esterne per supportare la gestione del rischio. L'organizzazione sfrutta i sistemi informativi per acquisire, elaborare e gestire dati e informazioni.

Le cinque componenti sono declinate in principi che rappresentano le iniziative che le aziende dovrebbero implementare per la realizzazione di processi integrati di gestione del rischio.

Figura 3- Principi dell'ERM

Fonte: COSO – Enterprise Risk Management Integrating with strategy and performance

L''organizzazione dovrebbe valutare il proprio processo di gestione del rischio considerando se:

- le componenti e i principi dell'ERM sono presenti e funzionanti;
- le componenti dell'ERM operano insieme in modo integrato;
- i controlli necessari per l'attuazione dei principi rilevanti sono presenti e funzionanti.

3. L'applicazione dell'ERM ai c.d. rischi ESG

Nel mese di ottobre 2018 il *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) ha sviluppato, in collaborazione con il *World Business Council for Sustainable Development* (WBCSD), le linee guida "*Environmental, Social & Governance – Enterprise Risk Management. Applying enterprise risk management to environmental, social and governance related risks*" per l'applicazione *dell'Enterprise Risk Management* anche ai rischi *Environmental, Social & Governance* (di seguito "rischi ESG").

I rischi ESG riguardano tematiche:

- ambientali, come i cambiamenti climatici, l'inquinamento e la tutela delle risorse naturali;
- sociali, come la difesa dei diritti umani e delle condizioni di lavoro o i rapporti con le comunità locali;

- di *governance*, come le politiche di remunerazione, la composizione del consiglio di amministrazione, le procedure di controllo e i comportamenti in termini di rispetto delle leggi e della deontologia.

Se dei rischi di *governance* se ne parla da tempo, negli ultimi 10 anni è aumentata notevolmente l'attenzione di media e investitori verso i temi ambientali e sociali e quindi diventa sempre più importante gestire questi rischi, in considerazione anche di una normativa nazionale e internazionale sempre più orientata agli aspetti ESG[1].

Nel tempo, anche a fronte di episodi negativi che hanno coinvolto alcuni grandi *player*, è diventato sempre più chiaro che i temi ESG siano temi di *business*. Gli stessi investitori istituzionali dimostrano sempre più interesse verso investimenti responsabili e sul modo con cui le aziende si stiano rivolgendo ai cambiamenti sociali e ambientali per raggiungere una crescita sostenibile e di lungo periodo. Il tema ESG è stato affrontato anche a livello normativo. In questo quadro si inserisce il D.Lgs. 254/2016 che, introducendo il "*non financial reporting*", impone alle società quotate di grandi dimensioni[2] di comunicare annualmente, tra gli altri aspetti, rischi e politiche adottate in campo ambientale, sociale, del personale, del rispetto dei diritti umani e della lotta alla corruzione.

La crescente *disclosure* sui temi ESG evidenzia tuttavia la debolezza dell'approccio alla gestione dei rischi ESG rispetto alla gestione dei più convenzionali rischi operativi, strategici e finanziari. Le cause, secondo il WBCSD sono rinvenibili in:

- difficoltà a quantificare in termini monetari i rischi ESG, essendo rischi a lungo termine con impatti incerti;
- mancanza di conoscenza dei rischi ESG che caratterizzano un'azienda e la scarsità di collaborazione interfunzionale tra il *risk manager* e chi si occupa di sostenibilità;

---

[1] Annualmente, il *World Economic Forum* pubblica un *Report* basato sul sondaggio condotto tra esperti e *decision-maker* dei vari settori dell'economia globale sulla percezione dei rischi a livello internazionale. Nel *Global Risk Report* del 2018, solo uno dei cinque *Top Risk* era un rischio di natura sociale, ovvero il rischio di pandemie. Nel 2019, ben quattro dei cinque *Top Risk* hanno natura sociale o ambientale, ovvero:
- eventi meteorologici estremi,
- crisi idriche,
- disastri naturali,
- inadeguatezza delle misure per mitigare gli effetti dei cambiamenti climatici.

[2] Il D.Lgs. 254/2016 all'art. 2. Ambito di applicazione recita:

1. Gli enti di interesse pubblico redigono per ogni esercizio finanziario una dichiarazione conforme a quanto previsto dall'articolo 3, qualora abbiano avuto, in media, durante l'esercizio finanziario un numero di dipendenti superiore a cinquecento e, alla data di chiusura del bilancio, abbiano superato almeno uno dei due seguenti limiti dimensionali:

a) totale dello stato patrimoniale: 20.000.000 di euro;

b) i ricavi netti delle vendite e delle prestazioni: 40.000.000 di euro;

2. Gli enti di interesse pubblico che siano società madri di un gruppo di grandi dimensioni redigono per ogni esercizio finanziario una dichiarazione conforme a quanto previsto dall'articolo 4.

- i rischi ESG sono inoltre spesso gestiti da un *team* di specialisti e visti in maniera separata o comunque meno importanti rispetto ai rischi strategici, operativi e finanziari.

Le Linee Guida proposte da COSO e WBCSD, cui si rinvia, rappresentano, pertanto, uno strumento utile per l'azienda che intenda affrontare i rischi ESG a partire dalla definizione della propria strategia.

Le Linee Guida, pur rinviando ad altri *framework* specifici in materia di sostenibilità, ripropongono le 5 componenti e i 20 principi dell'ERM, come descritti nei successi capitoli, ma declinati specificatamente rispetto alle tematiche ESG, ovvero:

- *Governance & Culture*: aumentare la consapevolezza del *board* e del *management* sulle tematiche ESG, promuovendo la cultura della collaborazione tra funzioni;
- *Strategy & Objective*: anticipare gli impatti dei rischi ESG nel breve, medio e lungo termine già in fase di definizione della strategia e degli obiettivi di *business*;
- *Performance*: identificare, valutare i rischi ESG e le relative misure di trattamento in base alla gravità del rischio;
- *Review & Revision*: sviluppare indicatori che consentano di allertare il *management* di eventuali cambiamenti che impattano su rischi e misure di trattamento;
- *Information, Communication & Reporting*: identificare le informazioni da comunicare all'interno e all'esterno, coinvolgendo ogni livello dell'organizzazione.

Si rimanda ai capitoli successivi per l'approfondimento di ciascuna componente del *Framework* COSO ERM e dei relativi principi.

CAPITOLO I

GOVERNANCE AND CULTURE

1. Principio n. 1 – Esercitare il *Board Risk Oversight* – 2. Principio n. 2 – L'organizzazione istituisce strutture operative nel perseguimento della strategia e degli obiettivi di *business* – 3. Principio n. 3 – Definire la cultura desiderata – 4. Principio n. 4 – L'organizzazione dimostra *commitment* verso i valori fondamentali – 5. Principio n. 5 – L'organizzazione si impegna a costruire capitale umano in linea con la strategia e gli obiettivi di *business.*

***

La *Governance* è l'insieme dei processi che assicurano l'efficienza e l'efficacia delle organizzazioni di qualsiasi tipo, presidiando le strutture e la cultura necessarie per la definizione degli obiettivi dell'organizzazione e delle modalità di raggiungimento degli stessi, anche attraverso l'identificazione di tutti i rischi ad essi associati.

Il COSO ERM *Framework* sottolinea che una *Governance* adeguata è un requisito essenziale per l'identificazione, la valutazione, il monitoraggio ed il presidio di tutti i rischi delle organizzazioni.

La "*Governance & Culture*" è la componente trasversale dell'*Enterprise Risk Management*: la cultura si riflette nei processi decisionali e la *Governance* definisce il livello di *commitment* rispetto all'*Enterprise Risk Management*, rafforzandone la rilevanza e identificandone i ruoli e le responsabilità di supervisione, nonché stabilendo le modalità con cui devono essere prese le decisioni e le modalità di esecuzione delle stesse.

***

1. Principio n. 1 – Esercitare il *Board Risk Oversight*

L'organo di governo deve supervisionare il raggiungimento della strategia, supportando il *management* nel raggiungimento degli obiettivi strategici e di *business*.

Di seguito si riportano le specifiche componenti da valutare.

Responsabilità e affidabilità

L'organo di governo, in quanto responsabile primario della gestione del rischio all'interno dell'organizzazione, interviene nella definizione degli obiettivi aziendali e delle linee di indirizzo, lasciando al *management* le responsabilità operative della gestione dei rischi e dell'implementazione delle linee di azione.

È prassi comune sviluppare un documento che definisca formalmente le rispettive responsabilità in tema di gestione del rischio.

Competenza, esperienza e conoscenza del *business*

L'organo di governo deve essere composto da membri con adeguate conoscenze e competenze, e deve valutare periodicamente la propria adeguatezza rispetto al proprio ruolo di supervisione del rischio aziendale; nel caso in cui si riscontrino carenze in alcune competenze specialistiche deve fare riscorso a competenze di consulenti indipendenti.

Indipendenza

L'organo di governo dovrebbe essere indipendente al fine di garantire imparzialità nelle valutazioni e nel processo decisionale senza alcun conflitto di interesse e sorvegliando l'effettiva gestione dell'organizzazione nell'interesse dei propri *stakeholder*.

Adeguatezza dell'*Enterprise Risk Management*

L'organo di governo deve avere consapevolezza della complessità dell'organizzazione e del modo in cui l'integrazione delle capacità e delle pratiche di gestione del rischio siano in grado di apportare valore. L'organo di gestione deve interfacciarsi costantemente con il *management* per determinare se la gestione del rischio d'impresa è adeguatamente progettata per apportare valore.

Orientamento organizzativo

È di fondamentale importanza comprendere le modalità con cui gli orientamenti organizzativi influenzano le decisioni connesse allo sviluppo del sistema di *Enterprise Risk Management* e le relative modalità di gestione.

2. Principio n. 2 – L'organizzazione istituisce strutture operative nel perseguimento della strategia e degli obiettivi di *business*

La struttura operativa indica le modalità secondo cui devono essere svolte le operazioni quotidiane all'interno dell'organizzazione, anche con riferimento alle pratiche di gestione del rischio. Tutto il personale è responsabile dello sviluppo e dell'implementazione delle pratiche di gestione del rischio e del mantenimento dei valori fondamentali nell'organizzazione.

Di seguito si riportano le specifiche componenti da valutare.

Strutture operative e linee di riporto

Ogni organizzazione ha una propria struttura operativa e proprie linee di riporto per la realizzazione della strategia e degli obiettivi di *business*. Strutture operative diverse danno luogo a diversi profili di rischio e influiscono sulle pratiche di gestione degli stessi. Nella definizione o nella valutazione di una struttura operativa è importante considerare i fattori che possono riguardare, a titolo esemplificativo: la strategia e gli obiettivi di *business* dell'organizzazione, la natura, le dimensioni e la distribuzione geografica dell'attività, il rischio connesso alla strategia e agli obiettivi aziendali oltre che i requisiti finanziari, fiscali e normativi.

