ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

La guida alla lettura del COSO ERM Framework proposta da ASSIREVI: la sfida dell'integrazione tra strategia, rischi e performance

18 dicembre 2020

ASSIREVI

La guida alla lettura del COSO ERM Framework proposta da ASSIREVI: la sfida dell'integrazione tra strategia, rischi e performance

Il Framework ERM e i fattori chiave per l'implementazione

Nicolò Zanghi
Gruppo di Ricerca Governance di Assirevi

18 dicembre 2020

Il Framework Enterprise Risk Management

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

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 lungo termine.

Il Framework Enterprise Risk Management

Il Framework COSO ERM raffigura le **cinque componenti caratterizzanti il ciclo di vita di un'organizzazione**.

5 componenti

Le componenti avvolgono
gli step chiave dello sviluppo e
dell'esecuzione di una strategia aziendale.

20 principi

I principi rappresentano le iniziative che le aziende dovrebbero implementare per la realizzazione di processi integrati di gestione del rischio.

Governance & Culture

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

Strategy & Objective-Setting

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

Performance

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

Review & Revision

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

Information, Communication, & Reporting

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

Il Framework Enterprise Risk Management

Il Framework COSO ERM posiziona chiaramente il processo di gestione dei rischi **al centro della catena del valore** tra la missione, la visione e i valori fondamentali dell'organizzazione e le sue performance.
L'ERM non è, pertanto, un'attività separata ma **parte integrante della definizione e dello sviluppo della strategia e dei processi di performance** dell'organizzazione.
Proprio per questo l'ERM supporta i Consigli di Amministrazione e le Direzioni in processi decisionali informati che consentano di gestire efficacemente quei rischi che potrebbero compromettere la capacità di raggiungere le strategie e gli obiettivi aziendali in ottica di miglioramento continuo delle performance.

Source: COSO ERM Framework, 2017

What ERM Is

- An ongoing/continuous process
- A way to help create and preserve value
- Includes practices that management puts in place to manage risks
- A process that can be used by organizations of any size
- An aid to making better decisions

What ERM Is not

- A separate activity, not coordinated or integrated with strategy setting activities
- A separate staff function or department
- A "to-do" or checklist
- Applicable only to large, public companies
- Simply a listing or inventory of risks
- A solely quantitative exercise

I fattori chiave per l'implementazione del Framework ERM

Tone from the Top

Affinché un processo ERM abbia successo, il Consiglio di Amministrazione e la Direzione dovrebbero tradurre i comportamenti, gli atteggiamenti e la cultura del rischio, il cd. "Tone from the Top", in azioni concrete con cui l'organizzazione possa raggiungere la mission e gli obiettivi di business.

Il Consiglio di Amministrazione individua la strategia, gli obiettivi, il profilo e il livello di rischio in funzione delle caratteristiche dell'organizzazione e, insieme alla Direzione, indirizza la cultura aziendale a supporto del funzionamento del processo di gestione dei rischi.

È responsabilità del Consiglio di Amministrazione verificare che la Direzione e il management dedichino il giusto livello di attenzione e risorse al processo di gestione dei rischi e che vengano intraprese azioni per l'integrazione con gli altri processi dell'organizzazione.

I fattori chiave per l'implementazione del Framework ERM

Il ruolo e l'obiettivo dell'ERM devono essere compresi e comunicati

Il Framework fornisce una descrizione esplicita del ruolo e dell'obiettivo dell'ERM ovvero supportare i processi decisionali informati del Consiglio di Amministrazione e della Direzione e le organizzazioni nella creazione di valore di lungo periodo.

L'attenzione rivolta all'ERM da parte di autorità di regolamentazione e agenzie di rating ha portato alcune organizzazioni a considerare il processo di gestione dei rischi come un'attività guidata da esigenze di compliance. Inoltre, l'ERM è considerato, talvolta, un semplice esercizio di identificazione dei rischi aziendali.

Pertanto il posizionamento corretto di un processo ERM passa dalla comprensione dei relativi obiettivi e della consapevolezza di tutti i membri dell'organizzazione che la gestione del rischio fa parte delle proprie responsabilità. Attività di comunicazione sul ruolo e sull'obiettivo dell'ERM diventano fattori abilitanti per stabilire e costruire la cultura del rischio desiderata.

I fattori chiave per l'implementazione del Framework ERM

L'ERM deve essere integrato nei processi e nella cultura dell'organizzazione

Un processo di gestione dei rischi di successo deve essere integrato nella cultura dell'organizzazione e nei processi di definizione e sviluppo della strategia e nelle performance aziendali.

Le organizzazioni dispongono di processi per definire le proprie strategie e implementarle nel business, oltre che processi di misurazione delle performance. Pertanto, l'integrazione delle attività di gestione dei rischi con tali processi esistenti permette alle organizzazioni di evitare un ambiente di gestione del rischio "a silos".

L'integrazione può anche promuovere un ambiente e una cultura di condivisione delle informazioni all'interno dell'organizzazione.

I fattori chiave per l'implementazione del Framework ERM

Il punto di partenza è concentrarsi inizialmente sulle principali strategie e obiettivi di business dell'organizzazione

Il punto di partenza per un'efficace gestione dei rischi è identificare in modo specifico e accurato le strategie chiave e gli obiettivi di business dell'organizzazione.

Secondo il Framework le organizzazioni devono identificare gli eventi di rischio che potrebbero compromettere la propria capacità di implementare le strategie e raggiungere gli obiettivi di business. Di conseguenza, il punto di partenza del processo ERM è costituito da una chiara comprensione delle strategie chiave e degli obiettivi aziendali prima di poter identificare e valutare gli eventi che potrebbero comprometterne l'implementazione e il raggiungimento.

