LUISS

Corso di laurea in Economia e Management

Cattedra Analisi e Contabilità dei Costi

Enterprise Risk Management: la gestione del rischio come leva strategica

Prof.ssa Adriana Rossi

RELATORE

Prof. Nicola D'Errico

CORRELATORE

Francesco Michelucci 229591

CANDIDATO

Anno Accademico 2024/2025

Indice:

1. Introduzione

Imprese e istituzioni operano oggi in uno scenario segnato da volatilità dei mercati, transizioni tecnologiche e regolatorie, interdipendenze globali e *shock*. In un contesto di questo tipo l'incertezza non è un'eccezione, ma una condizione strutturale: la sua gestione incide in modo diretto sulla definizione della strategia, sull'andamento delle performance e, in ultima istanza, sulla sostenibilità del modello di business nel medio-lungo periodo. Su questa base, l'elaborato indaga come integrare l'ERM con la strategia e con le tematiche ESG

In questo elaborato il rischio è considerato innanzitutto come informazione: un segnale sull'alea che condiziona il conseguimento degli obiettivi. Non soltanto minacce da contenere, dunque, ma anche opportunità da valutare e governare. Per renderlo comparabile tra aree diverse dell'organizzazione occorrono tassonomie coerenti, scale di severità e criteri di priorità che permettano di confrontare esposizioni eterogenee e di inserirle correttamente nel ciclo decisionale. In tale prospettiva, **l'Enterprise Risk Management** (ERM) è inteso come un'architettura organizzativa che allinea strategia, obiettivi e *performance*. L'integrazione dei riferimenti COSO ERM 2017 e ISO 31000:2018 consente di chiarire responsabilità di *governance*, definire il *risk appetite*, strutturare i processi di identificazione–valutazione–risposta–monitoraggio, adottare una visione a portafoglio delle esposizioni e integrare i flussi informativi nel *reporting* a supporto delle decisioni.

Saper gestire i rischi diventa così una **leva strategica**. Significa orientare scelte e allocazioni: collegare priorità ai piani e ai *budget*, confrontare alternative di *risk response* (evitare, ridurre, trasferire, accettare), valutare ritorni attesi e costi-opportunità, alimentare un *feedback loop* che apprende dagli esiti e rafforza la coerenza del profilo di rischio desiderato con la traiettoria di crescita dell'impresa. In altri termini, non si tratta di eliminare il rischio, ma di utilizzarlo per decidere meglio. Questa idea è ben sintetizzata dalla nota massima di Oscar Wilde: "Il grande vantaggio del giocare col fuoco è che non ci si scotta mai. Sono solo coloro che non sanno giocarci che si bruciano del tutto"[1]. Il punto non è quindi l'assenza di esposizione, ma la capacità di gestirla mediante la

[1] Wilde, O. (2003). *Aforismi e Massime.* Milano: Mondadori.

definizione di regole e limiti chiari. La stessa logica emerge nella riflessione di N. N. Taleb sui cigni neri[2] e sull'antifragilità[3]: in presenza di eventi rari e di grande impatto e di dinamiche a code pesanti, non basta resistere; occorre progettare sistemi che traggano beneficio dal disordine. L'ERM incorpora tali principi nella definizione del profilo di rischio, nei limiti operativi e nei cicli di revisione periodica.

Su queste basi si innesta la dimensione **ESG**, integrata nella panoramica dei rischi e quindi nell'ERM secondo la logica della doppia materialità. Quando rilevanti per il modello di business, gli aspetti ESG confluiscono nella mappa dei rischi, si riflettono nel *risk appetite* e negli obiettivi aziendali, entrano nei processi di pianificazione e nel *reporting*, diventando leve esplicite di decisione, resilienza e creazione di valore. La doppia materialità funge da ponte operativo tra impatto e *financial materiality*, rendendo tracciabile l'integrazione nel *risk universe*, nel *risk appetite* e nei KPI.

2. Fondamenti Teorici

Prima di analizzare in dettaglio l'Enterprise Risk Management (ERM), è opportuno chiarire i concetti fondamentali legati alla nozione di rischio, che rappresentano il pilastro teorico di qualsiasi approccio strutturato alla gestione dei rischi. Tale impostazione, coerente con quanto proposto dai principali standard internazionali, come il COSO ERM Framework e la norma ISO 31000, garantisce una progressione logica e una solida base concettuale per la trattazione di questo elaborato.

2.1 Definizioni e Tipologie di Rischio

Treccani definisce il **rischio** come l'"eventualità di subire un danno connessa a circostanze più o meno prevedibili"[4]. Questa definizione considera il rischio solamente nella sua componente negativa, tuttavia mostra già un concetto fondamentale, l'**incertezza**. Altra caratteristica della definizione economica di rischio è quella di **impatto**, ossia gli effetti generati dall'avverarsi della determinata situazione ipotetica.

[2] Taleb, N. N. (2007). *The Black Swan: The Impact of the Highly Improbable.* New York: Random House.
[3] Taleb, N. N. (2012). *Antifragile: Things That Gain from Disorder.* New York: Random House.
[4] https://www.treccani.it/enciclopedia/rischio/

Condensando questi due concetti possiamo arrivare ad una definizione del concetto di rischio più in linea con la materia trattata.

"*Risk is uncertainty that, if it occurs, will have a positive or negative effect on achievement of objective*"[5]

"Il rischio è l'incertezza che, se si verifica, avrà un effetto positivo o negativo sul raggiungimento dell'obiettivo"

In questa definizione di stampo economico possiamo riscontrare tutti gli elementi che saranno poi fondamentali per la gestione del rischio: **incertezza**, **probabilità**, **impatti** ed **obiettivi**. Tale accezione mostra la **natura dualistica del rischio**, aspetto cardine dei più moderni ed avanzati modelli di risk management, poiché se l'evento che si verifica ha un impatto negativo sugli obiettivi costituisce una **minaccia**, mentre se l'evento che si verifica genera un impatto positivo rappresenta un'**opportunità**.

Prendendo come riferimento i diversi criteri di classificazione dei rischi proposti sia dal COSO che dal World Economic Forum, è possibile individuare **due macrocategorie di rischi**: i rischi aziendali ed i rischi globali.

I **rischi aziendali** sono legati alle dinamiche organizzative e sono solitamente legati alle aree in cui questa è divisa:

- **Rischi finanziari**: sono legati all'operatività in ambito finanziario dell'impresa (processo di generazione o consumo di liquidità, rischio di credito, fluttuazioni su mercati finanziari, rischio di tasso di interesse…)
- **Rischi operativi**: sono associati alla gestione operativa dei processi aziendali (fattori umani, procedure interne, *supply chain*, *cyber risk*…)
- **Rischi strategici**: derivano dall'incertezza intrinseca associata al raggiungimento degli obiettivi di lungo periodo e alle decisioni strategiche (modifiche dello scenario competitivo, ingresso in nuovi mercati, incapacità di identificare e adattarsi alle tendenze di mercato…)
- **Rischi di conformità**: riguardano l'incapacità dell'organizzazione di adattarsi alle normative che interessano il proprio settore (ad esempio – a livello europeo – incapacità di applicare gli obblighi di reporting ESG…)

[5] Hillson, D. (2016). *The Risk management Handbook.* Kogan Page.

- **Rischi reputazionali**: comportano effetti negativi sulla percezione che il mercato ha di un'azienda o brand.