Strutture di *Enterprise Risk Management*

Il *management* è responsabile della pianificazione, organizzazione e realizzazione della strategia e degli obiettivi di *business* in accordo con la *mission*, la *vision* e i *core values* dell'organizzazione. Di conseguenza, il *management* ha bisogno di ricevere indicazioni sulle modalità con cui il rischio associato alla strategia si può presentare. Un metodo usato per raccogliere tali informazioni è, per esempio, quello di delegare la responsabilità ad un comitato, i cui membri sono in genere Amministratori o appartenenti al *senior management.*

Autorità e responsabilità

L'organo di governo delega al *management* il compito di progettare e attuare pratiche che supportano il raggiungimento della strategia e degli obiettivi aziendali. A sua volta, in linea con le indicazioni ricevute, il *management* definisce ruoli e responsabilità per l'organizzazione e per le unità operative, organizzando le responsabilità e i compiti per consentire al personale di prendere decisioni. Periodicamente, l'organo di governo deve valutare l'adeguatezza della struttura riducendo o aggiungendo livelli e revisionando le deleghe di responsabilità e compiti.

Enterprise Risk Management e i contesti in evoluzione

L'evoluzione di un'organizzazione dipende anche dalla capacità di apportare valore attraverso l'*Enterprise Risk Management*.

La struttura operativa e le modalità di gestione dei rischi evolvono con i cambiamenti della natura del *business* e della sua strategia, pertanto il *management* deve valutare con regolarità l'adeguatezza delle stesse.

3. Principio n. 3 – Definire la cultura desiderata

L'organizzazione definisce i comportamenti attesi che caratterizzano la cultura desiderata.

Di seguito si riportano le specifiche componenti da valutare.

Cultura e comportamenti attesi

La cultura di un'organizzazione deriva dai suoi valori fondamentali, dai comportamenti attesi e dalle decisioni che vengono prese. Essa influenza le modalità con cui l'organizzazione identifica e gestisce i rischi, in relazione ai livelli di tolleranza accettati. L'organo di governo ed il *management* definiscono la cultura desiderata dell'organizzazione e le modalità di trasmissione agli individui. I valori societari devono guidare i comportamenti attesi nel processo decisionale quotidiano al fine di soddisfare le aspettative degli *stakeholder*.

Applicazione del giudizio

Il giudizio è funzione dell'esperienza personale, della propensione al rischio, delle capacità e del livello di informazione disponibile.

L'uso del giudizio influenza la capacità di un'organizzazione di gestire i periodi di crisi e riprendere il normale funzionamento in modo più efficiente. Le organizzazioni che hanno esperienza, capacità consolidate e una giusta propensione al rischio esercitano l'utilizzo del giudizio con maggiore chiarezza.

L'effetto della cultura

La cultura di un'organizzazione influenza il modo in cui il rischio viene identificato, valutato e presidiato dal momento della definizione della strategia all'esecuzione delle attività e alla valutazione delle *performance*. A titolo esemplificativo, la cultura può influenzare non solo le scelte strategiche, ma anche il modo in cui si valuta la natura e la tipologia dei rischi e delle opportunità che si presentano.

Allineare i valori fondamentali, il processo decisionale e i comportamenti

La capacità di raggiungere con successo la propria strategia e gli obiettivi di *business* è ostacolata quando i comportamenti e le decisioni dell'organizzazione non sono in linea con i valori attesi. Il disallineamento può causare una perdita di fiducia da parte degli *stakeholder* o prestazioni inferiori a quanto previsto. A titolo esemplificativo, la mancata o errata trasmissione delle aspettative a tutta l'organizzazione e il mancato o errato controllo da parte degli organi di governo circa il rispetto degli standard di comportamento da parte del *management* possono influenzare il rispetto dei valori fondamentali.

Il cambiamento culturale

La cultura aziendale evolve nel tempo. I cambiamenti interni e le influenze esterne possono provocare un cambiamento culturale che influenzerà il modo in cui l'organizzazione valuta i rischi e le modalità con cui vengono prese le decisioni.

4. Principio n. 4 – L'organizzazione dimostra *commitment* verso i valori fondamentali

L'organizzazione definisce la propria struttura e i flussi informativi interni ed esterni in coerenza con i valori fondamentali adottati.

Di seguito si riportano specifici aspetti che dovrebbero essere considerati ed assicurati.

Riflettere i valori fondamentali in tutta l'organizzazione

I valori fondamentali si riflettono nelle azioni e nelle decisioni all'interno dell'organizzazione.

Il suo *management* ha la responsabilità di favorire una comprensione comune dei valori fondamentali, dei *driver* di *business* e dei comportamenti attesi dal personale e dalle terze parti. La condivisione dei valori dell'organizzazione con i propri dipendenti supporta il perseguimento della strategia e degli obiettivi aziendali.

Adottare una cultura consapevole dei rischi

Il *management* deve definire le caratteristiche necessarie all'ottenimento e al mantenimento nel tempo della cultura desiderata; l'organo di governo deve supervisionare il rispetto di tali caratteristiche. Fattori che possono favorire una cultura consapevole dei rischi possono essere, a titolo esemplificativo: una forte *leadership*, uno stile di *management* partecipativo, l'integrazione dell'analisi dei rischi nel processo decisionale o il favorire discussioni aperte e oneste sui rischi cui è esposta l'organizzazione.

Formalizzare la responsabilità

L'organo di governo supervisiona la corretta gestione del rischio attraverso l'implementazione dell'*Enterprise Risk Management* e supporta il *management* nel raggiungimento della strategia degli obiettivi strategici e di *business*. L'organo di governo e il *management* sono responsabili dell'*accountability* – dalla progettazione iniziale alla valutazione periodica – della cultura e delle capacità di gestione del rischio aziendale.

Assunzione di responsabilità

In alcune organizzazioni, gli obiettivi di *performance* sono individuati dall'organo di governo e declinati verso il *management* ed il personale. Ad ogni livello, è valutata l'adesione ai valori fondamentali e la conformità ai comportamenti attesi e possono essere assegnati premi o applicate azioni disciplinari. L'organo di governo può anche condurre un'autovalutazione per valutare i propri punti di forza ed individuare le opportunità di miglioramento in relazione all'*Enterprise Risk Management*.

Favorire una comunicazione aperta e senza ritorsioni

Il *management* deve favorire una comunicazione aperta e trasparente nell'ambito della gestione dei rischi, sottolineando le responsabilità comuni quotidiane e l'importanza per il successo e la sopravvivenza dell'organizzazione. L'organizzazione che favorisce una comunicazione aperta e trasparente deve prevedere una varietà di canali comunicativi per le segnalazioni di non conformità alle regole definite.

Rispondere alle deviazioni dai valori e dai comportamenti fondamentali

L'organizzazione deve inviare messaggi chiari sui comportamenti accettati e su quelli da evitare e deve tempestivamente identificare e sottoporre a specifiche azioni correttive eventuali violazioni dei principi etici e dei comportamenti attesi. Le azioni correttive devono essere determinate dal *management* in coerenza con le prescrizioni legislative e gli standard di condotta.

5. Principio n. 5 – L'organizzazione si impegna a costruire capitale umano in linea con la strategia e gli obiettivi di *business*

L'organizzazione deve supportare la propria strategia e il raggiungimento dei propri obiettivi di *business* attraverso adeguati strumenti di creazione e mantenimento del proprio capitale umano.

Di seguito si riportano specifici aspetti che dovrebbero essere considerati.

Definire e valutare le competenze necessarie

Il *management*, con la supervisione dell'organo di governo, definisce il capitale umano necessario per la realizzazione della strategia e degli obiettivi aziendali. Qualora siano identificate aree di debolezza, la funzione risorse umane supporta il *management* nell'individuazione delle competenze necessarie al raggiungimento degli obiettivi.

Attrarre, sviluppare e trattenere le persone

Il *management*, per ciascun livello e competenza, deve presidiare i processi per attrarre, formare, indirizzare, valutare e trattenere le migliori persone all'interno dell'organizzazione.

Premiare le *performance*

La *performance* è fortemente influenzata dalle modalità in cui le persone sono ritenute responsabili e dal modo in cui sono ricompensate. Spetta al *management* e all'organo di governo stabilire incentivi e altre ricompense coerenti con il ruolo ricoperto nell'organizzazione, considerando il raggiungimento di obiettivi aziendali sia nel breve che nel lungo periodo.

Gestire la pressione

Diversi sono i fattori che generano pressione in un'organizzazione. Gli obiettivi che il *management* stabilisce per il raggiungimento della strategia possono creare pressione nel personale. La pressione può anche manifestarsi durante lo svolgimento di determinati compiti (es. gestione di negoziazioni) o essere autoimposta. Le organizzazioni possono influenzare positivamente la pressione sia riequilibrando i carichi di lavoro sia aumentando il numero e la qualità delle risorse allocate.

Pianificare la successione

Il *management* e l'organo di governo devono predisporre piani di successione per l'assegnazione delle responsabilità chiave in tema di *Enterprise Risk Management*. In particolare, devono essere definiti piano di successione per i dirigenti chiave e devono essere formati i candidati alla successione.

CAPITOLO II

STRATEGY AND OBJECTIVE SETTING

1. Principio n. 6 – L'analisi del Contesto aziendale – 2. Principio n. 7 – La definizione di "*risk appetite*" (o propensione al rischio) – 3. Principio n. 8 – La valutazione delle strategie alternative – 4. Principio n. 9 – La formulazione degli obiettivi aziendali.

***

Ogni organizzazione definisce una strategia per realizzare la propria *mission* e per generare valore. Definire una strategia in linea con la *mission*, la *vision* e *core value* della società rappresenta un'attività articolata e complessa. L'integrazione della gestione del rischio aziendale nel processo di definizione della strategia permette di identificare il profilo di rischio associato alla strategia stessa ed agli obiettivi aziendali e, conseguentemente, di calibrare le azioni necessarie per perseguirli.

***

1. Principio n. 6 – L'analisi del Contesto aziendale

Un'organizzazione considera il contesto aziendale di riferimento quando sviluppa le strategie per il perseguimento della sua *mission*, secondo la propria *vision* ed i suoi *core value*. Con il termine "contesto aziendale" si fa riferimento agli andamenti delle variabili rilevanti, di natura esogena ed endogena all'azienda, che possono influenzare le strategie attuali e future di un'organizzazione.

Il contesto aziendale ha tre principali caratteristiche:

- Dinamicità: in qualsiasi momento può emergere un potenziale rischio per l'azienda che rompe gli equilibri esistenti sino a quel momento;
- Complessità: il contesto aziendale è costituito da una fitta rete di interconnessioni e interdipendenze;
- Imprevedibilità: ogni cambiamento avviene rapidamente e senza preavviso.

L'ambiente esterno

L'ambiente esterno è una delle componenti del contesto in cui un'azienda opera e coinvolge gli *stakeholder* (cioè i diversi portatori di interessi) non appartenenti all'azienda che possono influenzare il raggiungimento degli obiettivi aziendali.
Gli *stakeholder* esterni (come i clienti, i fornitori ed i *competitors*) non sono soggetti direttamente coinvolti nelle decisioni aziendali ma possono essere influenzati dalle

stesse, influenzare a loro volta l'ambiente nel quale opera l'azienda (governo, legislazione ecc.), oppure possono avere la capacità di incidere sulla reputazione aziendale e sulla percezione del brand. Un'organizzazione capace di identificare i fattori esterni e gli *stakeholder* ha maggiori possibilità di anticipare il cambiamento e adattarsi più rapidamente. L'ambiente esterno è caratterizzato da molteplici fattori che possono essere classificati in diverse categorie, quali ad esempio: politici, economici, sociali, tecnologici, legali, ambientali.