In altre parole, la costruzione di un processo ERM deve seguire un approccio "strategy-driven" piuttosto che "risk-driven" affinché le organizzazioni possano risultare vincenti nell'implementazione delle strategie definite.

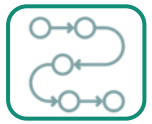
I fattori chiave per l'implementazione del Framework ERM

I "top risk" sono eventi collegati alle strategie chiave

I "top risk" sono gli eventi che potrebbero compromettere la capacità dell'organizzazione di implementare le strategie definite. Le maggiori perdite di valore per le organizzazioni derivano da rischi strategici, ovvero eventi negativi relativi a decisioni strategiche chiave.

Il collegamento tra la gestione dei rischi e la strategia aziendale fornisce una guida per l'organizzazione all'identificazione, nella popolazione complessiva dei rischi aziendali, degli eventi più significativi per il raggiungimento degli obiettivi strategici. Questa guida può essere particolarmente utile per le organizzazioni più complesse o di grandi dimensioni che affrontano molteplici rischi di natura e priorità differente. Collegare il concetto di rischio al raggiungimento degli obiettivi strategici consente al Consiglio di Amministrazione, alla Direzione e al management di concentrarsi su un set di rischi più critici che meritano e richiedono una maggiore attenzione.

I fattori chiave per l'implementazione del Framework ERM



Lo sviluppo dell'ERM può realizzarsi in modo graduale

Il successo dell'ERM può realizzarsi adottando un approccio graduale di implementazione o miglioramento del processo di gestione dei rischi.

Un potenziale ostacolo all'avvio di un processo ERM è la percezione che si tratti di un'iniziativa eccessivamente complessa e costosa. Collegata a ciò, la convinzione che un'organizzazione debba implementare tutte le componenti di un processo ERM in un'unica soluzione per ottenere valore concreto.

L'esperienza suggerisce il contrario. Lo sviluppo graduale di un processo ERM consente alle organizzazioni di:

- guidare il Consiglio di Amministrazione e la Direzione attraverso una curva di apprendimento delle tematiche di gestione dei rischi;
- valutare in ogni fase il modo migliore per adattare il processo rispetto alla struttura di governance e alla cultura dell'organizzazione;
- facilitare l'identificazione e la valutazione dei benefici in ogni fase dello sviluppo.

I fattori chiave per l'implementazione del Framework ERM

Sfruttare le risorse e le attività di gestione del rischio esistenti

Molte organizzazioni hanno sviluppato con successo processi ERM sfruttando le risorse e le attività di gestione del rischio in essere.

L'utilizzo di risorse e attività di gestione del rischio in essere, sebbene talvolta informali o non strutturate, aiuta a evitare il potenziale ostacolo all'avvio di un processo ERM ovvero l'opinione secondo cui sarebbero necessari investimenti significati o risorse ulteriori. Un tale punto di vista potrebbe rivelarsi un ostacolo significativo per le organizzazioni più piccole, in particolare, che potrebbero avere intenzione di sviluppare processi di gestione dei rischi ma avere risorse limitate per realizzarli.

Inoltre, la maggior parte delle organizzazioni avvia iniziative di ERM senza investimenti in alcuna tecnologia che può essere considerata un fattore successivo abilitante al percorso di evoluzione del processo.

La guida alla lettura del COSO ERM Framework proposta da ASSIREVI: la sfida dell'integrazione tra strategia, rischi e performance

GOVERNANCE, CULTURA E INTEGRAZIONE TRA STRATEGIA E RISCHI

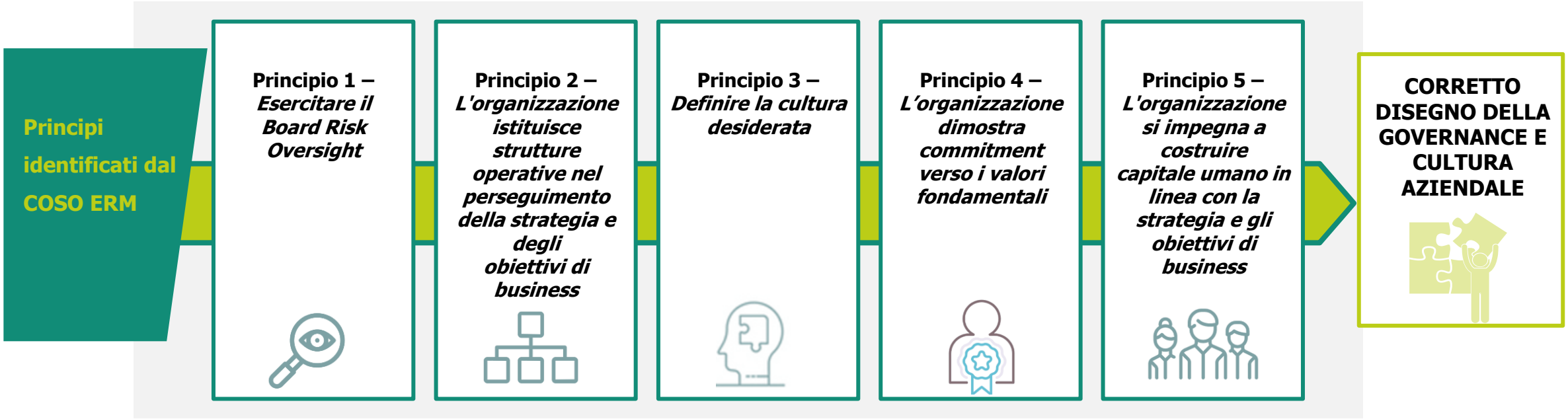
Fabrizio Marcucci
Gruppo di Ricerca Governance di Assirevi

18 dicembre 2020

Governance & Culture

La cultura si riflette nei processi decisionali e la Governance definisce il livello di commitment rispetto all'Enterprise Risk Management.