I **rischi globali**, invece, rappresentano "la possibilità che si verifichi un evento o una condizione che, se si verificasse, avrebbe un impatto negativo su una parte significativa del PIL globale, della popolazione o delle risorse naturali"[6]. Vengono definiti dal World Economic Forum (WEF) nel *global risk report* che li distingue in:

- **Rischi Sociali**: rischi legati a dinamiche sociali in grado di destabilizzare la società, come, polarizzazione, disuguaglianze, migrazioni o crisi sanitarie.
- **Rischi Tecnologici**: rischi derivanti da sviluppi tecnologici rapidi, abuso di tecnologie o vulnerabilità digitali che possono compromettere sicurezza e stabilità.
- **Rischi Geopolitici**: rischi derivanti da instabilità politica, conflitti tra stati o all'interno di essi, frammentazione geopolitica o uso di strumenti economici per scopi politici.
- **Rischi Ambientali**: rischi derivanti da cambiamenti climatici, disastri naturali o degrado ambientale che minacciano ecosistemi, popolazioni o infrastrutture.
- **Rischi Economici**: rischi legati a instabilità finanziarie, fluttuazioni di mercato, crisi economiche o politiche economiche che possono compromettere la crescita globale o la stabilità finanziaria.

2.2 Misurazione dei Rischi in Termini di Impatto e Probabilità

La gestione del rischio richiede una valutazione sistematica delle sue due componenti essenziali, probabilità (*likelihood*) ed impatto (*impact*). Su questi fattori trova fondamento una fase fondamentale del processo di gestione del rischio, il ***risk assessment***. Questa si sostanzia nell'attività di analisi e valutazione della probabilità ed impatto dei rischi, con il fine di stimarne la severità (*severity*) e stabilire priorità di trattamento e criteri di accettabilità coerenti con il contesto organizzativo e con l'orizzonte temporale degli obiettivi.

Lo strumento più utilizzato, per via della sua semplicità e immediatezza, per rappresentare in maniera grafica i rischi è la **matrice probabilità-impatto** (c.d. *Risk Assessment*

[6] WEF. (2025). *Global Risks Report 2025.* World Economic Forum.

Matrix). Mediante questo strumento, le due dimensioni del rischio vengono messe tra loro in relazione in modo tale da poter mappare i rischi su una griglia bidimensionale. Viene così generata una ***heat map*** che mostra con chiarezza i rischi più o meno critici per l'organizzazione mediante l'individuazione di diverse aree di accettabilità.

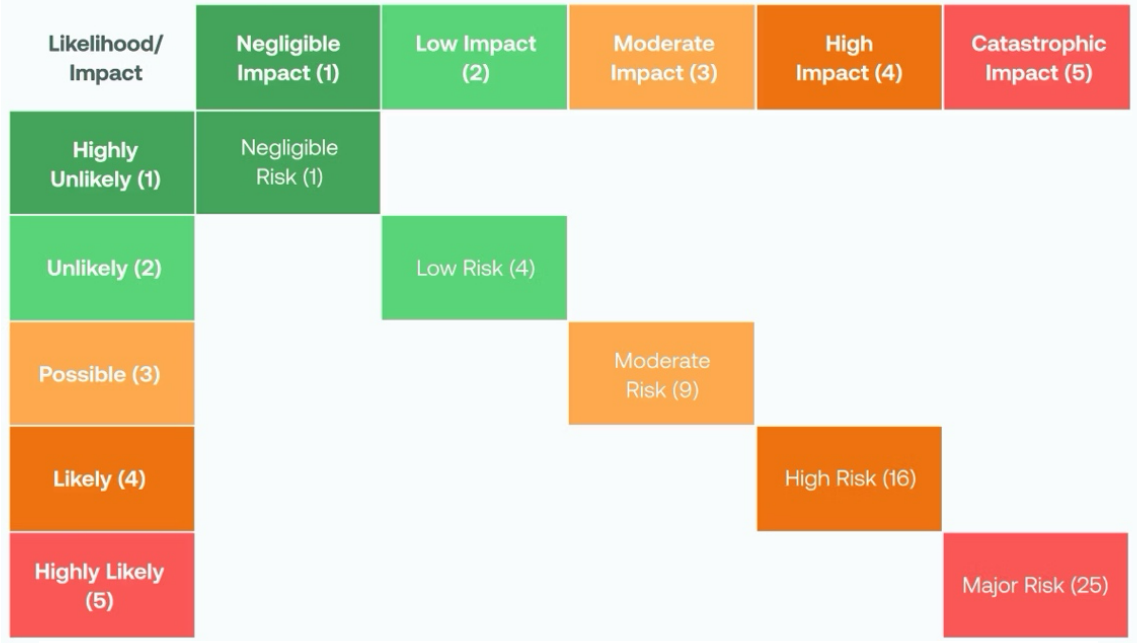

Figura 1. Matrice probabilità/impatto. Fonte: https://auditboard.com/blog/what-is-a-risk-assessment-matrix

Fondamentale per il corretto utilizzo di questo strumento di natura qualitativa/semi-qualitativa è la definizione di **scale di valutazione** che consentano di classificare i rischi in maniera sistematica e coerente attraverso l'intera organizzazione[7]. In questa prospettiva, Floreani[8] sottolinea l'importanza di predisporre scale **chiare e condivise**, capaci di tradurre sia la probabilità sia l'impatto in classi omogenee, rendendo così il processo di valutazione più trasparente e confrontabile, facilitando l'interpretazione dei risultati e il loro utilizzo da parte del *management*. Come evidenzia l'autore, la **probabilità** può essere descritta attraverso livelli qualitativi (ad esempio da molto bassa a molto alta) oppure, quando disponibili dati oggettivi, tramite intervalli quantitativi di frequenza o percentuali. L'**impatto**, invece, deve riflettere la gravità delle conseguenze sui principali obiettivi aziendali e può essere rappresentato con misure qualitative – spaziando da effetti trascurabili a conseguenze catastrofiche –, oppure attraverso metriche concrete quali perdite economiche, tempi di fermo o indicatori di reputazione.

[7] ISO, IEC. (2019). ISO/IEC 31010:2019 Risk Management - Risk Assessment Techniques.
[8] Floreani, A. (2004). *La valutazione dei rischi e le decisioni di risk management.* Milano: EDUCatt – ISU Università Cattolica.

Per Floreani la matrice non è solo uno strumento grafico, ma uno strumento operativo attraverso cui il rischio viene tradotto in termini decisionali generando *insights* in grado di supportare le decisioni manageriali. In questo senso, la **collocazione dei rischi** nella griglia consente di individuare immediatamente quelli che richiedono interventi urgenti rispetto a quelli accettabili[9]. I rischi situati nelle **aree a bassa criticità** (in verde) possono essere ritenuti accettabili; quelli nelle **aree ad alta criticità** (in rosso) risultano invece non accettabili e richiedono interventi immediati; i rischi **intermedi** (in giallo) necessitano di ulteriori analisi. In questa fascia, secondo Floreani[10], assume particolare rilevanza l'applicazione del principio ALARP (*as low as reasonably practicable*), che comporta una valutazione costo-beneficio per determinare fino a che punto sia ragionevole ridurre il rischio. Tale approccio consente di ottimizzare l'allocazione delle risorse, evitando sia eccessi di spesa per riduzioni marginali sia sottovalutazioni di rischi significativi.

Nonostante la sua ampia diffusione, la matrice probabilità-impatto presenta **limiti** e richiede alcune **cautele metodologiche**. Come osserva Floreani[11], le scale utilizzate sono per lo più di natura ordinaria e non consentono un'elaborazione matematica rigorosa: l'uso di indici, ottenuti dal prodotto P × I, può quindi generare un'illusione di precisione. Inoltre, il processo di collocazione dei rischi risente di una forte soggettività, che rende necessario predisporre scale e soglie chiare e documentate, in grado di assicurare coerenza tra valutatori e confrontabilità dei risultati. La matrice va dunque intesa come uno strumento di *screening* e prioritizzazione, utile per orientare le decisioni ma non sufficiente, da sola, ad esaurire la misurazione del rischio.