L'ambiente interno

L'ambiente interno di un'organizzazione è definito come l'insieme degli elementi interni che possono influenzare anch'essi il conseguimento degli obiettivi aziendali. Gli *stakeholder* interni sono soggetti che lavorano per l'organizzazione e possono influire direttamente sulle decisioni aziendali (gli amministratori, il *management*, etc.). Come per l'ambiente esterno, anche i fattori che compongono l'ambiente interno possono essere suddivisi in diverse categorie, quali ad esempio: capitale, risorse umane, processi e tecnologia.

Come il contesto aziendale influenza i profili di rischio

È possibile osservare gli effetti che il contesto aziendale determina sul profilo di rischio in tre diversi momenti: *a)* ***passato*** - tramite l'analisi delle *performance* realizzate in precedenza un'organizzazione può calibrare il suo profilo di rischio; *b)* ***presente*** - mediante la valutazione delle *performance* attuali l'organizzazione può comprendere come i trend di mercato, le relazioni economiche e gli altri fattori influenzano il profilo di rischio; *c)* ***futuro*** - facendo delle previsioni su come il contesto aziendale evolverà, l'azienda è in grado di definire in anticipo come il profilo di rischio impatterà sui risultati economici, finanziari e patrimoniali.

2. Principio n. 7 - La definizione di "*risk appetite*" (o propensione al rischio)

Le decisioni che riguardano le strategie aziendali e la definizione della propensione al rischio non possono essere standardizzate, poiché non esiste una propensione al rischio universalmente applicabile a qualsiasi soggetto economico.
Tuttavia, indipendentemente da come vengono assunte le decisioni, un'organizzazione dovrebbe identificare preliminarmente la sua propensione al rischio basandosi sulla propria *mission*, sulla visione d'impresa, condizionata anche dal contesto in cui opera, al fine di creare, preservare e incrementare valore. La propensione al rischio viene nel tempo calibrata e riadattata ogni qual volta vengano valutate strategie alternative e definiti gli obiettivi per raggiungere i livelli di *performance* desiderati.
Lo sviluppo di una efficace propensione al rischio si basa sulla ricerca dell'equilibrio ottimale tra rischio e opportunità e, quindi, un'organizzazione generalmente si impegna a mantenere la propensione al rischio al di sotto delle sue capacità di assumere rischi ("*risk tolerance*"), anche se in rare situazioni un'organizzazione può

scegliere di farlo, ad es. nei casi in cui si assume un livello di rischio tale da poter compromettere la capacità di assolvere alle proprie obbligazioni se la possibilità di successo è in grado di apportare un considerevole contributo in termini di valore/rendimento all'organizzazione. In questi casi il *management* è chiamato a riconsiderare le pratiche di *business* adottate, rivedere i limiti definiti ed ottenere l'approvazione dell'organo amministrativo.

Il *management* e il Consiglio di Amministrazione individuano la propensione al rischio analizzando tutti gli elementi pro e contro. Possono essere adottati diversi approcci, tra cui una revisione degli obiettivi di *performance* passati e attuali al fine di prevedere quelli futuri.

Alcune entità considerano la propensione al rischio in termini qualitativi, mentre altre preferiscono utilizzare parametri quantitativi, spesso concentrandosi sul bilanciamento di crescita, rendimento e rischio. La scelta di utilizzare parametri qualitativi e/o quantitativi dipende dal livello di maturità della società, dalla sensibilità interna alla tematica, dalle informazioni disponibili e dalle aspettative del Consiglio di Amministrazione.

La società può tuttavia prendere in considerazione una serie di parametri per definire la propria propensione al rischio in maniera più precisa e sofisticata. Ad esempio, ci si può riferire a:

- Parametri strategici, come i nuovi prodotti da portare sul mercato, gli investimenti da sostenere, le operazioni straordinarie da realizzare.
- Parametri finanziari, come il massimo livello accettabile sulla variazione delle *performance* finanziarie, o alcuni indici di bilancio, quali il ROA, il ROE, il rapporto tra debito e patrimonio netto.
- Parametri operativi, come il rispetto dei requisiti ambientali, di sicurezza, qualità, la concentrazione dei clienti, etc..

Un'organizzazione può declinare la propensione al rischio a livello di:

- Strategie e obiettivi aziendali allineati con la *mission*, la visione e i valori fondamentali.
- Obiettivi di *business*.
- Obiettivi di *performance*.

La propensione al rischio è proposta dal *management*, approvata dal Consiglio di Amministrazione e diffusa in modo capillare in tutta l'organizzazione. Diffondere la sensibilità sulla propensione al rischio è importante in modo che tutti i responsabili decisionali operino coerentemente con la propensione al rischio stabilita.

Il *management*, con la supervisione del Consiglio di Amministrazione, monitora continuamente la propensione al rischio su tutti i livelli organizzativi contribuendo a diffondere in tal modo una cultura basata sull'ottimizzazione dell'assunzione e gestione dei rischi entro i limiti stabiliti.

3. Principio n. 8 – La valutazione delle strategie alternative

La valutazione dei possibili scenari alternativi è parte integrante del processo di definizione della strategia da adottare per un'impresa. Una volta individuati i possibili scenari alternativi, ogni scenario dovrebbe essere valutato considerando le risorse e le capacità a disposizione dell'organizzazione, in modo da considerare la valutazione dei rischi e delle opportunità di ciascuna opzione ed effettuare la scelta della strategia più adatta a creare e preservare valore.

Nel considerare i possibili scenari alternativi, l'organizzazione identifica e valuta i potenziali rischi e le opportunità, in quanto diverse strategie producono diversi profili di rischio. Una volta definito il profilo di rischio relativo alla strategia scelta, il *management* sarà in grado di determinare le risorse necessarie e la loro allocazione, al fine di portare a compimento la strategia scelta.

Gli approcci più diffusi per la valutazione delle strategie alternative sono la SWOT *analysis*, la previsione dei ricavi, l'analisi dei *competitors* e la "*scenario analysis*".

Una volta definita la strategia, un'azienda può determinare gli effetti che si determinano al modificarsi degli elementi (variabili) di riferimento e le conseguenti modalità di gestione e monitoraggio.

4. Principio n. 9 – La formulazione degli obiettivi aziendali

Un'organizzazione è tenuta a considerare la componente rischio anche durante il processo di definizione e attribuzione degli obiettivi aziendali ai vari livelli dell'organizzazione, al fine di assicurare l'allineamento con la strategia definita. Gli obiettivi aziendali devono essere specifici, misurabili e funzionali alla realizzazione della strategia.

L'allineamento degli obiettivi di *business*

L'allineamento degli obiettivi di *business* alla strategia supporta l'organizzazione nel conseguimento della propria *mission*. Se tale allineamento non viene realizzato, o è solo parziale, possono insorgere dei rischi di inefficiente utilizzo delle risorse.
Gli obiettivi aziendali dovrebbero anche essere coerenti con la propensione al rischio dell'organizzazione. In caso contrario, l'organizzazione potrebbe accettare rischi eccessivi o troppo ridotti. Pertanto, quando un'organizzazione valuta un obiettivo aziendale, deve considerare i potenziali rischi che possono manifestarsi e determinare l'impatto presumibile sul profilo di rischio.

La definizione degli obiettivi di *business* e dei *target* di *performance*

Gli obiettivi, oltre ad essere coerenti con la strategia perseguita e con la propensione al rischio, devono poter essere osservati e misurabili.
A titolo esemplificativo, gli obiettivi aziendali possono riguardare:

- *Performance* finanziaria: mantenere profittabilità in tutti i *business* dell'azienda;

- Aspirazioni dei clienti: istituire centri di assistenza per i clienti in luoghi di facile accesso;
- Eccellenza operativa: attivare contratti di lavoro competitivi per attrarre e trattenere i dipendenti;
- Obblighi di conformità: rispettare le leggi applicabili in materia di salute e sicurezza sui luoghi di lavoro;
- Recuperi di efficienza: operare in un ambiente ad alta efficienza energetica;
- *Leadership* dell'innovazione: guidare l'innovazione nel mercato con frequenti lanci di nuovi prodotti.

Per supportare il raggiungimento degli obiettivi di *business*, l'organizzazione individua dei "*target*" utili a monitorare la propria *performance*.

La misurazione della *performance* in relazione ad un obiettivo aziendale può essere sia di tipo quantitativo che qualitativo, ed è utilizzata al fine di verificare che le prestazioni rientrino in un "*range*" di tolleranza stabilito.

Il livello di tolleranza considera le variazioni della *performance* sia in positivo che in negativo rispetto agli obiettivi di *business*: superare un obiettivo di solito indica efficienza o buone prestazioni, non semplicemente che si stia realizzando un'opportunità.

In ogni caso la tolleranza è fortemente influenzata dall'appetito al rischio, minore è l'appetito più stretta sarà la tolleranza rispetto al risultato atteso. Altro aspetto da considerare è costituito dalla correlazione tra tolleranza e costo: in generale, infatti, quanto più ridotti sono i margini di tolleranza tanto maggiori sono i costi da sostenere per operare assicurando determinati livelli di prestazione.

CAPITOLO III

PERFORMANCE

1. Principio n. 10 – L'identificazione dei rischi – 2. Principio n. 11 – La valutazione della gravità dei rischi – 3. Principio n. 12 – La prioritizzazione dei rischi – 4. Principio n. 13 – L'implementazione delle risposte ai rischi – 5. Principio n. 14 – Lo sviluppo di una visione d'insieme dei rischi.

***

L'Enterprise Risk Management sottolinea l'esigenza di adottare una visione dei rischi olistica (ossia d'insieme, a livello aziendale ed in ottica di integrazione/correlazione). I singoli rischi possono infatti avere effetti su più obiettivi di *business* così come i singoli obiettivi possono subire le conseguenze di diversi rischi: un'oculata gestione del rischio nel suo complesso è quindi più efficace ed efficiente di una gestione dei singoli rischi a livello di singola unità di *business* e può richiedere risposte a diversi livelli dell'organizzazione.

L'approccio operativo sotteso all'implementazione di un processo di ERM è orientato ad assicurare che i rischi siano identificati, valutati ed indirizzati nel contesto della strategia e degli obiettivi aziendali di un'organizzazione e che il *framework* sottostante sia progettato e implementato a supporto di tali obiettivi, tenuto conto della propensione al rischio dell'azienda.

L'organizzazione, nel prendere decisioni finalizzate al perseguimento della strategia ed il raggiungimento degli obiettivi di *business*, dovrebbe:

- identificare i rischi nuovi ed emergenti, affinché siano tempestivamente definite e sviluppate specifiche risposte;
- valutare la gravità dei rischi, sulla base di approcci qualitativi o quantitativi e avendo una conoscenza di come la tipologia e la natura di ogni rischio può cambiare a seconda del livello a cui viene effettuata la valutazione;
- prioritizzare i rischi sulla base di metriche rilevanti per l'organizzazione, al fine di allocare in maniera ottimale ed efficiente le risorse aziendali disponibili;
- identificare e selezionare le risposte ai rischi più appropriate;
- sviluppare una visione d'insieme dei rischi, per migliorare la capacità dell'organizzazione di assumere, gestire ed indirizzare i rischi nella loro complessità ai fini del perseguimento della strategia e degli obiettivi aziendali, grazie ad un approccio integrato.

L'attuazione di queste fasi comporta una gestione dei rischi dinamica, interattiva e consapevole, che richiede il coinvolgimento e la responsabilità dell'intero *management* e che sia coerente con la propensione e la tolleranza al rischio dell'impresa.