Il COSO ERM Framework declina la componente "**Governance & Culture**" quale **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.



Governance & Culture

La Governance nella definizione delle strategie

Governance e cultura aziendale sono alla base della definizione degli obiettivi e della gestione dei rischi

La *Governance* è l'insieme dei **principi**, delle **regole** e delle **procedure** che riguardano la gestione e il governo dell'impresa che si innesta all'interno del sistema dei valori, dello stile di direzione e della cultura che la caratterizzano; una Governance adeguata supporta la definizione degli obiettivi e delle modalità di raggiungimento degli stessi, anche attraverso l'identificazione di tutti i rischi ad essi associati.

Gli elementi che garantiscono una governance solida orientata a presidiare i rischi dell'azienda sono:

- Requisiti e competenze dell'organo di governo
- Organizzazione, ruoli e responsabilità
- Cultura e valori
- Risorse umane

Governance & Culture

Esercitare il Board Risk Oversight

La Governance è attuata dall'organo di governo (il Consiglio di Amministrazione, in un modello tradizionale) che definisce le strategie e ne supervisiona il perseguimento da parte dell'organo di gestione (es. Amministratore Delegato, Comitato Esecutivo)

I principali elementi su cui si fonda l'azione dell'organo di governo sono:

- **Responsabilità** nella definizione degli **obiettivi**, degli **indirizzi** e della gestione del **rischio**
- **Delega** al management della **gestione operativa,** volta all'attuazione delle strategie
- **Competenza**, **esperienza** e conoscenza del **business** (da valutarsi in ottica collegiale)
- **Indipendenza** e assenza di conflitti di interesse, garantendo la tutela di quelli degli **stakeholders**
- Indirizzare la **gestione del rischio** entro **limiti di accettabilità**

Governance & Culture

L'organizzazione istituisce strutture operative nel perseguimento della strategia e degli obiettivi di business

Le regole alla base dell'organizzazione di un'azienda definiscono le modalità secondo cui si deve svolgere l'operatività, anche con riferimento alle pratiche di gestione del rischio. Tutto il personale è responsabile dell'attuazione delle pratiche di gestione del rischio

Una azienda «organizzata» definisce:

- **Ruoli e responsabilità**
- **Procure** e **deleghe**
- Chiare **linee di riporto**
- Requisiti di **separatezza funzionale** e segregazione di responsabilità

Tali responsabilità devono essere assegnate anche con riferimento alla **gestione dei rischi** al fine di assicurare il perseguimento delle strategie entro i limiti definiti.

Sono quindi identificati funzioni e organi deputati all'analisi e valutazione dei rischi, nonché al coordinamento di tutte le unità operative coinvolte o impattate dai rischi che possono manifestarsi nelle attività aziendali.

Governance & Culture

Definire la cultura desiderata

La cultura di un'organizzazione riflette lo stile della proprietà e del management; deriva dai suoi valori fondamentali, dai comportamenti attesi e dalle decisioni che vengono assunte. Essa influenza le modalità di gestione dei rischi, in relazione ai livelli di tolleranza accettati

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 nonché alla valutazione delle *performance.*

La cultura aziendale può evolvere nel tempo. I **cambiamenti interni** e le **influenze esterne** (mercati, regolamentazioni, aspettative degli stakeholders, etc.) possono provocare un cambiamento culturale che influenzerà il modo in cui l'organizzazione valuta i rischi e le modalità con cui vengono assunte le decisioni.

Il management ha la responsabilità di favorire la comprensione 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 dipendenti facilita il perseguimento della strategia e degli obiettivi aziendali.

Governance & Culture

L'organizzazione si impegna a costruire capitale umano in linea con la strategia e gli obiettivi di business

Il capitale umano è fondamentale per l'azienda e per il raggiungimento degli obiettivi definiti. E' necessario prevedere e definire strumenti adeguati per accrescere le qualità del capitale umano

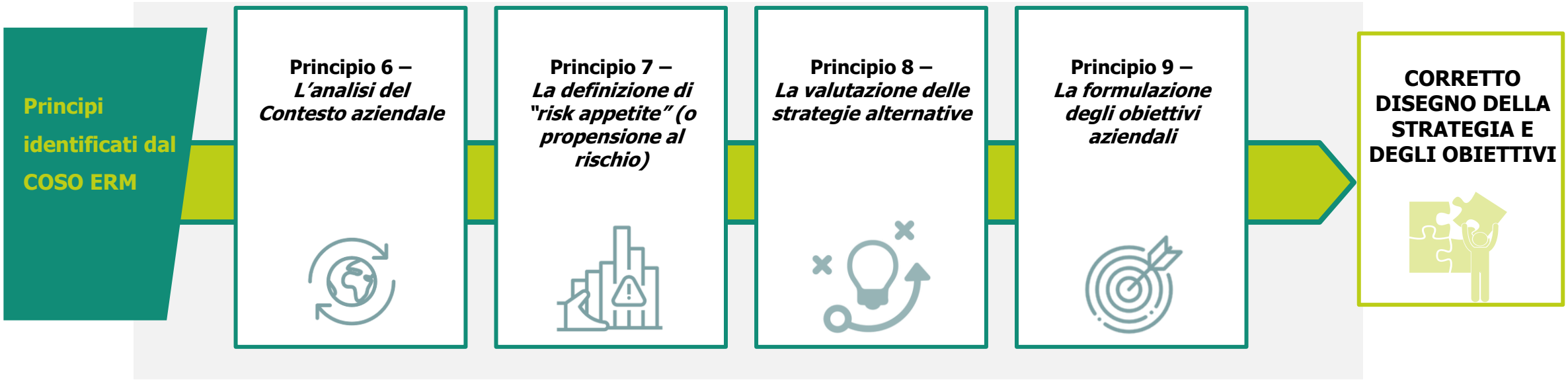
Il capitale umano rappresenta uno dei fattori principali per il successo di ogni azienda.