2.3 Rischi Emergenti, Resilienza e Sostenibilità

Negli ultimi cinque anni il panorama economico globale è stato scosso da una serie di avvenimenti che hanno generato impatti devastanti sugli equilibri internazionali in essere. Prima, in ordine di tempo, è stata la pandemia da COVID-19, iniziata nei primi mesi del 2020, che ha messo a dura prova le catene di approvvigionamento globali sviluppatesi

[9] Floreani, A. (2004). *La valutazione dei rischi e le decisioni di risk management.* Milano: EDUCatt – ISU Università Cattolica.
[10] Floreani, A. (2005). *Introduzione al risk management. Un approccio integrato alla gestione dei rischi aziendali.* Milano: Etas.
[11] Floreani, A. (2004). *La valutazione dei rischi e le decisioni di risk management.* Milano: EDUCatt – ISU Università Cattolica.

con il processo di globalizzazione innescata negli anni a cavallo del nuovo millennio. Successivamente, le crescenti tensioni geopolitiche, lo scoppio del conflitto tra Russia ed Ucraina nel febbraio del 2022 e l'improvviso aumento dell'inflazione hanno contribuito a ledere definitivamente gli equilibri economici internazionali. A queste dinamiche si sono aggiunti il conflitto a Gaza, gli attacchi degli Houthi alla navigazione nel Mar Rosso e più ampie tensioni regionali in Medio Oriente, aggravando i rischi logistici ed energetici e accrescendo l'incertezza. Si arriva così al 2025, anno in cui queste tensioni accumulatesi nel tempo hanno avuto sfogo, andando a generare un nuovo panorama economico portatore di profonde trasformazioni.

Il World Economic Forum (WEF) nel suo report "*Chief Economist Outlook – May 2025*"[12] evidenzia, mediante le opinioni di un *panel* di capi economisti internazionali, i **tre fondamentali *driver*** che avranno un maggior impatto sullo **scenario economico** nei prossimi anni: crescente volatilità dei mercati, incertezza sistemica ed intelligenza artificiale. Il primo driver, la **crescente volatilità dei mercati**, alimentato dalle crescenti tensioni geopolitiche, dal rafforzamento di politiche di nazionalismo economico e dalla minaccia dell'infiammarsi di una guerra commerciale tra i principali blocchi economici, contribuisce ad una maggior frammentazione dell'economia globale andando ad impattare direttamente sulle *value chain* accelerando i *trend* di *de-risking*, *friend-shoring* e ri-regionalizzazione delle catene del valore, con effetti permanenti su costi, tempi e investimenti. Secondo elemento di criticità, l'**incertezza sistemica**, derivante dall'aumento della volatilità dei mercati e dalla difficoltà di prevedere con adeguata confidenza l'evoluzione di scenari sempre più complessi, rende sempre più complicato ad aziende e istituzioni di prendere decisioni razionali. Infine, **l'intelligenza artificiale** è vista come una rivoluzione tecnologica in grado sia di generare impatti di breve periodo sia di apportare cambiamenti strutturali ai sistemi produttivi ed al mercato del lavoro.

Crescente Volatilità dei Mercati	Incertezza Sistemica	Intelligenza Artificiale
•Tensioni geopolitiche •Politiche di nazionalismo economico •Ipotesi di guerra commerciale	•Aumento di Volatilità dei Mercati •Difficoltà di effettuare previsioni attendibili	•Impatti di breve periodo •Possibili effetti strutturali sul mercato del lavoro

[12] WEF. (2025). *Chief Economists Outlook – May 2025.* World Economic Forum.

In questo contesto globale, caratterizzato da profonde discontinuità e rischi sistemici, diventa di fondamentale importanza definire un'ulteriore tipologia di rischio, il **rischio emergente**:

"*Either new risks or familiar risks that are evolving due to new or unfamiliar conditions*" [13]

"Rischi nuovi o rischi noti che stanno evolvendo a causa di condizioni nuove o sconosciute"

Le imprese devono quindi essere pronte ad affrontare questi rischi emergenti, adattando la propria governance e la propria struttura organizzativa al fine di non solo garantire la propria sopravvivenza ma anche di cogliere le opportunità che derivano direttamente da tali *shock*. In risposta a ciò, diventa quindi cruciale per le imprese integrare la resilienza nei propri processi decisionali e modelli di gestione, così da affrontare con efficacia l'incertezza.

2.3.1 Resilienza

La **resilienza** è "la capacità di un'organizzazione di superare gli *shock* esterni e cogliere le nuove opportunità che ne derivano"[14]. La resilienza è un concetto multifattoriale che dipende da come l'organizzazione nel suo insieme approccia l'incertezza. Come evidenziato dal World Economic Forum (WEF), in collaborazione con McKinsey (2022) nel *White Paper* "Resilience for Sustainable, Inclusive Growth", è possibile individuare **cinque *pillar*** che ne rappresentano i differenti aspetti:

- **Resilienza Operativa**: indica la capacità dell'impresa di continuare nella propria operatività durante, o a seguito, di uno *shock*.
- **Resilienza Strategica**: capacità di rispondere in maniera appropriata ai cambiamenti strutturali dell'ambiente in cui l'impresa opera.
- **Resilienza Finanziaria**: stabilità delle finanze aziendali a seguito di *shock* e la loro adeguatezza per affrontarli.

[13] Polchar, J., & Santamaria, N. A. (2024). Mapping Emerging Critical Risks. *Working Papers on Public Governance No. 78.* OECD (Organization for Economic Co-operation and Development)

[14] WEF, McKinsey. (2022). *Resilience for Sustainable, Inclusive Growth - White Paper.* World Economic Forum.

- **Resilienza Sociale**: le aziende operano all'interno di comunità, di conseguenza la loro resilienza è direttamente correlata a quella del tessuto sociale in cui l'impresa è stabilita, sia da un punto di vista sociale che politico.
- **Resilienza Organizzativa**: capacità della struttura organizzativa aziendale – da un punto di vista di: capitale umano, cultura e processi – di gestire l'incertezza.

Questi cinque *pillar* non sono da intendere come silos indipendenti, ma come **componenti strettamente legate tra loro**. Infatti, in caso di *shock*, l'incapacità dell'impresa di riprendersi non dipenderà da uno solo di essi, ma sarà il risultato dell'interrelazione di criticità in ognuno dei diversi componenti.

L'importanza della resilienza per un'organizzazione è mostrata chiaramente da una ricerca svolta dal WEF in collaborazione con McKinsey dove viene analizzato, sia dopo la crisi del 2009 che dopo la pandemia da COVID-19, come le aziende resilienti e non, si sono riprese dopo lo *shock* rispetto ad un valore di riferimento, in questo caso l'indice S&P 500. Facendo specifico riferimento allo *shock* pandemico, le imprese resilienti sono state in grado di generare il 10% di valore in più per i soci rispetto alle altre. Questo ha permesso loro di avere una crescita accelerata durante il periodo successivo.