1. Principio n. 10 – L'identificazione dei rischi

I rischi sono presenti in tutte le attività aziendali. L'obiettivo dell'identificazione dei rischi è *in primis* quello di individuare i rischi nuovi, emergenti o differenti rispetto a quelli già noti all'organizzazione che possono impattare sul raggiungimento della strategia e degli obiettivi aziendali. I rischi devono essere identificati a livello di unità, divisione, attività operativa e società nel suo complesso. Questa fase rappresenta un passaggio critico nell'intero processo in quanto un'analisi incompleta o intempestiva può compromettere l'efficacia delle contromisure necessarie per il loro contenimento e da ultimo il raggiungimento degli obiettivi prefissati.

L'identificazione dei rischi nuovi e emergenti ed i cambiamenti nei rischi esistenti dovrebbe comprendere tutte le attività finalizzate ad identificare quei fattori o eventi interni (ad esempio cambiamenti negli obiettivi di *business* o del contesto di riferimento, personale, infrastrutture e risorse finanziarie, fenomeni sconosciuti in precedenza) ed esterni all'organizzazione (ad esempio nuove regolamentazioni, evoluzione della tecnologia, riduzione della disponibilità di materie prime e risorse naturali, cambiamenti ambientali, politici e sociali, mutamenti nelle caratteristiche della forza lavoro) che possono incidere significativamente sull'implementazione della strategia o sul conseguimento degli obiettivi. Il relativo aggiornamento dovrebbe essere correlato con la rapidità di cambiamento del contesto di riferimento e l'evoluzione organizzativa e di *business*, nonché in relazione a modifiche inerenti alla strategia e agli obiettivi aziendali.

A diversi livelli dell'organizzazione e secondo un approccio *top-down*, il *management,* ciascuno per la propria funzione o unità dovrebbe procedere ad una mappatura dei rischi (cd. "inventario dei rischi" o *risk inventory*). Tale fase richiede il coinvolgimento di appropriati livelli di *management*, ognuno per il proprio ambito di competenza affinché si abbia una comprensione quanto più completa di tutti i rischi rilevanti (es. apposite funzioni di secondo livello, quali *risk management, compliance*, ecc., ove definite).

L'inventario dei rischi rappresenta sostanzialmente un elenco di tutti i rischi che l'organizzazione deve fronteggiare, a livello di singola unità di *business* o di entità nel suo complesso, con differente impatto sulla strategia aziendale, rilevanti se valutati singolarmente o in loro aggregazioni. Anche tenendo conto della numerosità dei rischi identificati, l'inventario dei rischi può essere strutturato per categorie (es. rischi strategici, operativi, finanziari e di conformità) e sottocategorie e può includere anche l'impatto di ciascun rischio, le azioni di mitigazione e il *risk owner*.

Il risultato di questa mappatura non è statico, ma richiede una costante rielaborazione al fine di renderlo il più completo possibile e aggiornato.

L'identificazione dei rischi può avvenire nello svolgimento di attività ordinarie come i processi di *budgeting* e *business planning*, le *performance review* o lo svolgimento di *meeting*, nel processo autorizzativo per il lancio di nuovi prodotti, ovvero nell'ambito della gestione di reclami a clienti, perdite finanziarie o incidenti ma può essere integrata anche da momenti/attività addizionali come il completamento di questionari e lo svolgimento di *workshop*, anche corroborati dalla raccolta e dall'analisi di dati.

In ogni caso, indipendentemente dagli approcci scelti per l'identificazione dei rischi, oltre a tenere in considerazione i dati storici, è fondamentale procedere ad un'analisi prospettica del rischio, considerando anche gli eventuali cambiamenti nelle ipotesi sottostanti la strategia e gli obiettivi di *business*.

Qualsiasi rischio identificato deve essere considerato, descritto e inquadrato nel contesto di quale sarà l'impatto sulla strategia e *performance* aziendali, tenendo conto delle possibili implicazioni e interdipendenze degli accadimenti correlati.

Per una corretta gestione dei rischi è quindi particolarmente importante anche una loro corretta definizione/descrizione, che si focalizzi sul rischio in quanto tale e non si confonda/esaurisca con le potenziali cause, gli impatti dell'accadimento dell'evento o gli effetti di una risposta al rischio non propriamente implementata[3].

2. Principio n. 11 – La valutazione della gravità dei rischi

Un'efficace gestione dei rischi richiede un bilanciamento costante tra esposizione/propensione al rischio, costi e benefici attesi. Per tale motivo, il *management* valuta la gravità dei rischi come base per la definizione delle priorità di intervento e delle misure da adottare al fine di massimizzare i vantaggi strategici, finanziari e operativi dell'organizzazione stessa.

Valutare i rischi significa determinare il livello di gravità di ciascuno in funzione della loro natura e tipologia ossia misurare l'incidenza (o impatto) di un evento potenziale - inatteso e/o possibile - sul conseguimento delle *performance* aziendali attese.

La valutazione della gravità del rischio indirizza le azioni di risposta (trattamenti) allo stesso: se i rischi non sono valutati e misurati opportunamente, non sarà possibile giungere ad una decisione di trattamento adeguata, con possibili conseguenze in termini di allocazione non ottimale di risorse e possibile perdita del valore.

Il livello di gravità dei rischi può essere misurato in diversi modi, tenendo in considerazione le dimensioni, la natura e la complessità dell'azienda e il *risk appetite*, ossia il livello di rischio ritenuto accettabile dalla stessa. In ogni caso, le soglie dovrebbero essere fissate in misura differente a seconda che la valutazione sia effettuata a livello di *business unit* o di azienda nel suo complesso. In questo contesto, compito del *management* è quello di comprendere quali siano le caratteristiche degli eventi, le possibili conseguenze e la frequenza del loro manifestarsi.

In ogni caso, il *management* dovrebbe valutare ciascun rischio secondo due prospettive:

---

[3] Un'appropriata descrizione dei rischi dovrebbe articolarsi alternativamente come segue: a) la possibilità che [descrizione dell'accadimento] e gli associati impatti su [obiettivi dell'organizzazione], oppure b) il rischio di [categoria definita dall'organizzazione] relativo a [descrizione dell'accadimento] e [descrizione impatto].

- l'impatto, ossia il risultato o possibile effetto che il manifestarsi dell'evento può avere sul perseguimento degli obiettivi e sulla strategia aziendale;
- la probabilità, ossia la possibilità di accadimento, che può essere espressa in termini quantitativi, qualitativi o di frequenza di manifestazione dell'evento.

Assume rilievo anche l'orizzonte temporale scelto per la valutazione dei rischi, che deve essere uguale a quello identificato per determinare la strategia e gli obiettivi così da indentificare e valutare tutti i rischi che possono presentarsi nel periodo.

Nell'ambito del processo di valutazione del rischio, gli approcci più comunemente utilizzati sono i metodi qualitativi, quantitativi (monetari o non monetari) o, in alternativa, una combinazione di questi[4] e tengono conto del fatto che i rischi si possano manifestare contestualmente o in momenti successivi.

Un opportuno processo di valutazione del livello di gravità dei rischi non può prescindere dal considerare specifiche viste quali il "rischio inerente", il "rischio residuo *target*" e il "rischio residuo reale"[5].

La conoscenza e consapevolezza da parte del *management* del valore di queste dimensioni, ed in generale del profilo di rischio della propria organizzazione, può facilitare una gestione integrata ed interattiva dei rischi, finalizzata ad individuare quelli su cui sono state allocate risorse in maniera non ottimale (risposte al rischio non necessarie o ridondanti), nonché di definire le azioni che permettano al *management* di modificare il livello di significatività del rischio.

Dopo aver individuato i rischi (inventario dei rischi o *risk register*) e averne misurato il livello di significatività, coerentemente con il profilo di rischio dell'organizzazione, i relativi risultati possono essere rappresentati tramite una matrice (quella più comunemente usata è la matrice impatto-probabilità, cd. *heat map*) o altra rappresentazione grafica per evidenziare in modo immediato il livello di gravità associato a ciascuno dei rischi in relazione al raggiungimento di una determinata strategia o di un obiettivo aziendale.

Un ulteriore aspetto da considerare è l'identificazione di opportuni *trigger*, ossia di *alert* tempestivi alle ipotesi sottostanti le valutazioni della gravità dei rischi (*early-*

---

[4] A titolo esemplificativo, tra le tecniche qualitative si segnalano le interviste, i *workshop*, i sondaggi e le analisi di *benchmarking*. Tali approcci sono spesso utilizzati quando la tipologia di rischio non è facilmente quantificabile oppure quando è oneroso e non praticabile ottenere una mole significativa di dati affidabili necessari per una corretta quantificazione. Le tecniche quantitative (tra cui alberi decisionali, simulazioni Monte Carlo, ecc.) consentono una maggiore granularità e precisione delle informazioni, supportano un'analisi costi-benefici e sono tipicamente utilizzate in attività più complesse. La validità di queste tecniche si basa sull'affidabilità della base dati. Le tecniche quantitative includono ***modelli probabilistici*** (ad esempio *value at risk*, *earning at risk*, *cash flow at risk*) che associano una serie di eventi e l'impatto risultante con la probabilità di tali eventi sulla base di determinati presupposti e ***modelli non probabilistici*** (ad esempio analisi di scenario, analisi di sensitività, *stress test*) che si basano su ipotesi soggettive dell'impatto senza quantificarne la probabilità.

[5] Il "rischio inerente" è il rischio che un'organizzazione assume in assenza di una qualsiasi azione da parte del *management* che possa modificare l'impatto e la probabilità di accadimento; il "rischio residuo *target*" è la quantità di rischio che un'organizzazione preferisce assumere nel perseguire la propria strategia e gli obiettivi aziendali, sapendo che la direzione attuerà o ha attuato azioni dirette o mirate per modificare la gravità del rischio. Il "rischio residuo reale" è il rischio rimanente dopo che la direzione si è attivata per modificare il livello di gravità. Il rischio residuo reale deve essere uguale o inferiore al rischio residuo *target*.

warning indicator). Tali indicatori possono determinare la necessità, da parte del *management*, di una rivalutazione del processo di stima del rischio.

3. Principio n. 12 – La prioritizzazione dei rischi

La prioritizzazione dei rischi è alla base della capacità del *management* di indirizzare le decisioni in merito a:

- quali azioni di risposta ai rischi intraprendere, e
- come ottimizzare l'allocazione delle risorse disponibili tra i diversi rischi.

Affinché ci sia un'uniformità nell'approccio da seguire da parte del *management* coinvolto, la prioritizzazione dei rischi può essere condotta utilizzando dei criteri prefissati dall'organizzazione[6].

A seconda di come un rischio si posiziona nella scala delle priorità, il *management* indirizza le azioni di risposta o trattamenti, che sono tanto più efficaci quanto più sono in grado di rispondere al livello di significatività (impatto e probabilità), al criterio di prioritizzazione utilizzato e alla propensione al rischio dell'organizzazione stessa.

L'utilizzo di opportuni criteri facilita il *management* nell'assegnazione delle priorità: rischi con valutazioni di gravità similari possono essere posizionati differentemente nella scala delle priorità, sulla base di un'ulteriore valutazione effettuata in relazione al criterio scelto, tenendo conto del *risk appetite*. A questo proposito, esemplificazioni comuni di *rating* di rischio utili a consentire un'agevole prioritizzazione portano ad identificare rischi catastrofici/alti/medi/bassi, considerando elementi quali ad esempio le perdite finanziarie associate, il *turnover* del personale, l'impatto sulla reputazione, la perdita di clienti strategici, la comminazione di sanzioni o la possibilità di contenziosi, l'impatto sul clima aziendale.