Gli **interventi da adottare** in favore delle risorse devono essere orientati ad assicurare: i) il mantenimento e l'accrescimento delle necessarie **competenze** per l'esercizio del ruolo assegnato; ii) l'attrazione ed il mantenimento delle **risorse-chiave**; iii) l'adozione di strumenti di **valutazione periodica** finalizzati a definire **percorsi** per allineare i profili professionali ai profili di ruolo da ricoprire; iv) lo sviluppo di sistemi **premianti** le **performance** conseguite, tali da mantenere un elevato livello **motivazionale**; v) la definizione di metodi per semplificare la **successione** ed il ricambio generazionale

Strategy and Objective Setting

Non può esistere una strategia individuata senza la definizione di livelli di rischio accettabili e delle relative soglie di tolleranza.

Il CoSO Framework declina la componente "**Strategy & Objective setting**" secondo cui **ogni organizzazione definisce una strategia per realizzare la propria mission e per generare valore**. Definire una strategia in linea con la mission, la vision ed i core value della società rappresenta un'attività articolata e complessa. L'**integrazione della gestione del rischio 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 in maniera sostenibile.



Strategy and Objective Setting

L'analisi del Contesto aziendale

Il contesto aziendale di riferimento condiziona la definizione delle strategie. Il contesto è dinamico e complesso, talvolta imprevedibile, basandosi solo sull'esperienza pregressa

I **fattori 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.

I **fattori interni** sono l'insieme degli elementi 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.).

La pianificazione tiene conto di come i fattori esterni ed interni possono influenzare il raggiungimento degli obiettivi, tenendo in considerazione i dati e l'esperienza passata, gli andamenti attuali e i dati attesi, anche mediante **analisi di scenario e/o predittive**

Strategy and Objective Setting

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 su livelli universalmente applicabili a qualunque soggetto economico

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 particolari situazioni un'organizzazione può scegliere di farlo.

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, nonché dalla disponibilità di conoscenze e strumenti.

La propensione al rischio è proposta dal management, approvata dal Consiglio di Amministrazione e diffusa in modo capillare in tutta l'organizzazione.

Strategy and Objective Setting

Formulazione degli obiettivi aziendali

Un'azienda considera la componente rischio durante il processo di definizione e attribuzione degli obiettivi 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 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 identifica un **obiettivo** aziendale, deve considerare i potenziali rischi che possono manifestarsi e determinare l'impatto presumibile sul profilo di rischio.

Per supportare il raggiungimento degli obiettivi di business, l'organizzazione declina "**target**" **specifici** utili a indirizzare e monitorare la propria performance attraverso le strutture operative che conducono le attività.

La tolleranza è fortemente influenzata dall'appetito al rischio, minore è l'appetito più stretta sarà la tolleranza rispetto al risultato atteso.

ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

La guida alla lettura del COSO ERM Framework proposta da ASSIREVI: la sfida dell'integrazione tra strategia, rischi e performance

La gestione integrata dei rischi e delle performance

Cinzia Damiano
Gruppo di Ricerca Governance di Assirevi

ASSIREVI

18 dicembre 2020

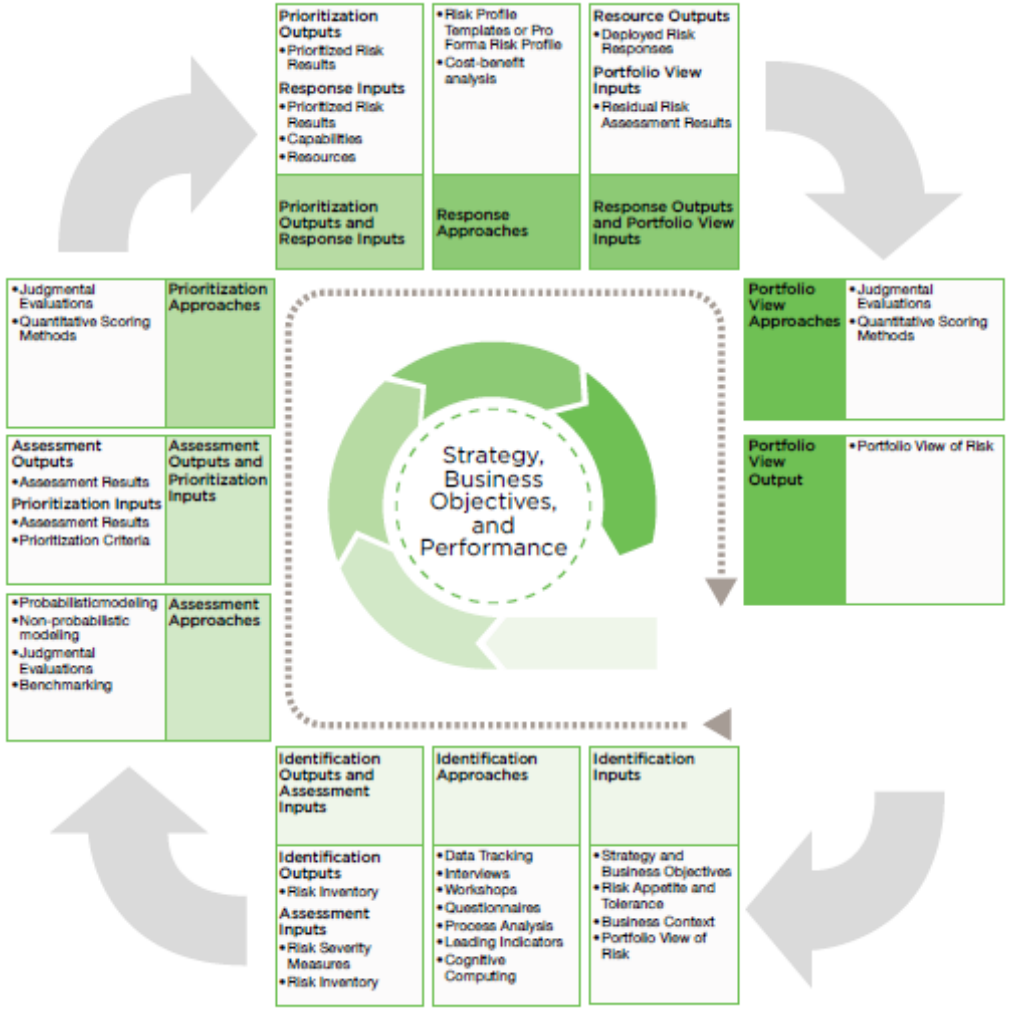
La gestione integrata dei rischi e delle performance