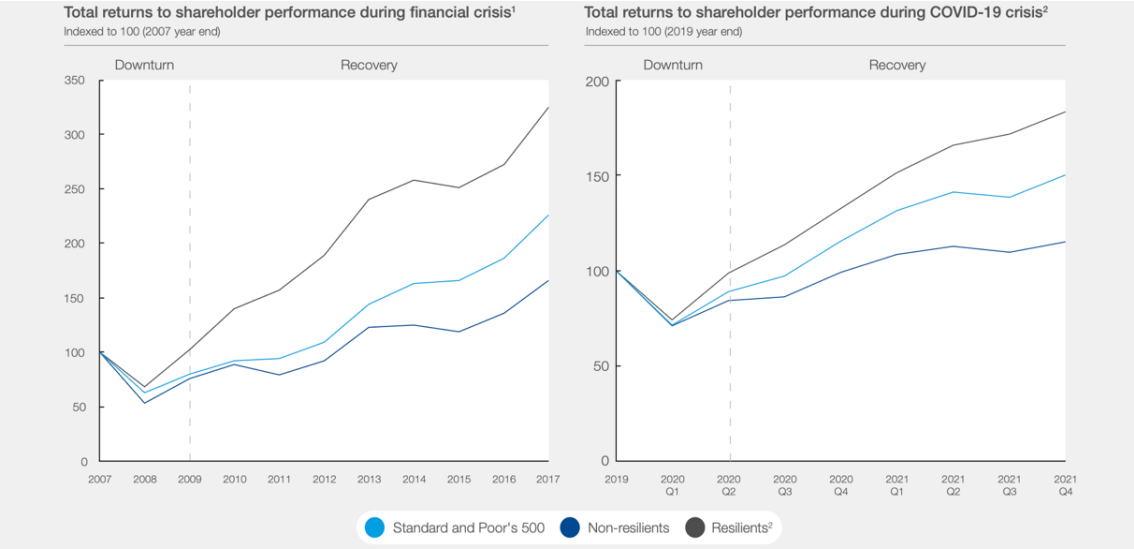

Figura 2. Fonte: WEF, McKinsey. (2022) Resilience for Sustainable Inclusive Growth

Le **aziende resilienti** sono meglio posizionate in un contesto sempre più complesso e ricco di rischi emergenti. Tuttavia, per competere non è sufficiente saper reagire: le organizzazioni necessitano di un ***business model* sostenibile**, orientato al lungo periodo, che consenta un posizionamento proattivo. Le organizzazioni resilienti sono in grado di generare maggior valore proprio perché fondano la loro strategia su un *business model*

sostenibile. In questa sede, il termine **sostenibilità** fa riferimento alla capacità di un modello di *business* di generare risultati economici stabili nel tempo, preservando e rigenerando le risorse critiche (finanziarie, produttive, organizzative e relazionali), mantenendo adattabilità rispetto ai cambiamenti competitivi. Tale accezione non coincide necessariamente con l'insieme delle tematiche ESG, che qui consideriamo rilevanti nella misura in cui sono materialmente connesse al *business*.

2.3.2 Sostenibilità e Business Model Innovation

Il mondo dell'impresa ha compreso che "la **sostenibilità** è diventata una priorità (…) grazie all'accumularsi di prove aneddotiche che dimostrano una maggiore redditività nel lungo termine[15]", inoltre rappresenta un **elemento fondamentale per creare resilienza e vantaggio competitivo di lungo periodo**. In quest'ottica per creare valore a lungo termine per i propri *stakeholder* le imprese devono includere nel proprio modello di business non solo la dimensione economica, ma anche quella sociale ed ambientale. Queste due "nuove" dimensioni, adeguatamente ricomprese all'interno del processo di pianificazione strategica, permettono al *management* di innovare il proprio piano di *business* integrando una visione di lungo periodo che tenga conto di impatti, responsabilità ed opportunità che altrimenti il *management* non sarebbe stato in grado di individuare.

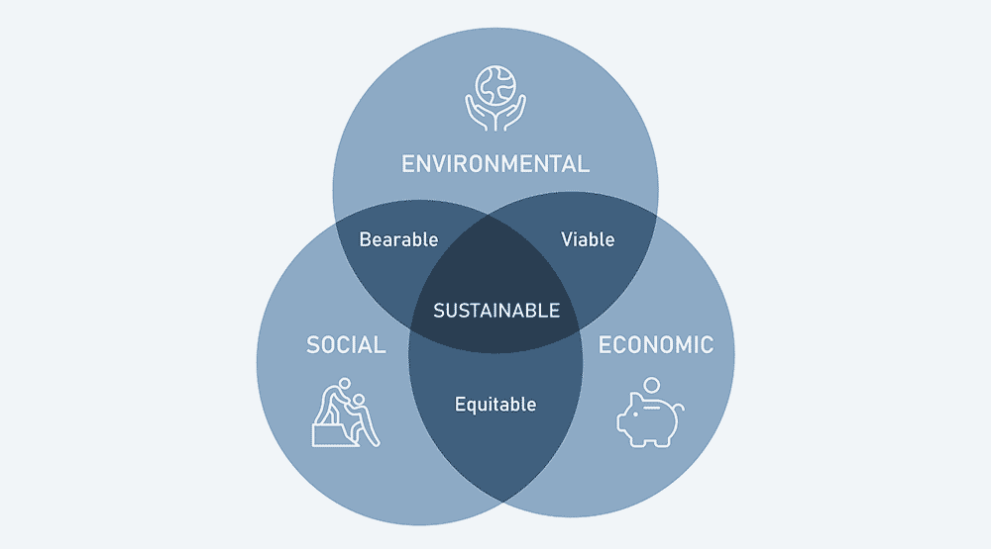

Figura 3. TBL model. Fonte: www.zenbird.media/3-pillars-of-sustainability-and-the-triple-bottom-line/

[15] Slaper, T. F., & Hall, T. J. (2011). The Triple Bottom Line: What is it and how does it work? *Indiana Business Review*, p. 4-8.

Il **Modello *Triple Bottom Line***, noto anche come modello delle 3P, permette di comprendere in maniera intuitiva come queste tre componenti sono tra loro correlate. Sviluppato nel 1994 da John Elkington, è un *framework* che si propone di espandere la tradizionale visione del successo aziendale affiancando alla *performance* economica (*profit*) anche quella del benessere sociale (*people*) e dell'impatto ambientale (*planet*). Per quanto riguarda la dimensione del **profitto**, tradizionalmente inteso come guadagno in termini finanziari, questa viene ampliata andando a ricomprendere l'impatto economico generato dalla gestione aziendale nei confronti di tutti gli *stakeholder*; le *performance* generate possono essere misurate ad esempio in termini di creazioni di posti di lavoro, pagamento di tasse ed investimenti sostenibili. Passando alla seconda dimensione del modello – le **persone** – questa, misura l'impatto sociale che l'azienda produce e può essere espressa in termini di *retention* dei dipendenti, *benefit* aziendali ed etica nella catena del valore. Infine, la dimensione del **pianeta**, riguarda l'impatto ambientale e ricomprende tutte le attività aziendali volte a minimizzare o eliminare i danni ambientali, ad esempio mediante l'utilizzo di energie rinnovabili o riduzione dell'emissione di anidride carbonica (CO_2).

L'adozione di questa nuova **prospettiva multifattoriale** del concetto di *performance* consente alle imprese di prendere decisioni più etiche e responsabili e, mediante l'integrazione di questi valori all'interno del processo di pianificazione strategica, permette di indirizzare le decisioni di lungo periodo in una direzione di sviluppo sostenibile. Questo cambiamento pone le imprese di fronte alla necessità di **innovare il proprio modello di *business*** "attraverso la ridefinizione dello scopo dell'azienda e della logica di creazione di valore, nonché un ripensamento della percezione del valore"[16] con il fine di sviluppare una visione sostenibile di lungo periodo.