La scelta di tali criteri dipende principalmente dalla tipologia e natura del rischio.

Le risposte al rischio più efficaci sono quelle che indirizzano siano la gravità che la prioritizzazione.

Ulteriore elemento da considerare quando si assegna una priorità ai rischi è il *risk appetite*, ossia il livello di rischio (complessivo e per tipologia) che l'organizzazione è disposta ad assumere per il perseguimento dei suoi obiettivi, ritenuto accettabile.

Attraverso la definizione delle priorità dei rischi, l'Alta Direzione individua anche quei rischi che la stessa sceglie di accettare e per i quali non sarà contemplata alcuna ulteriore risposta.

---

[6] La priorità di un rischio è determinata applicando dei criteri prefissati dall'organizzazione, tra i quali è possibile indicare: **Adattabilità**: la capacità di un'organizzazione di adattarsi e rispondere ai rischi; **Complessità**: la natura e tipologia di un rischio ai fini del successo dell'organizzazione; **Velocità**: la velocità con la un rischio influisce sull'organizzazione; **Persistenza**: per quanto tempo un rischio ha un impatto su una organizzazione; **Recupero**: la capacità di un'organizzazione di rientrare nei limiti di tolleranza.

L'assegnazione della priorità ai rischi deve essere gestita a tutti i livelli dell'organizzazione e a diversi rischi possono essere assegnate priorità differenti a seconda del livello organizzativo a cui si riferiscono (*business unit*, entità nel suo complesso).

L'utilizzo di una categorizzazione standard consente di assegnare priorità ai rischi comuni in modo coerente in tutta l'organizzazione. Il risultato che ne deriva è lo sviluppo di risposte al rischio più coerenti ed efficienti di quelle che si avrebbero se ciascun rischio fosse classificato separatamente come prioritario.

In ogni caso, considerata la responsabilità di valutare i rischi, determinarne le relative priorità e identificare su tali basi le relative risposte, i *risk owner* devono avere una sufficiente autorità per gestire efficacemente i rischi.

4. Principio n. 13 – L'implementazione delle risposte ai rischi

Il *management* deve selezionare ed attuare le azioni di risposta (*risk response*) più idonee a tutelare l'azienda dal verificarsi di tali rischi, coerentemente con le strategie aziendali, gli obiettivi di *business* e di *performance* ed il profilo di rischio. Il modo in cui l'azienda risponde ai rischi identificati determina in ultima analisi quanto efficacemente la stessa riesce a preservare o a creare valore a lungo termine.

I principali approcci per la scelta delle possibili risposte al rischio rientrano nelle seguenti categorie:

- accettare il rischio;
- evitare il rischio;
- perseguire il rischio;
- ridurre/mitigare il rischio;
- condividere/trasferire il rischio[7].

[7] Le azioni di risposta al rischio rientrano comunemente nelle seguenti categorie:

Accettare il rischio: non è intrapresa alcuna azione per proteggersi dall'eventuale manifestarsi del rischio. Questa risposta è generalmente adottata dal *management* quando la gravità del rischio (e quindi le eventuali conseguenze) rientrano nei livelli di tolleranza al rischio dell'azienda. Accettare un rischio comporta spesso, soprattutto per i rischi di tipo ambientale, sociale e di *governance*, la necessità di un attento monitoraggio delle ipotesi che hanno portato l'organizzazione a tale scelta: se naturalmente queste ipotesi cambiano, potrebbe essere necessario attribuire una risposta al rischio differente. **Evitare il rischio:** si intraprendono azioni per rimuovere il verificarsi del rischio a priori. Le organizzazioni possono avere *tolleranza zero* per alcuni rischi correlati all'*ESG* che li porta ad evitare il rischio del tutto o almeno a ridurre notevolmente la probabilità che si verifichi. **Perseguire il rischio:** l'azienda decide di intraprendere un'azione che accresce il rischio di ottenere prestazioni migliori. Quando si sceglie di *perseguire il rischio*, la direzione comprende la natura e l'estensione di eventuali modifiche richieste per raggiungere le prestazioni desiderate pur rimanendo nei limiti della tolleranza accettabile. **Mitigare/Ridurre il rischio**: il *management* decide di adottare una serie di azioni finalizzate a ridurre l'esposizione al rischio. Ciò comporta una miriade di decisioni aziendali quotidiane che riducono il rischio a un livello di gravità allineato al profilo di rischio residuo *target* e alla propensione al rischio. **Condividere/trasferire il rischio**: consiste nel trasferimento dell'intero rischio o di parte di esso ad un soggetto esterno all'impresa, tipicamente esternalizzando una attività o stipulando delle assicurazioni.

In alcune circostanze il *management* può invece dover considerare la necessità di rivedere gli obiettivi oppure la strategia.

Per molte tipologie di rischio le risposte possono essere facilmente identificabili; in alcuni casi si tratta di scelte "obbligate", mentre in altri potrebbe non essere altrettanto chiara la relativa scelta. La selezione di una risposta al rischio appropriata si basa sulla considerazione di una serie di fattori, tra cui il contesto di *business*, l'analisi costi-benefici, eventuali obblighi e aspettative, la priorità associata al rischio, il *risk appetite* e il livello di gravità.

Tale analisi è finalizzata a valutare gli effetti delle possibili azioni di risposta sulla probabilità e sull'impatto affinché la scelta effettuata faccia ricadere il rischio residuo entro i livelli di tolleranza al rischio stabiliti a livello di organizzazione.

Una volta identificate le risposte al rischio, è necessario individuare le attività di controllo che consentano di assicurarsi che le stesse siano implementate per come ipotizzate.

In considerazione del fatto che le risorse disponibili sono limitate, nella scelta delle risposte più adeguate da attuare è bene considerare il rapporto costi/benefici. I costi e i benefici che derivano dalle risposte definite possono essere misurati sia in termini quantitativi che qualitativi, utilizzando unità di misura coerenti con le stesse con cui sono stati definiti gli obiettivi e la tolleranza al rischio.

Di norma, è più agevole da parte *del management* procedere ad una valutazione dei costi, in genere più facilmente quantificabili. La valutazione dei benefici è spesso più soggettiva e può essere ricondotta ai vantaggi/benefici che si otterrebbero complessivamente dal raggiungimento della strategia e degli obiettivi di *business*.

La scelta di una determinata risposta al rischio può introdurre nuovi rischi che non sono stati precedentemente identificati o che potrebbero avere conseguenze indesiderate. Può accadere tuttavia che siano individuate nuove opportunità non considerate in precedenza. In tali casi, la Direzione aziendale dovrà riconsiderare tali opportunità nell'ambito della strategia complessiva.

L'adozione di approcci che considerano i vari aspetti collegati ai rischi, nonché i costi e i benefici di ciascun approccio favorisce il successo delle risposte selezionate ai rischi.

Una volta che il *management* seleziona una o più risposte ai rischi, sarà necessario sviluppare un piano di implementazione di specifiche attività di controllo finalizzate a verificare che l'azione di risposta sia effettivamente ed efficacemente realizzata.

5. Principio n. 14 – Lo sviluppo di una visione d'insieme dei rischi

Uno dei concetti-chiave sviluppati nel COSO ERM è la visione del "portafoglio" dei rischi (*portfolio view*), vale a dire considerare tutte le potenziali implicazioni sul profilo di rischio da una prospettiva di intera organizzazione. Nello sviluppare questa visione d'insieme, l'organizzazione deve considerare il tipo, la gravità, le

interdipendenze dei rischi e il modo in cui tali aspetti possono influire sulle *performance* complessive aziendali.

Se valutato a livello di singola unità o funzione, un rischio potrebbe rientrare nei limiti di tolleranza di quella stessa unità. Avendo a disposizione un quadro di insieme, il *management* è in grado di stabilire se il rischio residuo a livello aziendale si posiziona o meno entro il livello di rischio ritenuto accettabile e di indirizzare conseguentemente le decisioni strategiche e gli obiettivi di *business*.

La visione del rischio che considera la società nel suo complesso può essere sviluppata in vari modi, a seconda che ci si concentri principalmente sui rischi di maggior rilievo o su categorie di eventi che possono riguardare più unità o funzioni, piuttosto che sul rischio specifico dell'azienda considerata nel suo insieme. La visione dei rischi può essere rappresentata su differenti livelli a seconda dell'integrazione: minima integrazione (vista per rischi), limitata integrazione (vista per categorie di rischi), parziale integrazione (vista per profilo di rischio), integrazione totale (rispetto agli obiettivi aziendali e alla strategia nel suo complesso).

Quanto più si riesce a sviluppare una visione complessiva dei rischi, tanto più l'organizzazione può prendere decisioni basate sul rischio, fissare obiettivi di *performance* coerenti e gestire tempestivamente eventuali modifiche al profilo di rischio.

Nel valutare la visione di insieme, l'organizzazione può utilizzare sia tecniche di tipo quantitativo (che includono modelli di regressione e altri strumenti di analisi statistica) che di tipo qualitativo, tra le quali si possono citare le analisi di scenario e il *benchmarking*. In tale contesto, l'organizzazione può rivedere tra l'altro l'impatto dei cambiamenti nel contesto di riferimento o di altre variabili sul raggiungimento degli obiettivi, per verificare le *assumption* sottese alla valutazione dei rischi, il comportamento dei rischi al verificarsi di situazioni di stress, le interdipendenze tra rischi e l'efficacia delle risposte. Ad esempio, l'organizzazione potrebbe decidere di valutare l'effetto sull'insieme dei rischi di un cambiamento dei tassi di interesse, oppure di considerare l'effetto di eventi concomitanti come la variazione dei tassi unita ad un'impennata nei prezzi delle materie prime o ancora l'impatto di un fallimento su larga scala di una terza parte rilevante.

A prescindere dalla tecnica utilizzata, analizzando l'effetto dei potenziali cambiamenti sulla visione dei rischi a livello d'insieme, l'organizzazione può identificare potenziali nuovi rischi emergenti e valutare l'adeguatezza delle risposte ai rischi adottate.

Questa valutazione può generare un processo interattivo attraverso il quale il *management* può rivedere le ipotesi poste alla base della strategia, degli obiettivi di *business* e della valutazione del profilo di rischio.

CAPITOLO IV

REVIEW AND REVISION

1. Principio n. 15 – La valutazione dei cambiamenti sostanziali – 2. Principio n. 16 – La valutazione del rischio e delle *performance* – 3. Principio n. 17 – Perseguire il miglioramento nella gestione del rischio d'impresa.

***

Il processo di *Enterprise Risk Management* non può essere considerato come un'attività *"one and done"* ma va inteso come un processo dinamico che richiede una continua revisione sia dei singoli rischi identificati sia del processo di gestione dei rischi nel suo complesso.

La strategia e gli obiettivi aziendali potrebbero mutare nel corso del tempo in linea con un contesto in continua evoluzione. Conseguentemente, la società potrebbe aver necessità di rivedere ed aggiornare periodicamente le prassi di *risk management* in uso.

Il COSO ERM *Framework* declina la componente *Review & Revision* focalizzata sul monitoraggio delle *performance* del modello di *risk management* e, più in generale, sull'efficacia delle componenti del *Framework* nel tempo. Processi di monitoraggio efficaci supportano le organizzazioni con l'obiettivo di meglio comprendere il rapporto tra rischio e *performance* aziendale.