La **creazione e la conservazione del valore aziendale** possono essere significativamente impattate dall'identificazione, valutazione e risposta ai rischi che possono impattare sulla strategia e sugli obiettivi aziendali.

I **rischi** possono originarsi da varie fonti, manifestarsi a vari livelli e richiedere pertanto risposte a tutti i livelli dell'organizzazione.

Le **risposte ai rischi** possono richiedere significativi investimenti, anche in infrastrutture o possono essere parte integrante di misure da adottare nell'operatività quotidiana.

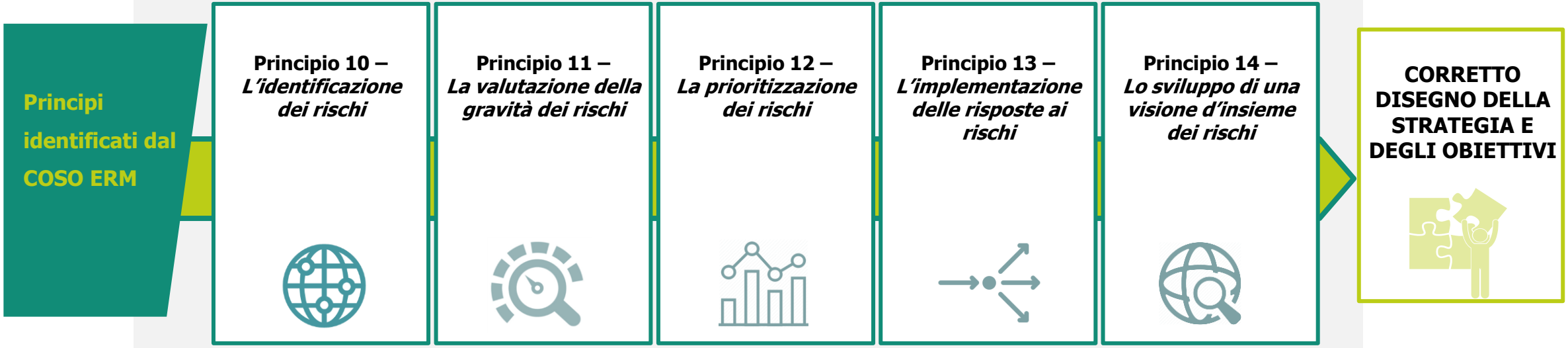
La **gestione dei rischi** deve pertanto coinvolgere tutti i livelli dell'organizzazione, con opportune responsabilità, per definire risposte allineate al tenore dei rischi, secondo un **processo strutturato**.



Performance

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.

Il CoSO Framework declina la componente **Performance** secondo cui **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.



Performance

L'identificazione dei rischi

Identificare tempestivamente i rischi nuovi, emergenti o differenti rispetto a quelli già noti all'organizzazione (attenzione al cambiamento), tenendo conto degli obiettivi e delle strategie

Fattori ed eventi da considerare

- **Interni** (cambiamenti negli obiettivi di business, personale, infrastrutture, risorse finanziarie, …)
- **Esterni** (nuove normative, evoluzione tecnologica, disponibilità di materie prime, cambiamenti ambientali, politici e sociali, cambiamenti nella forza lavoro, …)

Mappatura dei rischi (risk inventory)

- Insieme dei rischi che l'organizzazione deve fronteggiare
- Può essere strutturata per categorie e sottocategorie (es. strategici, operativi, finanziari, di conformità)
- Può includere la rilevanza, le azioni di mitigazione e il risk owner

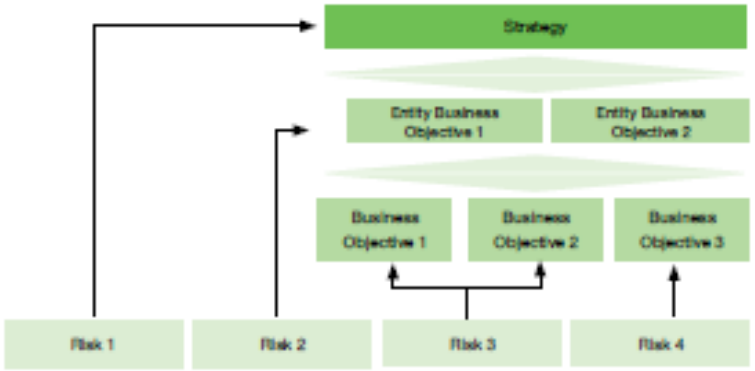
I rischi sono presenti in tutte le attività aziendali

Performance

L'identificazione dei rischi

La mappatura dei rischi non può essere statica, ma richiede una costante rielaborazione/manutenzione al fine di renderla completa e **aggiornata**.