Un esempio di *business model innovation* è rappresentato da **WashPass di Haier**[17], un servizio che sposta il fulcro della proposta di valore dalla transazione avente ad oggetto un bene durevole alla fornitura continuativa di un servizio (*wash-as-a-service*). Il cliente, a fronte del pagamento di un canone mensile riceve: una lavatrice connessa in comodato

[16] Bocken, N. M., Short, S. W., Rana, P., & Evans, S. (2014). A literature and practice review to develop sustainable business model archetypes. *Journal of Cleaner Production*, 42-56.

[17] Haier. (s.d.). *Washpass by Haier*. Tratto da Haier: https://subscriptions.haier-europe.com/it_IT/washpass/

d'uso, un sistema smart di detergenti proprietari – le quali ricariche sono comprese nell'abbonamento – ed una piattaforma digitale che consente il controllo remoto del sistema. Mediante quest'offerta, Haier **riconfigura l'intero sistema di valore**: la *value proposition* non risiede più nella sola *performance* tecnica dell'elettrodomestico, ma nell'esito d'uso (qualità del lavaggio, semplicità, affidabilità del risultato). La *companion app*, diventa l'interfaccia di servizio, tramite la quale il cliente delega all'algoritmo la gestione ottimale delle impostazioni riguardanti il lavaggio. Grazie a questa proposta, Haier è in grado di trasformare i ricavi una tantum in un flusso costante e prevedibile, mentre l'uso dei consumabili proprietari ed il sistema digitale creano un *lock-in "soft"* dell'utente. Inoltre, l'integrazione IoT-chimica-piattaforma funge da *asset* complementare difficile da imitare da parte della concorrenza costituendo di fatto un vantaggio competitivo sostenibile. Il caso WashPass dimostra come la *business model innovation* non consista soltanto nell'introduzione di nuove tecnologie, ma nella ridefinizione del processo stesso di creazione e cattura del valore. Attraverso la transizione da prodotto a servizio, Haier evidenzia come la riconfigurazione della proposta di valore e dei meccanismi di *revenue* possa costituire una leva strategica per accrescere resilienza, rafforzare il legame con gli *stakeholder* e generare vantaggio competitivo di lungo periodo.

2.4 Risk Management ed Enterprise Risk Management

Questo nuovo modo di intendere l'impresa ed il proprio *business model* porta con sé la necessità di raccogliere ed elaborare molte più informazioni da parte dei sistemi aziendali, in modo da offrire al *management* una visione più completa su tutte le nuove prospettive che deve tenere in considerazione nel proprio processo decisionale. Inoltre, lo sguardo di lungo periodo e la consapevolezza di essere inseriti in un contesto economico sempre più complesso ed interconnesso richiedono lo sviluppo di sistemi interni in grado di gestire questi ulteriori elementi caratterizzanti l'incertezza.

Il **Risk Management**, ed ancora in maniera più completa l'**Entreprise Risk Management,** nascono come risposta a queste necessità e si propongono come approcci volti a fornire alle organizzazioni strumenti, processi e strutture per identificare, valutare e affrontare i rischi. L'incertezza viene così trasformata in una leva strategica in grado non solo di proteggere il valore ma anche di crearlo in un'ottica di lungo periodo.

2.4.1 Definizione

Minacce ed opportunità – come indicato nel paragrafo 2.1 – sono due dimensioni opposte ma inscindibili di uno stesso concetto, il rischio. Il ***Risk Management*** si presenta come un insieme di tecniche, strumenti e procedure volte a gestire i rischi; questi, infatti, per via della loro natura duale sono impensabili da rimuovere completamente in quanto questo comporterebbe come diretta conseguenza l'eliminazione di ogni possibilità di rendimento.

L'***Enterprise Risk Management*** (ERM), prende il concetto di gestione del rischio e lo adatta alle necessità delle imprese, si presenta quindi come un approccio sistematico, integrato ed olistico ai rischi che possono influenzare le performance aziendali.

Definizione ERM dell'International Organization for Standardization (**ISO**):

"*coordinated activities to direct and control an organization with regard to risk*" [18]

"attività coordinate volte a dirigere e controllare un'organizzazione in relazione al rischio"

Definizione ERM del Committee of Sponsoring Organizations of the Treadway Commission (**COSO**):

"*is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives*" [19]

"è un processo, attuato dal consiglio di amministrazione, dalla direzione e da altro personale, applicato nella definizione della strategia e in tutta l'impresa, volto a identificare potenziali eventi che potrebbero influire sull'entità e a gestire il rischio in modo che rimanga entro i limiti della sua propensione al rischio, al fine di fornire una ragionevole garanzia circa il raggiungimento degli obiettivi dell'entità"

Come si evince da entrambe le definizioni, l'ERM non è una funzione, bensì un **processo** del quale fa parte ogni soggetto coinvolto nell'organizzazione a partire dal *top*

[18] ISO. (2018). ISO 31000:2018 Risk Management - Guidelines.
[19] COSO. (2004). Enterprise risk management - Integrated Framework.

management sino al personale operativo. In questo sistema ogni soggetto ha le proprie responsabilità e partecipa alla gestione collettiva dei rischi aziendali, del resto questi difficilmente riguardano una funzione specifica, ma possono altresì interessare più funzioni o addirittura l'organizzazione nella sua interezza. La stessa COSO, nel suo framework, indica che l'ERM è più efficace quando è parte integrante della struttura aziendale ed è inserito in maniera nativa nei processi decisionali. La natura olistica di questo processo è ulteriormente evidenziata dal fatto che deve essere applicato "*across the enterprise*", in questo senso i flussi informativi prodotti dalle varie unità aziendali devono andare a confluire in un unico sistema informativo in grado di fornire ai singoli attori le migliori informazioni possibili per supportare il loro processo decisionale. Quest'ultimo punto evidenzia inoltre un principio cardine del sistema ERM, quello della condivisione delle informazioni con gli stakeholder interessati; infatti, mediante il coinvolgimento di soggetti terzi – a seconda del grado di analisi: alla singola unità, funzione aziendale o impresa stessa – permette di generare importanti *insights* utili ad ampliare la visione del rischio ed a perfezionare l'*output* del processo di *decision-making*.

2.4.2 Indole Iterativa dell'ERM

L'ERM non è un processo statico, ma richiede di essere costantemente rivisto ed adattato rispetto ai cambiamenti che colpiscono sia l'ambiente interno che quello esterno all'organizzazione. La natura iterativa del processo di Enterprise Risk Management è direttamente collegata alla natura dinamica dei rischi, i quali evolvono nel tempo in funzione di nuove tecnologie, mutamenti normativi, fattori geopolitici o trasformazioni nei modelli di business.

Liz Taylor[20], applica al processo di implementazione dell'ERM la struttura ciclica tipica del **modello PDCA** (*Plan/Do/Check/Act*) proposta da Deming – questo stesso approccio è riscontrabile nella struttura dei framework elaborati sia dalla ISO che dal COSO – e procede a suddividere le fasi basilari del sistema all'interno delle quattro componenti del modello.

[20] Hillson, D. (2016). *The Risk management Handbook.* Kogan Page.