***

1. Principio n. 15 – La valutazione dei cambiamenti sostanziali

Le aziende dovrebbero monitorare i cambiamenti sostanziali del contesto interno ed esterno che possono compromettere le *performance* di *business* e invalidare le ipotesi sottostanti le strategie adottate in relazione alla gestione dei rischi.

L'identificazione dei cambiamenti è essenziale per la comprensione delle modalità con cui si modificano la gestione dei rischi d'impresa e il raggiungimento degli obiettivi aziendali. A tal proposito, tale attività dovrebbe essere inglobata all'interno dei processi aziendali e continuamente messa in atto.

Alcuni esempi di cambiamenti sostanziali interni ed esterni al contesto aziendale sono di seguito elencati:

- rapida crescita/espansione: quando un'organizzazione si espande rapidamente, la struttura organizzativa, le attività, i sistemi informativi o le

risorse esistenti potrebbero esserne influenzate. Ad esempio, una rapida espansione geografica per acquisizione potrebbe richiedere la ridefinizione di ruoli e responsabilità dei soggetti coinvolti nel presidio dei rischi aziendali secondo i nuovi assetti;

- innovazione: ogniqualvolta viene introdotta un'innovazione, le strategie di risposta al rischio dovranno essere ricalibrate. Ad esempio, l'opportunità di vendere tramite piattaforme di *e-commerce* potrebbe richiedere un approfondimento specifico dei rischi insiti nell'uso di tale tecnologia;
- cambiamenti nella leadership e nel personale: un cambiamento nella gestione manageriale potrebbe influenzare le componenti del processo di *risk management*. Ad esempio, una nuova compagine dirigenziale potrebbe essere caratterizzata da una propria cultura aziendale oppure una differente propensione al rischio;
- cambiamenti nel contesto legislativo o economico: cambiamenti nel contesto legislativo o economico esterno all'azienda potrebbero tradursi in una maggiore pressione concorrenziale, in modifiche nei requisiti operativi in un dato mercato o nell'individuazione di *emerging risk*.

L'identificazione dei cambiamenti sostanziali, la valutazione dei loro effetti e l'individuazione della risposta agli stessi dovrebbero rappresentare attività aziendali iterative in grado di influenzare la gestione aziendale dei rischi. Potrebbe, inoltre, risultare produttivo per l'organizzazione effettuare una sorta di "*incident analysis*" dopo il verificarsi del rischio-evento al fine di monitorare quanto efficace sia stata la risposta dell'organizzazione e di individuare quale approccio sarà possibile applicare agli eventi futuri.

2. Principio n. 16 – La valutazione del rischio e delle *performance*

Gran parte dell'attenzione alla gestione del rischio aziendale riguarda la gestione del rischio in senso stretto, ovvero la gestione del livello di rischio entro soglie accettabili oppure il perseguimento di opportunità emergenti.

Nel tempo, un'organizzazione potrebbe non condurre le proprie attività di *risk management* nel modo più efficace, incidendo così sul manifestarsi dei rischi o sulle *performance* aziendali. Risulta, pertanto, fondamentale riconsiderare, nel tempo, le proprie capacità e pratiche di gestione del rischio. Gli aspetti oggetto di attenzione potrebbero riguardare ipotesi errate, prassi inefficaci, competenze deboli in azienda o aspetti culturali.

Tramite la periodica valutazione delle proprie *performance*, un'organizzazione potrebbe essere in grado di rispondere a quesiti del tipo:

- *"L'organizzazione ha agito come previsto e ha raggiunto i propri obiettivi?"* L'organizzazione dovrebbe individuare gli scostamenti che si sono verificati nelle *performance* e prendere in considerazione ciò che potrebbe aver contribuito.

- *"Quali rischi si stanno verificando e stanno influenzando le performance?"* La valutazione delle *performance* potrebbe permettere di comprendere se rischi precedentemente identificati o rischi emergenti si siano verificati nell'organizzazione e se i livelli di rischio rientrano nei limiti di tolleranza stabiliti.
- *"L'organizzazione sta assumendo un livello di rischio sufficiente per raggiungere i suoi obiettivi?"* Quando un'organizzazione non raggiunge i propri obiettivi dovrebbe determinare se il fallimento sia dovuto a rischi che incidono negativamente sul conseguimento degli obiettivi o ad un livello di rischio non adeguato a sostenere il raggiungimento degli obiettivi.
- *"La stima del livello di rischio è accurata?"* L'organizzazione dovrebbe avere un'accurata comprensione del contesto aziendale e delle ipotesi sottostanti alla valutazione iniziale del livello di rischio. Dovrebbe inoltre valutare la disponibilità di informazioni che potrebbero aiutare a perfezionare la valutazione iniziale.

Se un'organizzazione determina che la propria *performance* non rientra nei livelli accettabili o *target*, il *management* dovrebbe rivedere il processo di *risk management* ovvero mettere in discussione e rivedere i seguenti aspetti:

- strategia e obiettivi aziendali: nel caso in cui la *performance* aziendale sia caratterizzata da una deviazione sostanziale dal profilo di rischio atteso, l'organizzazione potrebbe scegliere di rivedere la propria strategia oppure riconsiderare strategie alternative precedentemente escluse o identificare nuove strategie;
- cultura aziendale: un'organizzazione potrebbe voler rivedere la propria cultura e determinare se sta adottando comportamenti *risk-based* in modo consapevole;
- valutazione e prioritizzazione del rischio: un'organizzazione potrebbe aggiornare la valutazione dei rischi significativi al variare del contesto aziendale oppure della disponibilità di nuovi dati o informazioni e decidere di agire sulla priorità dei rischi identificati per supportare la riallocazione delle risorse;
- risposta al rischio: un'organizzazione può considerare di modificare le risposte ai rischi in linea con le *performance target* e il profilo di rischio atteso. Qualora si rilevi uno scostamento il *management* potrebbe riflettere sulle relative cause e, pertanto, sull'opportunità di rivedere la propria strategia;
- propensione al rischio: le azioni correttive sono in genere intraprese per mantenere o ripristinare l'allineamento del profilo di rischio con la propensione al rischio dell'organizzazione. L'organizzazione dovrebbe valutare se sta assumendo un livello di rischio sufficiente per avere successo o se è esposta ad un livello di rischio eccessivo. La revisione della propensione al rischio richiede il coinvolgimento del Consiglio di Amministrazione.

3. Principio n. 17 – Perseguire il miglioramento nella gestione del rischio d'impresa

Qualora siano individuati cambiamenti significativi nell'ambiente interno ed esterno oppure la *performance* aziendale sia valutata come "non in linea" rispetto ai *target*, l'organizzazione potrebbe dover rivedere il processo di *risk management* nel suo complesso. Le organizzazioni, difatti, dovrebbero monitorare il processo in un'ottica di miglioramento continuo, per aumentare in maniera sistematica il valore aggiunto generato da una gestione dei rischi efficace ed efficiente.

Anche le organizzazioni con un buon sistema di gestione del rischio possono diventare più efficienti attraverso la previsione di una valutazione continua delle proprie modalità di gestione del rischio e l'identificazione delle potenziali aree di miglioramento.

L'opportunità di rivedere e migliorare l'efficienza e il valore generato dal processo di gestione dei rischi potrebbe essere attivata, a titolo esemplificativo, nelle seguenti condizioni:

- nuove tecnologie: le nuove tecnologie potrebbero rappresentare un'opportunità per il miglioramento dell'efficienza dei processi offrendo la possibilità di elaborare, in tempo reale, un'elevata mole di dati relativi all'andamento dei rischi aziendali;
- trend storici: la revisione dei processi di *risk management* potrebbe servire ad indagare le cause di fallimenti accaduti nel passato;
- propensione al rischio: la revisione della *performance* della gestione dei rischi potrebbe comportare la revisione della propensione al rischio dell'organizzazione;
- categorie di rischio: un'organizzazione che persegue il miglioramento continuo potrebbe rivedere e aggiornare periodicamente il modello di categorizzazione dei rischi;
- confronto con la concorrenza: uno sguardo ai rischi identificati dai *competitor* potrebbe essere d'aiuto per determinare se l'organizzazione sta operando in linea con le prestazioni del settore;
- velocità di evoluzione del contesto: il *management* deve considerare come e a quale velocità il contesto imprenditoriale si evolve. Ad esempio, un'organizzazione che opera in un settore in cui la componente tecnologia è rilevante e cambia velocemente ha più opportunità di migliorare l'efficienza del proprio processo di gestione del rischio, in particolare tecnologico, rispetto ad un'organizzazione che opera in un settore più stabile.

CAPITOLO V

INFORMATION, COMMUNICATION, AND *REPORTING*

1. Principio n. 18 – L'utilizzo delle informazioni e della tecnologia – 2. Principio n. 19 – La comunicazione delle informazioni sui rischi - 3. Principio n. 20 – Il *reporting* sui rischi, sulla cultura e sulla *performance.*

***

La sempre maggiore centralità delle tecnologie digitali e della gestione delle informazioni nell'attuale contesto economico, determinata in parte dalla costante espansione delle soluzioni *cloud* e di *knowledge sharing*, ha portato ad una crescita esponenziale del volume dei dati disponibili. In parziale contrapposizione a tale fenomeno è inoltre importante considerare l'aumento della sensibilità della collettività e delle autorità riguardo la tutela dei dati personali.

Dal punto di vista operativo, ciascuna organizzazione deve innanzitutto essere in grado di strutturare i dati e le informazioni in categorie coerenti, con l'obiettivo di identificare i rischi che potrebbero influenzare la strategia e gli obiettivi aziendali. La quantità e soprattutto la qualità delle informazioni sono pertanto fondamentali per avere una corretta visione d'insieme del sistema di gestione dei rischi aziendali.

In considerazione degli elementi di complessità prima citati, disporre di adeguate informazioni che consentano di conoscere i rischi significa poter garantire la continuità della strategia aziendale e poter adottare una visione di lungo periodo. Tra i requisiti essenziali per un efficace trasferimento delle informazioni ed una chiara comunicazione dei rischi rientrano sicuramente l'adozione di un linguaggio e di strumenti comuni, nonché lo sviluppo di competenze specifiche per la gestione degli stessi strumenti.

Tale componente del *Framework* ERM evidenzia perciò la necessità di un processo continuo di raccolta e condivisione di informazioni rilevanti, interne ed esterne, che consentano all'organizzazione di prendere decisioni consapevoli in termini di gestione dei rischi.

1. Principio n. 18 – L'utilizzo delle informazioni e della tecnologia

L'utilizzo di "informazioni rilevanti" permette alle organizzazioni di anticipare situazioni che potrebbero ostacolare il raggiungimento degli obiettivi strategici e di *business.*

Oggi i dati vengono generati così velocemente che spesso è difficile per il *management* elaborarli e perfezionarli in informazioni utilizzabili. I sistemi informatici possono aiutare le organizzazioni a far fronte a questa sfida.

Nella definizione delle esigenze funzionali è necessario considerare la capacità delle soluzioni informatiche di assistere il *management* nella comprensione e nell'analisi dei rischi e nella definizione di decisioni consapevoli, in aggiunta alle necessità basilari per soddisfare i requisiti di *reporting*. Oltre a rendere più celeri ed efficienti le attività di elaborazione ed analisi delle informazioni, tali soluzioni informatiche devono essere in grado di preservare la qualità dei dati, nonché di trasferire e condividere le informazioni con gli altri sistemi dell'azienda e degli altri interlocutori del proprio *network*.