Opportunità di considerare i **dati storici** ma di effettuare sempre **analisi prospettiche**.



Identificazione dei rischi: chi e quando?

- Tutto il management, per competenza
- All'interno delle attività ordinarie (budgeting e business planning, lancio di nuovi prodotti, inserimento in nuovi mercati, gestione reclami, analisi incidenti / perdite, ecc.)
- Attività ad hoc (questionari, workshop, analisi dati, ecc.)

Rappresentazione / descrizione dei rischi

- Utile focalizzarsi sul rischio in quanto tale (non solo su cause, impatti dell'evento, effetti di risposte non propriamente implementate)
- *Possibilità che [descrizione accadimento] e associati impatti su [obiettivi dell'organizzazione]* oppure *rischio di [categoria] relativo a [descrizione accadimento] e [descrizione impatto]*

Performance

La valutazione della gravità dei rischi

Un'efficace gestione dei rischi richiede un bilanciamento costante tra esposizione / propensione al rischio, costi e benefici attesi

Valutare i rischi:

- significa determinarne il livello di gravità in funzione della natura e tipologia ossia **misurare l'incidenza di un evento potenziale sul conseguimento delle performance aziendali attese**
- consente di indirizzare le azioni di risposta (trattamenti e relative priorità)

Aspetti da considerare:

Dimensioni, natura, complessità dell'organizzazione, risk appetite, livello di valutazione (business unit/ unità organizzativa vs organizzazione nel suo complesso)

Dimensioni:

- IMPATTO (possibile effetto sul raggiungimento degli obiettivi)
- PROBABILITA' (possibilità di accadimento)

Orizzonte di valutazione:

Lo stesso per considerato per strategia / obiettivi

Performance

La valutazione della gravità dei rischi

Metodi

- Qualitativi (es.: interviste, workshop, analisi di benchmarking)
- Quantitativi – non monetari, monetari (modelli probabilistici e non probabilistici)
- Una combinazione tra essi

Le viste

- Rischio inerente
- Rischio residuo (target e reale)

In considerazione della dinamicità del contesto di riferimento, assume particolare rilevanza la **capacità di reagire prontamente** agli eventi avversi, anche di difficile previsione.

Questo può essere facilitato da:

- Utilizzo di analisi di scenario e stress test
- Identificazione di opportuni trigger, ossia alert tempestivi di variazione di gravità (early-warning indicators)

Performance

La prioritizzazione dei rischi

E’ alla base della capacità del management di indirizzare:

- **quali risposte** intraprendere
- **come ottimizzare l’allocazione delle risorse**

Necessario considerare opportunamente il *risk appetite*

Criteri da considerare nella definizione delle priorità:

- Adattabilità
- Complessità
- Velocità
- Persistenza
- Recupero

Elementi considerabili: perdite finanziarie, turnover del personale, impatto su reputazione, sanzioni e contenziosi, …

Esempi di rating:

Rischi catastrofici, alti, medi, bassi

Performance

L'implementazione delle risposte ai rischi

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.

Il management deve selezionare ed attuare le azioni di risposta (risk response) più idonee a tutelare l'azienda dal verificarsi dei rischi, coerentemente con le strategie aziendali, gli obiettivi di business e di performance ed il profilo di rischio.

APPROCCI PER LA SCELTA DELLE RISPOSTE


EVITARE


RIDURRE / MITIGARE


CONDIVIDERE / TRASFERIRE


ACCETTARE


PERSEGUIRE

Performance

L'implementazione delle risposte ai rischi

Per il successo delle risposte ai rischi:

- Adeguata considerazione del contesto, delle priorità e del risk appetite
- Valutazione **costi-benefici**
- Considerazione degli **impatti/conseguenze** delle risposte identificate
- Individuazione delle **attività di controllo** che consentono di assicurare che siano implementate per come ipotizzate

- Necessità di definire risposte che riconducano il rischio residuo entro il limite di tolleranza definito
- Valutazione costi-benefici con metriche coerenti alla misurazione di obiettivi e rischi
- Anche le risposte ai rischi possono generare a loro volta rischi e opportunità da considerare nell'ambito della strategia complessiva
- Opportunità di sviluppare un piano di implementazione di specifiche attività di controllo finalizzate a verificare che le azioni di risposta siano effettivamente ed efficacemente realizzate

Performance

Lo sviluppo di una visione d'insieme dei rischi

«Portfolio view»: Opportunità di definire una visione di insieme dei rischi, considerando tutte le potenziali implicazioni sul profilo di rischio da una prospettiva di intera organizzazione.

Interdipendenze e integrazione

- Necessità di considerare: il tipo, la gravità, le **correlazioni tra gli eventi** e il loro possibile **effetto combinato sulle performance** aziendali
- I limiti di tolleranza al rischio possono essere superati se si considerano i rischi in forma aggregata (ad esempio da unità / funzione a intera organizzazione)

Modalità e strumenti

- Differenti livelli per l'integrazione e la vista dei rischi: rischio singolo, categorie, profilo di rischio, riferimento agli obiettivi aziendali nel loro complesso
- Utilizzo di tecniche quantitative (modelli di regressione e analisi statistica) e qualitative (analisi di scenario, benchmarking, …)

La visione dei rischi a livello di insieme agevola:

- una miglior comprensione dell'impatto di potenziali cambiamenti e l'identificazione dei rischi emergenti
- la possibile revisione delle ipotesi alla base di obiettivi, strategia e profilo di rischio.