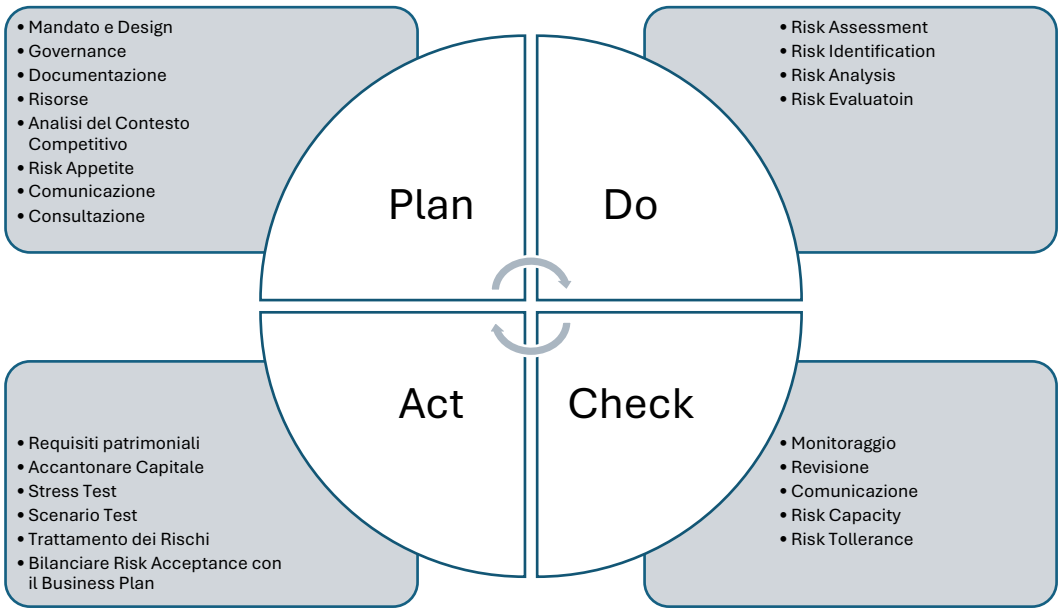

Figura 4. Rappresentazione del processo ERM mediante modello PDCA

Nella prima fase del modello (***Plan***) l'impresa si occupa di tutte quelle attività che le permetteranno di affrontare l'incertezza. Dopo la delibera da parte del CdA di avviare il processo di sviluppo dell'ERM si procede con la **definizione della *governance*** del rischio, ossia si identificano i soggetti sui quali graverà la responsabilità di occuparsi di una specifica parte del processo di *risk management*. Successivamente verrà **analizzato il contesto**, sia interno che esterno all'azienda, ed in base a questo verrà **identificato il *risk appetite*** (esposizione al rischio) ossia la quantità di rischi che l'azienda è disposta ad assumersi nel conseguimento dei propri obiettivi.

La seconda fase (***Do***) riguarda lo svolgimento di tutte quelle attività che sono direttamente collegate alla valutazione del rischio (*risk assessment*). In questa fase si procede quindi a **identificare i rischi** ai quali l'organizzazione è esposta arrivando così a definire il *risk universe*, un documento nel quale sono indicati tutti i rischi che possono condizionare concretamente gli obiettivi aziendali. Successivamente questi vengono **analizzati** comprendendone la natura, gli impatti – sia quantificandoli che identificando che aree aziendali impattano – e la probabilità con cui possono avvenire. Infine, si procede ad una loro **classificazione** e **valutazione** per decidere che strategia di trattamento adottare.

Nella terza fase (***Check***), si procede controllando se il risultato delle attività della fase precedente è in linea con quanto pianificato. Si comparano quindi i risultati del processo di *risk assessment* con il *risk appetite* definito inizialmente, sia analizzando i rischi

singolarmente sia in maniera aggregata. Inoltre, viene definito il ***risk tollerance***, ossia il livello massimo di variabilità delle performance rispetto a quanto preventivato.

Nella quarta ed ultima fase (***Act***) l'organizzazione procede ad operare basandosi su quanto il processo di ERM ha prodotto finora. Si individuano i **requisiti patrimoniali** per attuare i piani di trattamento del rischio e, in caso di necessità, si accantonano opportuni fondi. Vengono inoltre effettuati *stress test* e *scenario test* per **verificare il corretto funzionamento** delle strategie di gestione del rischio ed individuare eventuali punti critici da dover affrontare. Infine, sulla base di quanto appreso sino a questo punto, l'impresa procederà ad **operare opportune modifiche** al proprio modello di ERM per renderlo adatto ad affrontare la realtà dinamica dei rischi.

La **natura iterativa** del processo di ERM porta con sé diversi **benefici**. Diversi autori[21] sottolineano come questa tipologia di approccio graduale e ciclico consenta di partire da un perimetro operativo limitato, per poi espandere progressivamente il programma di gestione dei rischi, migliorando lungo il percorso grazie alle lezioni apprese e all'adattamento organizzativo. Inoltre, permette di affinare, ciclo dopo ciclo, le metodologie utilizzate, le fonti informative e il coinvolgimento degli stakeholder decisionali, contribuendo così a rendere l'ERM un sistema flessibile, resiliente e realmente integrato nella governance aziendale.

2.4.3 Benefici di un ERM Integrato

Per definizione, l'Enterprise Risk Management non è un insieme di pratiche gestite "a silos": è un processo integrato che collega in modo sistematico rischi, strategia e performance. L'adozione di un sistema strutturato di Enterprise Risk Management rappresenta quindi un passaggio strategico fondamentale ed ineludibile per le organizzazioni che intendono affrontare con consapevolezza l'incertezza e la complessità del contesto competitivo attuale.

Nelle **organizzazioni prive di un sistema ERM**, le decisioni assunte dal vertice aziendale si basano frequentemente su processi di reportistica frammentati e non omogenei. Tali processi sono spesso affidati a una pluralità di attori interni che, pur

[21] von Känel, J., Cope, E. W., Deleris, L. A., Nayak, N., & Torok, R. G. (2010). Three Key Enablers to Successful Enterprise Risk Management. *IBM Journal of Research and Development, 54*(3), p. 1-15.

utilizzando le medesime basi informative, tendono a rielaborarle in modo disomogeneo e non coordinato, generando ridondanze, inefficienze e potenziali incoerenze nei dati trasmessi. Al contrario, nelle **organizzazioni dotate di un sistema ERM integrato**, il processo di reportistica si fonda su un'unica base dati condivisa. Ciascuna funzione aziendale è responsabile dell'elaborazione delle informazioni di propria competenza, contribuendo alla costruzione di un flusso informativo coerente, tracciabile e ad alto valore aggiunto. In tal modo, il vertice aziendale può disporre di un quadro informativo più affidabile e tempestivo, utile a supportare decisioni strategiche maggiormente consapevoli e orientate alla gestione proattiva dei rischi.

Lo stesso COSO, nell'*executive summary* del framework del 2017 individua una serie di **vantaggi** che le imprese che integrano un **processo di ERM strutturato** possono ottenere. In primo luogo, l'ERM consente un miglioramento nella capacità di cogliere nuove opportunità, grazie a una visione più consapevole del contesto di rischio in cui l'organizzazione opera. Inoltre, favorisce una gestione più efficace dei rischi trasversali all'intera organizzazione (*entity-wid*e), superando così approcci frammentati e settoriali. Tra gli altri vantaggi rilevati si annoverano l'incremento delle performance positive, la riduzione della probabilità di eventi negativi inattesi e una minore variabilità nei risultati aziendali, elementi fondamentali per garantire stabilità e continuità operativa. L'ERM contribuisce anche a un miglioramento nell'allocazione delle risorse, poiché permette di indirizzare gli sforzi aziendali verso ambiti prioritari e maggiormente critici. Infine, l'adozione di un sistema integrato di gestione del rischio comporta un rafforzamento della resilienza organizzativa, rendendo l'impresa più pronta ad affrontare e superare situazioni di crisi o discontinuità.