L'organizzazione potrà trarre utilità solo da informazioni di qualità rese disponibili in modo tempestivo, o comunque quando opportuno, ai responsabili delle decisioni. Se i dati sottostanti sono inaccurati o incompleti, il *management* potrebbe non essere in grado di emettere giudizi, fare stime o prendere decisioni valide. Di conseguenza, per mantenere informazioni di qualità, le società sono chiamate ad implementare sistemi di gestione dei dati e stabilire politiche di gestione delle informazioni con chiare linee di responsabilità.

Oggi i progressi nel calcolo cognitivo, come l'intelligenza artificiale e il *data mining*, consentono di raccogliere ed analizzare grandi volumi di dati non strutturati, supportando il processo di elaborazione delle informazioni e aiutando le organizzazioni ad evitare il "sovraccarico di informazioni".

I dati devono essere ben gestiti per fornire le giuste informazioni per supportare decisioni consapevoli del rischio. Ciò richiede di catturare e preservare la qualità dei dati consentendo, al tempo stesso, a diverse tecnologie di scambiarli ed utilizzarli.

Le organizzazioni che hanno provveduto ad implementare un sistema integrato di gestione del rischio ed un processo di *internal audit* strutturato, potranno sicuramente trarre beneficio da *software* dedicati in grado di supportare la gestione dell'intero processo. Per categorie di rischio specifiche (finanziari, reputazionali o connessi a particolari aspetti di *compliance*, tra cui ad esempio la gestione in ambito HSE), ciascuna azienda potrà invece valutare l'adozione di tool specifici, in considerazione dell'effettivo livello di criticità e dei benefici conseguibili.

2. Principio n. 19 – La comunicazione delle informazioni sui rischi

Le attuali organizzazioni possono disporre di vari canali per comunicare i dati e le informazioni sui rischi agli *stakeholder* interni ed esterni. Internamente, la direzione deve comunicare chiaramente la strategia e gli obiettivi aziendali a tutti i livelli della società, in modo che ciascuno comprenda il proprio ruolo. Esternamente la direzione deve saper informare gli azionisti e le altre parti interessate in merito alle modalità di gestione dei rischi aziendali, al fine di far comprendere agli *stakeholder* esterni non solo le prestazioni rispetto alla strategia, ma anche le azioni intraprese consapevolmente per raggiungerle.

Avere canali di comunicazione aperti permette alle società di essere anche nelle condizioni di ricevere informazioni da parte di soggetti esterni.

Inoltre, una comunicazione efficace tra il Consiglio di Amministrazione e il *management* è fondamentale per raggiungere gli obiettivi aziendali: le organizzazioni devono esaminare la propria struttura di *governance* per garantire che le responsabilità siano chiaramente assegnate e definite e che la struttura supporti il dialogo in merito alle pratiche di *risk management*.

Nell'ambito del ruolo di supervisione, il Consiglio di Amministrazione deve garantire che, in funzione dell'evoluzione della strategia e degli obiettivi aziendali, le comunicazioni relative al *risk appetite* rimangano aperte, ad esempio organizzando riunioni del Consiglio trimestrali e convocando riunioni straordinarie per affrontare tematiche specifiche, come, ad esempio, la sicurezza informatica, i rischi legati alla successione nel *management* o le criticità potenzialmente derivanti da operazioni straordinarie.

Il Consiglio di Amministrazione, nel discutere i rischi emergenti che possono minare qualsiasi ipotesi alla base della strategia e degli obiettivi di *business* esistenti, può incoraggiare il *management* a fornire informazioni più tempestive, piuttosto che aspettare che tali rischi si evolvano all'interno dell'organizzazione.

3. Principio n. 20 – Il *reporting* sui rischi, sulla cultura e sulla *performance*

Ogni destinatario di un *report* può avere diverse esigenze informative in considerazione dei rischi presidiati e dei risultati da conseguire.

I *report* combinano informazioni quantitative e qualitative sul rischio e variano nella loro forma ed estensione, in funzione degli argomenti affrontati.

Tipicamente, i *report* riguardanti i risultati commerciali delle aziende devono essere sintetici, fornire informazioni comparabili nel tempo e che interessano un intero processo o un'area di riferimento.

I *report* relativi ad attività di *audit*, invece, riportano in genere informazioni maggiormente dettagliate, che possono anche riguardare una singola pratica, operazione o transazione e che forniscono una rappresentazione della rilevanza statistica e del grado di gravità.

I *report* riguardanti nello specifico aspetti di *risk management* devono contenere sia dati storici, che informazioni relative a rischi potenziali, ai rischi emergenti, alle analisi delle tendenze e ai cambiamenti nelle prestazioni.

Esistono diversi modi in cui il *management* può riferire ad un Consiglio di Amministrazione, ma è fondamentale che l'obiettivo del *reporting* sia il collegamento tra strategia, obiettivi aziendali, rischio e rendimento. Un *reporting* efficace al Consiglio di Amministrazione deve favorire la discussione delle prestazioni dell'organizzazione nel soddisfare la sua strategia, gli obiettivi di *business* e l'impatto del rischio potenziale sul raggiungimento di tali obiettivi.

La frequenza dei *report* dovrebbe essere commisurata alla gravità e alla priorità del rischio che si vuole monitorare. In mancanza di criticità specifiche, i destinatari del

reporting, che si tratti del *management*, del Consiglio di Amministrazione, o di entrambi, potranno monitorare l'evoluzione dei differenti profili di rischio analizzando i *report* trasmessi periodicamente in base alle tempistiche predefinite.

Chiaramente, sarà sempre facoltà del *management* o del Consiglio di Amministrazione richiedere in ogni momento adeguate informazioni su determinati profili di rischio, ad esempio qualora intercettassero elementi di rischiosità relativi al mercato di riferimento, al rapporto con le autorità e gli altri *stakeholder*, a criticità interne all'organizzazione, oppure derivanti da un presidio inadeguato da parte dei responsabili operativi.

D'altro canto, quando i responsabili di una specifica attività di *reporting* identificano criticità riguardo ad una specifica area di rischio, sono tenuti a segnalarle tempestivamente al *management* e, ove necessario, direttamente al Consiglio di amministrazione, mediante flussi informativi ad hoc che forniscano informazioni quanto più complete ed accurate.

Le segnalazioni devono consentire al *management* di determinare i tipi e l'entità del rischio assunto dall'organizzazione e l'idoneità delle risposte al rischio esistenti.

La completezza e la correttezza dei dati contenuti nei *report* devono sempre rappresentare degli elementi di attenzione dei responsabili dell'attività di *reporting*, i quali dovranno fornire adeguati livelli di *assurance* sulla veridicità e l'attendibilità delle fonti, verificando inoltre che non siano omesse informazioni essenziali per un'adeguata valutazione dei rischi.

L'esclusivo utilizzo di dati storici per la comprensione dei risultati consente unicamente di descrivere un evento pregresso, senza effettuare delle ipotesi su potenziali trend delle *performance* e dei profili di rischio.

Al fine di valutare la probabilità con cui un rischio potrebbe manifestarsi è invece utile prendere in considerazione dati prospettici, anche al fine di anticipare eventuali interventi preventivi.

Tra gli esempi di indicatore chiave che riguardano le prestazioni del personale aziendale è importante menzionare il tasso di *turnover*. Per mantenere elevati livelli di competenza, un'azienda può definire una soglia massima per il tasso di *turnover* annuo.

Qualsiasi valore del tasso superiore al *target* fissato indica che il rischio di indebolimento del *know how* aziendale si sta potenzialmente manifestando.

CAPITOLO VI

L'APPROCCIO COSO ERM INTEGRATO CON I TEMI DI SOSTENIBILITÀ (ESG)

Ogni entità, impresa, governo e organizzazione *no profit*, si trova ad affrontare un panorama di rischi in grande evoluzione. Oltre quelli di natura più tipicamente operativa, legati direttamente al raggiungimento degli obiettivi di *business* e con impatti economici diretti così come tradizionalmente identificati, esistono tipologie di rischio ricomprese all'interno del concetto di sostenibilità, come quelli legati all'ambiente, ai temi sociali ed alla *governance* (ESG).

Anch'essi possono avere un impatto sulla redditività, sul successo e persino sulla sopravvivenza delle organizzazioni in cui si manifestano.

Non esiste una definizione universale per i rischi ambientali, sociali e di *governance*; essi possono essere generalmente indicati anche come rischi di sostenibilità, non finanziari o extra-finanziari. Ogni entità adotta una propria definizione che può richiamarsi alla cospicua letteratura che si è sviluppata in materia.

In linea generale i principali elementi critici riconducibili a ciascun ambito possono essere riepilogati come segue:

- Ambiente: cambiamento climatico, emissione di gas a effetto serra, inquinamento, gestione dei rifiuti, efficienza energetica, riscaldamento globale.
- Sociale: diritti umani, standard di lavoro nella catena di approvvigionamento, lavoro minorile, rispetto della salute e della sicurezza sul lavoro.
- *Governance*: insieme di regole o principi che definiscono diritti, responsabilità e aspettative delle diverse parti coinvolte nella gestione delle società e di tutti gli altri portatori d'interessi.

Bisogna inoltre registrare una crescente sensibilità da parte degli investitori che cercano di comprendere come le organizzazioni stanno identificando e rispondendo ai rischi legati all'ESG. Negli ultimi anni ad esempio, circa il 50% delle proposte presentate dagli azionisti negli Stati Uniti ha riguardato temi ambientali e sociali (riferiti a finanziamenti ai partiti, attività di *lobbying*, emissioni di gas a effetto serra, *disclosure* sulla sostenibilità, remunerazione degli amministratori, diversità e inclusione, diritti umani, controllo delle armi, etc.). È opinione diffusa che nel futuro prossimo i temi di sostenibilità influenzeranno fortemente le azioni e le strategie delle organizzazioni, anche nostrane, con riflessi sui mandati degli amministratori, sul corso dei titoli e sulle capitalizzazioni di borsa, sui risultati e sulla reputazione delle stesse.

Di seguito sono riportate sintetiche esemplificazioni delle modalità con cui i rischi ESG possono essere considerati in ciascuna componente del COSO ERM.

Governance and Culture

Il trattamento dei rischi ESG deve essere integrato nella struttura, nei sistemi, nei processi di *governance* e nella comunicazione dell'organizzazione attraverso:

- miglioramento della consapevolezza del Consiglio di Amministrazione rispetto ai rischi di sostenibilità;
- identificazione e definizione dei requisiti ESG obbligatori e facoltativi;
- definizione di una strategia coerente con gli obiettivi ESG che l'organizzazione si pone;
- identificazione delle strutture operative, dei *risk owner*, dei flussi informativi, dell'integrazione del processo di pianificazione strategica con l'ERM e delle modalità di gestione delle azioni di miglioramento relativamente ai rischi ESG;
- identificazione ed applicazione di opportuni *driver* di valutazione dei rischi applicabili anche alle tematiche ESG;
- sviluppo di una comunicazione coerente con gli obiettivi ESG definiti nella strategia;
- creazione di opportunità di collaborazione interna;
- integrazione delle tematiche di sostenibilità nella cultura e nei valori fondamentali dell'organizzazione;
- ricerca e valorizzazione delle competenze ESG nell'ambito dei processi di selezione e di gestione dei talenti nell'ottica del rafforzamento dell'integrazione nell'organizzazione.