Performance: sintesi dell'approccio

Nel prendere decisioni finalizzate al perseguimento della strategia ed al raggiungimento degli obiettivi di business occorre:

- ✓ **identificare i rischi** prestando attenzione a quelli **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;
- ✓ **identificare e selezionare le risposte ai rischi più appropriate** (capacità di reazione);
- ✓ **sviluppare una visione d'insieme** dei rischi (interdipendenze, approccio integrato).

*Gestione dei rischi **dinamica, interattiva e consapevole**,*
coerente con la propensione e la tolleranza al rischio dell'impresa.

La guida alla lettura del COSO ERM Framework proposta da ASSIREVI: la sfida dell'integrazione tra strategia, rischi e performance

Attività di monitoraggio e di informazione, comunicazione e reporting

Alberto Girardi
Gruppo di Ricerca Governance di Assirevi, Commissione Governance delle Società Quotate ODCEC Milano

18 dicembre 2020

Attività di monitoraggio – Review and Revision

Sviluppare processi di monitoraggio efficaci con l'obiettivo di meglio comprendere il rapporto tra rischio e performance aziendale

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.**

Attività di monitoraggio – Review and Revision

Valutazione dei cambiamenti sostanziali

L'organizzazione **identifica i cambiamenti sostanziali interni ed esterni** al contesto al fine di analizzare e **comprendere le modalità** con cui si verificano, **valutare** i loro **effetti** e **individuare le risposte** agli stessi.

Cambiamenti sostanziali interni ed esterni da individuare per attuare correttamente il principio:

- **Rapida crescita / espansione:** Ridefinizione di ruoli e responsabilità dei soggetti coinvolti nel presidio dei rischi aziendali secondo i nuovi assetti
- **Innovazione:** Individuazione e ricalibrazione di nuove strategie di risposta all'introduzione di nuovi sistemi, processi e metodi
- **Cambiamenti** nella **leadership** e nel **personale:** Adattamento ad una eventuale nuova cultura aziendale e ad una conseguente potenziale propensione al rischio differente
- **Cambiamenti** nel **contesto legislativo** o **economico:** Monitoraggio costante ed analisi delle modifiche normative e/o requisiti operativi in un dato mercato e individuazione di *emerging risk*

Effettuate «**Incident Analysis**» dopo il verificarsi del rischio-evento al fine di **monitorare** il **livello di efficacia della risposta** dell'organizzazione e di **individuare** quale **approccio** sarà possibile **applicare agli eventi futuri**.

Attività di monitoraggio – Review and Revision

Valutazione del rischio e delle perfomance

L'organizzazione **conduce efficacemente le proprie attività di risk management, valutando i rischi e le proprie perfomance,** al fine di **gestire il livello del rischio entro soglie accettabili** oppure di **perseguire opportunità emergenti.**

Aspetti da monitorare per attuare correttamente il principio:

- **Strategia e obiettivi aziendali:** Revisione della propria strategia oppure riconsiderazione di strategie alternative precedentemente escluse o identificazione di nuove
- **Cultura aziendale:** Revisione della propria cultura e valutazione consapevole dei comportamenti risk-based
- **Valutazione e prioritizzazione del rischio:** Aggiornamento della valutazione dei rischi significativi al variare del contesto aziendale oppure della disponibilità di nuoci dati
- **Risposta al rischio:** Modifica delle risposte ai rischi in linea con le performance target e il profilo di rischio atteso, in caso di scostamenti
- **Propensione al rischio:** Identificazione di azioni correttive per mantenere o ripristinare l'allineamento del profilo di rischio con la propensione al rischio dell'organizzazione

Periodica valutazione della propria perfomance al fine di stabilire se rientra nei target prefissati:

- *L'Organizzazione ha agito come previsto e ha raggiunto i propri obiettivi?*
- *Quali rischi si stanno verificando e stanno influenzando le performance?*
- *L'Organizzazione sta assumendo un livello di rischio sufficiente per raggiungere i suoi obiettivi?*
- *La stima del livello di rischio è accurata?*

Attività di monitoraggio – Review and Revision

Perseguire il miglioramento nella gestione del rischio di impresa

L'organizzazione **monitora 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.

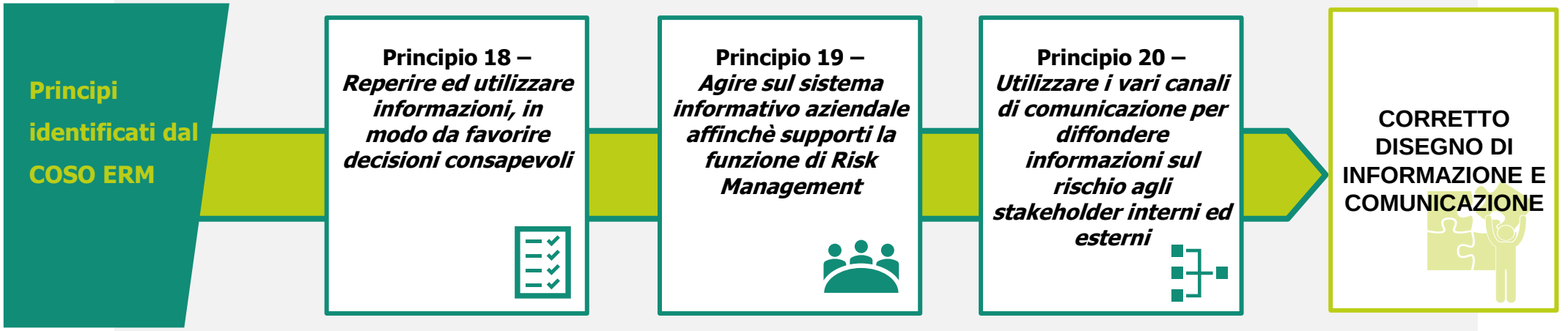
Condizioni ed opportunità nelle quali attuare correttamente il principio:

- **Nuove tecnologie:** Identificazione di nuove tecnologie quali opportunità per il miglioramento dell'efficienza dei processi (elaborazione, in tempo reale, di un'elevata mole di dati relativi all'andamento dei rischi aziendali)
- **Trend storici:** Revisione dei processi di *risk management* per indagare le cause di fallimenti accaduti nel passato
- **Propensione al rischio:** Revisione della performance della gestione dei rischi per valutare la revisione della propensione al rischio dell'organizzazione
- **Categorie di rischio:** Aggiornamento periodico del modello di categorizzazione dei rischi
- **Confronto con la concorrenza:** Identificazione dei competitor al fine di valutare se l'organizzazione sta operando in linea con le prestazioni del settore
- **Velocità di evoluzione del contesto:** Analisi del contesto imprenditoriale al fine di individuare opportunità di migliorare l'efficienza del proprio processo di gestione del rischio, in particolare tecnologico

Information, Communication & Reporting

Disporre di adeguate informazioni al fine di conoscere i rischi, garantire la continuità della strategia aziendale e adottare una visione di lungo periodo

Tale componente del Framework ERM evidenzia 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.**



Information, Communication & Reporting

Reperire ed utilizzare informazioni, in modo da favorire decisioni consapevoli

La **disponibilità**, la **qualità** e l'**utilizzo** di **informazioni rilevanti** permette all'Organizzazione di **anticipare situazioni** che potrebbero ostacolare il raggiungimento degli obiettivi strategici e di business ed **agire tempestivamente**.

L'efficacia della Gestione dei Rischi è strettamente correlata ad:

- **Affidabilità**
- **Tempestività**
- **Qualità**

delle **informazioni** necessarie al raggiungimento degli obiettivi strategici e di business.

Strumenti applicativi per la corretta attuazione del principio:

- **Sistemi di gestione dei dati**
- **Politiche di gestione delle informazioni con chiare linee di responsabilità**
- Processo di **Internal Audit** strutturato
- Sistemi di **business intelligence**
- **Software** per la raccolta delle informazioni
- **Applicativi** per la gestione del SCIGR
- Sistema di segnalazione delle violazioni **(whistleblowing)**
- **Sistemi contabili e gestionali**
- Sezioni dedicate dei **siti web**
- Partecipazione delle funzioni di controllo ai **management meeting**
- **Reporting** alle funzioni di controllo
- **Data Analytics**
- **Scambio di informazioni** tra funzioni di controllo
- Funzione **Investor Relations**

Information, Communication & Reporting

Agire sul sistema informativo aziendale affinchè supporti la funzione di Risk Management

L'organizzazione **comunica internamente la strategia e gli obiettivi aziendali a tutti i livelli della società**, in modo che ciascuno comprenda il proprio ruolo, ed **esternamente informa gli azionisti e le altre parti interessate** in merito alla **gestione dei rischi aziendali**.

Il processo di comunicazione tra l'organizzazione e gli stakeholder interni ed esterni deve produrre il **risultato** di

Attivare una comunicazione efficace in merito alle **modalità di gestione dei rischi aziendali,** trasmettendo ad ognuno le specifiche **responsabilità**

Strumenti applicativi per la corretta attuazione del principio:

- Comunicazioni relative al **risk appetite**
- **Riunioni trimestrali** del **CdA**
- **Riunioni straordinarie**
- **Comunicazioni al management della società**
- Relazione periodica dell'**Organismo di Vigilanza**
- Comunicazione degli **amministratori indipendenti** al CdA
- Indicazioni del **Comitato Controllo e Rischi**
- Relazione annuale del **Collegio Sindacale**
- Relazioni rilasciate dal **revisore**
- **Relazioni e verbali sul SCIGR**
- **Modello** di Organizzazione, Gestione e Controllo ex **D.Lgs. 231/2001**
- Comunicazione su **strumenti normativi e organizzativi**
- **Ordini di servizio o mandati** delle funzioni preposte ad attività di Controllo Interno
- Risultati del **Risk Assessment**
- **Risk & Control Matrix**
- **Piano di Internal Audit** Risk-based
- Evidenze ed esiti dei **test**
- Report dell'**Internal Audit**

Information, Communication & Reporting

Utilizzare i vari canali di comunicazione per diffondere informazioni sul rischio agli stakeholder interni ed esterni

Il management svolge nei confronti del Consiglio di Amministrazione un'attività di ***reporting*** il cui obiettivo è il **collegamento tra strategia, obiettivi aziendali, rischio e rendimento**. Inoltre un reporting efficace deve favorire la **discussione delle prestazioni dell'organizzazione** nel soddisfare la strategia, gli obiettivi e l'impatto del rischio.

I **report** combinano i**nformazioni quantitative e qualitative** sul rischio e variano nella loro forma ed estensione, in considerazione dei rischi presidiati e dei risultati da conseguire.

La **frequenza** dei report dovrebbe essere **commisurata alla gravità e alla priorità del rischio** che si vuole monitorare.

La **completezza e la correttezza dei dati** devono rispettare **adeguati livelli di assurance** sulla **veridicità** e **l'attendibilità delle fonti.**

Tipologie di Reporting

- **Report commerciali**: sintetici con informazioni comparabili nel tempo e che interessano un intero processo/area di riferimento
- **Report di audit:** informazioni dettagliate che forniscono una rappresentazione della rilevanza statistica e del grado di gravità
- **Report di risk management**: dati storici, informazioni relative a rischi potenziali, a rischi emergenti, alle analisi delle tendenze e ai cambiamenti nelle prestazioni