3. Framework di Riferimento

Nel panorama dell'Enterprise Risk Management, i legislatori non prescrivono un *framework* specifico da adottare, lasciando alle aziende la libertà di sviluppare il sistema di gestione del rischio più adatto alle specifiche esigenze. Tuttavia, la necessità di avere delle linee guida chiare e che possano indirizzare le organizzazioni nello sviluppo di un sistema ERM integrato e performante, ha spinto diverse istituzioni a sviluppare degli standard di riferimento.

Due pilastri fondamentali in questo ambito sono: il COSO *Enterprise Risk Management–Integrating with Strategy and Performance* e lo standard ISO31000:2018. Il primo, elaborato dal Committee of Sponsoring Organization of the Treadway Commission (**COSO**), sviluppa un modello incentrato nell'integrazione della gestione del rischio nei processi decisionali della *governance* aziendale. Il secondo, sviluppato dalla Intenational Organization of Standardization (**ISO**), propone linee guida universali e flessibili per implementare processi di risk management efficaci ed applicabili ad organizzazioni di ogni dimensione e settore.

Nonostante i differenti approcci adottati dai due modelli, questi *framework* non si escludono reciprocamente; al contrario, si completano, andando così a disegnare un sistema che promuove una gestione del rischio non più meramente miope e passiva, ma integrata e proattiva. Una vera e propria leva strategica da sfruttare per assumere decisioni più consapevoli e per affrontare con maggiore preparazione l'incertezza che sempre di più caratterizza il panorama economico.

3.1 COSO ERM Integrated Framework

Il COSO[22] **(Committee of Sponsoring Organizations of the Treadway Commission)** nasce nel 1985 come iniziativa congiunta di organismi professionali statunitensi per migliorare l'affidabilità della rendicontazione finanziaria e rafforzare controllo interno, gestione del rischio e governance. Nel tempo, è divenuto un riferimento internazionale per la definizione di *framework* che orientano prassi e regolazione, con un'evoluzione che dal controllo interno è approdata alla gestione integrata dei rischi in relazione a strategia e *performance*.

Nel 2004 – paragrafo 3.1.1 – il COSO pubblica "*Enterprise Risk Management: Integrated Framework"*, che estende l'orizzonte del precedente "*Internal Control: Integrated Framework"* del 1992. Con questa prima iterazione si passa dalla centralità del controllo contabile ad una visione più ampia di gestione dei rischi a supporto della creazione e protezione del valore.

Nel 2017 – paragrafo 3.1.2 – con il *framework "Enterprise Risk Management: Integrating with Strategy and Performance"* avviene un fondamentale cambio di paradigma: l'ERM

[22] https://www.coso.org/about-us

viene esplicitamente integrato nella pianificazione strategica e nella misurazione delle *performance*, abbandonando la rappresentazione "a cubo" a favore di 5 componenti e 20 principi fortemente interconnessi. L'enfasi si sposta dalla sola mitigazione alla creazione di valore nel tempo attraverso scelte informate sul profilo di rischio.

3.1.1 COSO ERM Framework – 2004

La prima iterazione del *framework* ERM redatto dal COSO, pubblicato nel 2004, si inserisce in un contesto economico-finanziario turbolento, diretta conseguenza della crisi scatenata dallo scoppio della bolla speculativa delle dot-com. I primi anni del 2000 sono infatti scossi da un repentino crollo delle valutazioni dei titoli tecnologici che ha comportato una diffusa instabilità nei mercati ed un grave deterioramento della fiducia degli investitori. Ad aggravare ulteriormente la situazione si sono aggiunti numerosi scandali societari di portata rilevante – tra i quali Enron, WorldCom e Tyco – che hanno evidenziato tutti i limiti e le debolezze intrinseche ai sistemi di controllo interno e di governance che caratterizzavano la quasi totalità delle imprese.

Questa situazione di tensione ha spinto il legislatore americano ad intervenire con numerose riforme – tra cui il *Sarbanes-Oxley Act* – con lo scopo di richiedere alle aziende quotate la certificazione dell'efficacia dei controlli interni e imporre nuovi obblighi di trasparenza ed *auditing*. Si venne così a creare l'esigenza di un *framework* che superasse i limiti dei tradizionali sistemi di controllo contabile.

Proprio come risposta alle necessità di questo nuovo contesto normativo COSO presenta nel 2004 il suo primo *framework* in ambito ERM, denominato "*Enterprise Risk Management – Integrated Framework"*. Questo nuovo *standard* si propone di "estendere il controllo interno in una visione più ampia, focalizzata sulla creazione e protezione del valore aziendale nel lungo periodo"[23]. Procedendo in quest'ottica, il *framework* del 2004 non soppianta il precedente ("*Internal Control – Integrated Framework",* 1992) ma lo incorpora e ne amplia l'ambito applicativo, incorporando dimensioni fondamentali quali la definizione degli obiettivi strategici, l'identificazione degli eventi potenzialmente impattanti, e la valutazione dei rischi connessi all'intera attività d'impresa.

[23] COSO. (2004). Enterprise risk management - Integrated Framework.

In questa prima versione, è prevalente l'impostazione secondo cui l'ERM si presenta come un'estensione del preesistente sistema di controllo interno.

Il *framework* parte dalla definizione delle **quattro tipologie di obiettivi aziendali**. La fase di identificazione degli obiettivi viene vista come precondizione necessaria per poter successivamente effettuare tutte le analisi associate ai rischi. Questi sono:

- **Obiettivi strategici**: obiettivi di alto livello, riguardano il raggiungimento di quanto l'impresa si è fissata nei suoi piani strategici.
- **Obiettivi operativi**: riguardano le attività *day-by-day*, sono principalmente legati all'uso efficace ed efficiente delle risorse aziendali.
- **Obiettivi di reporting**: affidabilità dei dati raccolti dal sistema aziendale di controllo interno.
- **Obiettivi di compliance**: conformità alle norme e regolamenti cui l'impresa è sottoposta.

A questi vengono affiancati gli **otto componenti dell'Enterprise Risk Management**:

- **Ambiente interno**: è relativo ai principi e valori che guidano i comportamenti dell'organizzazione. Influenza come il rischio è percepito all'interno dell'organizzazione e quanto questa è in grado di sopportarne.
- **Definizione degli obiettivi**: come osservato in precedenza, la definizione degli obiettivi aziendali è un prerequisito per l'individuazione dei rischi.
- **Identificazione degli eventi**: eventi interni ed esterni che possono influenzare il raggiungimento degli obiettivi identificati. Attività che consente la definizione dell'universo dei rischi (*risk universe*).
- **Risk assessment**: analisi dei rischi in base alla loro probabilità di avvenire ed il loro impatto sugli obiettivi.
- **Risk response**: il *management* decide le modalità con cui rispondere ai rischi: evitandoli, accettandoli, riducendoli, o condividendoli.
- **Attività di controllo**: creazione di procedure per assicurarsi che l'organizzazione risponda nella maniera preventivata.
- **Informazione e comunicazione**: le informazioni rilevanti per gli *stakeholders*, sia interni che esterni, vengono raccolte, elaborate e comunicate. Questo permette ai vari soggetti interessati di adempiere alle proprie responsabilità.

- **Monitoraggio**: fase finale del processo. L'ERM è per sua stessa natura un sistema in divenire, questa è la fase di apprendimento che consente all'organizzazione di migliorare le proprie risposte future.