Definizione delle strategie e degli obiettivi

Una chiara comprensione della strategia aziendale, degli obiettivi e del contesto aziendale è un fattore critico ai fini dell'approccio COSO ERM.

Integrare gli aspetti di sostenibilità tramite l'identificazione, valutazione e gestione dei rischi legati agli aspetti ESG consente di avere una visione completa, permettendo altresì di adottare una accezione più ampia del concetto di creazione di valore, che superi i fattori esclusivamente legati a dati finanziari e/o economici, ma che inglobi anche temi che impattano sui gruppi di *stakeholder* e/o rappresentanze sociali.

La tabella seguente riporta, a titolo esemplificativo, un elenco di aspetti legati ai rischi ESG che dovrebbero essere considerati nel momento della definizione degli obiettivi e dei piani al fine di gestire opportunamente il contesto in cui opera l'organizzazione.

		Elementi	Elementi da considerare
Processo di creazione del valore		**Overview dell'azienda e contesto di riferimento esterno**	· Quali sono gli aspetti legali, commerciali, sociali, ambientali e politici del contesto esterno che impattano sulla capacità di creare valore nel breve, medio, lungo termine? · La *mission* e la *vision* dell'azienda cosa richiedono in un'ottica ESG? · Come è collegato il contesto ESG alla creazione di un valore più esteso? · Quali sono i *megatrend* che potrebbero impattare la società? · Quali sono i bisogni e gli interessi di uno *stakeholder* chiave in ottica ESG? · Quali sono i punti di forza/debolezza, le opportunità e le minacce relativi all'ottica ESG?
	Business model	**Inputs**	· Quali sono i problemi legati alle tematiche ESG su cui fa affidamento il *business* come ad esempio fattori ambientali, materie prime, risorse naturali, risorse idriche, etc.? · Come gli stock e i flussi finanziari impattano sulla affidabilità e flessibilità del modello di *business*?
		Attività di Business	· Qual è la catena di valore della società? · Come si differenzia nel mercato? · Come la società apporta innovazione? · Qual è la capacità dell'impresa di adattarsi ai cambiamenti?
		Output	· Qual è l'impatto o i potenziali impatti dei prodotti o degli scarti sulla catena di valore?
		Outcome	· Quali sono i risultati e i contributi in termini di coinvolgimento dei dipendenti, reputazione, soddisfazione del cliente ecc.?
		Strategia e allocazione delle risorse	· Quali sono gli obiettivi strategici nel breve, medio e lungo termine? · Quali sono gli impatti dei rischi ESG sul raggiungimento degli obiettivi (es. cambiamento climatico)? · Le considerazioni ambientali e sociali in che misura sono state integrate nella strategia societaria al fine di conseguire un vantaggio competitivo? · Quali allocazioni di capitale e risorse sono richieste per implementare la strategia?

L'integrazione nell'approccio COSO ERM dei temi di sostenibilità richiede inoltre di ampliare la definizione di *risk appetite* (o propensione al rischio). Le diverse entità dovrebbero chiedersi infatti come i fattori e i relativi rischi ESG possono impattare sulla propria propensione al rischio andando ad esempio ad individuare quei rischi legati ai temi di sostenibilità la cui assunzione può ritenersi necessaria e/o accettabile per realizzare le proprie ambizioni strategiche e quali invece la società vorrebbe/dovrebbe evitare in assoluto.
Rimane essenzialmente similare l'approccio da perseguire nella formulazione degli obiettivi di *business*, in quanto l'individuazione degli obiettivi andrà effettuata tenendo conto dei rischi a cui è assoggettata la società, integrando in essi anche le potenziali ricadute derivanti da problematiche di natura ambientale, sociali e di *governance*, le quali dovranno essere gestite unitariamente con gli obiettivi e le strategie definiti.

Performance

L'identificazione dei rischi ESG può risultare particolarmente critica perché spesso si tratta di rischi nuovi o emergenti, rilevanti nel lungo termine, difficili da quantificare, talora connotati da elementi non prevedibili e qualificabili come "cigni neri", le cui conseguenze possono avere un impatto anche estremamente rilevante sul conseguimento della strategia e degli obiettivi di *business*.

Con riferimento alla valutazione, bisogna tener conto che spesso i rischi ESG si manifestano su un orizzonte temporale più lungo rispetto a quello tipicamente utilizzato per la definizione della strategia (tre o cinque anni). La valutazione dei rischi ESG può risultare alquanto sfidante poiché, per la natura intrinseca di tali rischi, vi è spesso una maggiore difficoltà nel comprendere le ricadute di tipo finanziario e/o di *business* e la relativa quantificazione. In questo contesto l'organizzazione dovrà comunque definire criteri e modalità per valutare ogni singolo rischio ESG individuato affinché possa comunque essere considerato nelle analisi complessive.

Data la relativa imprevedibilità di tali rischi, in ottica di *mitigation* la scelta più efficace potrebbe essere quella di concentrarsi su strategie adattive e resilienti, che preparino le organizzazioni ad affrontare i rischi nel momento in cui si presentano, piuttosto che preselezionare specifiche azioni di risposta che potrebbero però rivelarsi non completamente calibrate rispetto alle effettive esigenze. Si tratta quindi di adottare *policy* e strumenti di gestione delle crisi evoluti e sufficientemente flessibili, che l'organizzazione sia pronta ad attuare.

Review and Revision

Con riferimento alle tematiche ESG, è fondamentale tenere in considerazione che, rispetto ai rischi tradizionali, i rischi ESG possono mutare ed evolversi assai velocemente. In considerazione di tale dinamicità, è fondamentale che l'organizzazione monitori nel continuo i cambiamenti del contesto interno ed esterno al fine di determinare la necessità di una risposta da parte del *management*.

Quest'ultimo dovrebbe inoltre monitorare periodicamente l'efficacia delle risposte ai rischi e se tali azioni siano capaci di mantenere il livello di rischio entro una soglia di tolleranza. A tal fine l'organizzazione potrebbe definire specifici KPI e le relative soglie di allerta. Per determinare gli indicatori appropriati per monitorare un rischio, le organizzazioni potrebbero sfruttare gli indicatori chiave di *performance* (ad es. *target* di fidelizzazione dei dipendenti, obiettivo di riduzione delle emissioni) o *framework* esistenti utilizzati per la rendicontazione delle informazioni non finanziarie, come i GRI *Standards*, che rappresentano una *best practice* riconosciuta a livello internazionale relativamente all'informativa sulla sostenibilità, in grado di compendiare elementi di *risk management* e di CSR.

Information, communication, and reporting

I recenti cambiamenti culturali hanno incrementato notevolmente la rilevanza per le aziende del concetto di reputazione come valore da tutelare e da monitorare, perché elemento fondante della sopravvivenza e della resilienza aziendale nel medio/lungo periodo.

In particolare, negli ultimi anni si è assistito ad una accelerazione verso l'adozione e la promozione dei valori di sostenibilità, in parte perché legati al rispetto delle normative esistenti in materia ambientale, giuslavoristica e societaria, in parte perché tutti gli *stakeholder*, a partire dalla Pubblica Amministrazione e dalla collettività, hanno incrementato le aspettative riguardo ai comportamenti etici delle imprese.

In quest'ottica, la comunicazione di un'immagine aziendale positiva, attraverso appropriate modalità di *reporting* in cui evidenziare chiaramente le misure per la gestione delle aree di rischio che possano avere un impatto in termini di responsabilità sociale e ambientale, si integra perfettamente con una politica di *Enterprise Risk Management* che, operando in termini di prevenzione con riferimento alle aree prioritarie di rischio, contribuisce ad evitare impatti negativi sull'immagine e in generale sul *brand* aziendale.

AUTORI

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

Nicolò Zanghi (KPMG - Coordinatore)
Adele Lorenzoni (ASSIREVI)
Giuseppe Carnesecchi (BDO Italia)
Laura Cattaneo (Audirevi)
Cinzia Damiano (PricewaterhouseCoopers)
Ginevra De Romanis (EY)
Alfredo Gallistru (PricewaterhouseCoopers)
Alberto Girardi (EY)
Stefano Gnocchi (Mazars Italia)
Manuela Losa (Audirevi)
Fabrizio Marcucci (Deloitte)
Eugenio Mittiga (Mazars Italia)
Alessandra Rizzo (KPMG)

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.

Consiglio Direttivo

CONSIGLIERE	VICE CONSIGLIERE
Gianmario Crescentino (P)	Mauro Di Bartolomeo
Simone Scettri (VP)	Beatrice Amaturo
Simone Del Bianco (VP e T)	Rosanna Vicari
Anna Baldini	Alfonso Laratta
Sandro Gherardini	Michele Milano
Umberto Giacometti	Maria Luisa Delcaldo
Maurizio Lonati	Giorgio Greco
Angelo Pascali	Luca Ferranti
Olivier Rombaut	Marco Lumeridi
Davide Trinchero	Bruno Piazza

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

ASSIREVI

ASSIREVI è un'associazione privata senza scopo di lucro fondata nel 1980 e riconosciuta ai sensi del D.P.R. 361/2000, che riunisce oggi 16 società di revisione italiane di grandi, medie e piccole dimensioni. Le Associate rappresentano la quasi totalità delle società che svolgono la revisione sugli Enti di Interesse Pubblico in Italia (vale a dire società quotate, banche e assicurazioni).

Le Associate di ASSIREVI si caratterizzano per una vocazione professionale europea e internazionale, nonché per una visione spiccatamente multidisciplinare della loro attività, che sempre più richiede il coordinamento di competenze professionali evolute e tra loro diversificate. Grazie alle proprie Associate, ASSIREVI dispone pertanto di un osservatorio privilegiato sul contesto economico, aziendale, legislativo e regolamentare europeo e mondiale.

Tra gli scopi principali di ASSIREVI vi è quello di promuovere, sostenere e fornire contributi alla valorizzazione dell'attività di revisione legale e delle altre attività di *assurance* e alla loro evoluzione, nonché alla cultura ad esse relativa.

A tal fine, ASSIREVI promuove e realizza l'analisi scientifica di supporto all'adozione o alla modifica dei principi e delle norme tecniche e operative per lo svolgimento della revisione legale e delle altre attività di *assurance*, ed è costantemente impegnata nella risoluzione di problematiche professionali, giuridiche e fiscali di comune interesse delle Associate.

ASSIREVI si occupa inoltre di promuovere nei confronti delle Associate e del mercato la diffusione della conoscenza tecnico-scientifica in materia di *audit* e *assurance*, nonché delle altre tematiche a queste strettamente connesse, anche attraverso la predisposizione di quaderni, documenti di ricerca, *position paper* e monografie.

Nel perseguire le proprie finalità istituzionali, ASSIREVI intrattiene consolidati rapporti di collaborazione e confronto con le principali *Authorities* italiane, con gli Ordini Professionali e con altre associazioni a livello nazionale e internazionale. ASSIREVI è, tra l'altro, membro fondatore dell'Organismo Italiano di Contabilità (OIC), *standard setter* nazionale in materia di principi contabili, nonché dell'Organismo Italiano di Valutazione (OIV).

www.assirevi.it

Milano, Novembre 2020
Provider: register.it