Ulteriore elemento distintivo e peculiare è la **matrice tridimensionale**, una rappresentazione grafica elaborata dalla stessa COSO che permette di visualizzare graficamente il sistema di ERM nelle sue tre dimensioni: **componenti del sistema** (frontalmente), **categorie di obiettivi** (lato superiore), e **livelli organizzativi** (lateralmente). "Questa rappresentazione illustra la capacità di concentrarsi sull'insieme della gestione del rischio aziendale di un'entità, oppure per categoria di obiettivi, componente, unità dell'entità o qualsiasi sottoinsieme di questi"[24].

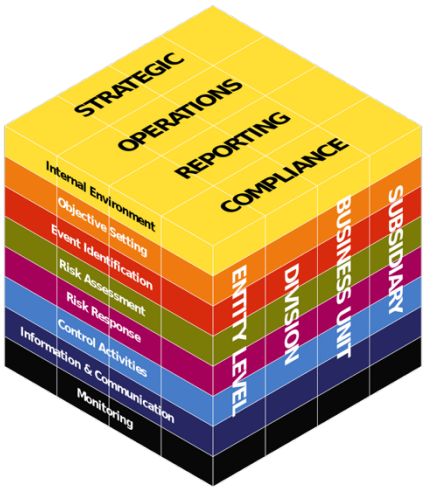

Figura 5. Matrice tridimensionale ERM. Fonte: COSO. (2004). Enterprise risk management - Integrated Framework

Nonostante il COSO *Enterprise Risk Management – Integrated Framework* del 2004 abbia rappresentato un punto di riferimento fondamentale per strutturare processi di gestione del rischio aziendale, la sua applicazione ha suscitato diverse **critiche** in letteratura accademica e professionale. Tra le varie spiccano in particolate:

- Eccessiva complessità ed orientamento teorico: l'essere un processo "meccanico" definito in maniera top-down e astratto dai processi organizzativi reali, risultando in una visione semplicistica dell'azienda[25];
- Natura prescrittiva, che lo rende poco adattabile alle mutevoli realtà aziendali che dovranno applicarlo[26];
- Mancanza di indicazioni pratiche nell'implementazione del *framework*[27];

[24] COSO. (2004). Enterprise risk management - Integrated Framework.
[25] Power, M. (2007). *Organized uncertainty: designig a world of risk management.* Oxford University Press.
[26] Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise Risk Management: Review, Critique, and Research Directions. *Long Range Planning, 48*, 265-276.
[27] Fraser, J., Schoening-Thiessen, K., & Simkins, B. (2010). Who reads what most often?: A survey of enterprise risk management literature. In J. Fraser, & B. Simkins, *Enterprise risk management: Today's leading research and best practices for tomorrow's executives* (p. 399-401). John Wiley & Sons.

- Mancanza di integrazione tra il *risk management* e la pianificazione strategica: questo ha portato le aziende a sviluppare i due processi come silos separati, inficiando la capacità di identificare rischi e di raggiungere gli obiettivi[28].

3.1.2 COSO ERM Framework – 2017

L'evoluzione del contesto economico e normativo, sempre più articolato e interconnesso, unita all'emergere di nuovi rischi e alla crescente consapevolezza delle criticità strutturali del *framework* del 2004, ha spinto il COSO a rivedere l'approccio tradizionale all'Enterprise Risk Management. In risposta a tali esigenze, nel 2017 è stato pubblicato il nuovo documento intitolato "*Enterprise Risk Management – Integrating with Strategy and Performance"*, il quale non si presenta solo come un aggiornamento, ma introduce un vero cambio di paradigma. Nel nuovo *framework*, l'ERM non è più concepito come un'estensione del sistema di controllo interno ed orientato prevalentemente alla mitigazione dei rischi. Bensì si evolve in una vera e propria leva strategica in grado di supportare il processo decisionale.

Tuttavia, la principale critica che affronta e supera è quella relativa all'integrazione dell'ERM con il processo di pianificazione strategica. COSO stessa sottolinea "*the importance of enterprise risk management in strategic planning and embedding it throughout an organization—because risk influences and aligns strategy and performance across all departments and functions*"[29]. In quest'ottica viene totalmente rimossa la struttura precedente – graficamente rappresentata dal cubo ERM – e viene sostituita da una molto più snella, organizzata in 5 componenti tra loro strettamente correlati, articolati a loro volta in una serie di 20 principi.

[28] Pierce, E., & Goldstein, J. (2016). Moving from enterprise risk management to strategic risk management: Examining the revised COSO ERM framework. Research Gate.

[29] COSO. (2017). Enterprise Risk Management - Integrating with Strategy and Performance - Executuve Summary.

Figura 6. Processo ERM. Fonte: COSO. (2017). Enterprise Risk Management - Integrating with Strategy and Performance

Governance e Cultura: l'organo di governo societario definisce il "tono" dell'organizzazione in ambito di propensione al rischio e stabilisce le responsabilità di supervisione. La cultura riguarda i valori etici ed i principi che guidano i comportamenti dei soggetti coinvolti nell'organizzazione.

1. **Supervisione del rischio da parte del board**: il Consiglio di Amministrazione elabora e supervisiona la strategia ed i rischi che possano inficiarne il raggiungimento.
2. **Istituire strutture operative**: sviluppo di una struttura organizzativa in grado di perseguire la strategia e gli obiettivi aziendali.
3. **Definire la cultura organizzativa**: definire i principi che orientano l'operatività dei soggetti coinvolti in azienda.
4. **Dimostrare impegno verso i valori fondamentali**
5. **Attrarre, Sviluppare e Trattenere il personale competente**: impegno nello sviluppo del capitale umano in linea con la strategia e gli obiettivi aziendali.

Strategia e Obiettivi: ERM, strategia e obiettivi diventano componenti integranti della pianificazione strategica. Propensione al rischio e strategia vengono allineati, gli obiettivi aziendali derivano e mettono in pratica la strategia e costituiscono le fondamenta per identificare, valutare e rispondere ai rischi.

6. **Analisi del contesto**: analisi potenziale impatto del contesto aziendale sul profilo di rischio.
7. **Definizione della propensione al rischio**: definizione della propensione al rischio caratteristica dell'impresa.
8. **Valutazione delle alternative strategiche**: valutazione delle strategie alternative ed il loro potenziale impatto sul profilo di rischio.
9. **Formulazione degli obiettivi**: integrare considerazioni sui rischi nella fase di definizione degli obiettivi a vari livelli in modo tale da garantire allineamento alla strategia.

Performance: identificati i rischi che posso avere un impatto rilevante nel raggiungimento degli obiettivi aziendali, questi vengono classificati in base all'impatto generato, alla loro probabilità di avvenire ed alla propensione al rischio. L'organizzazione procede poi ad elaborare come rispondere ed adotta una visione di portafoglio.

10. **Identificazione dei rischi:** identificazione dei rischi che hanno un impatto rilevante sulle performance aziendali.
11. **Valutazione della gravità dei rischi**
12. **Ordinare i rischi per priorità**
13. **Implementare risposte ai rischi**
14. **Sviluppare una "Visione a portafoglio" dei rischi**

Revisione e Miglioramento: attraverso la revisione della propria *performance*, l'organizzazione può valutare l'efficacia del sistema elaborato, ed alla luce di cambiamenti sostanziali, definire i perfezionamenti da apportare.

15. **Valutazione dei cambiamenti:** identificare e valutare i cambiamenti in grado di influenzare in modo sostanziale le performance aziendali.
16. **Revisione dei rischi e delle performance**
17. **Miglioramento continuo dell'ERM**

Informazione, Comunicazione e *Reporting*: l'ERM per funzionare correttamente necessita di un processo continuo di ottenimento e condivisione delle informazioni, sia da fonti interne che esterne, che fluiscono verso l'alto, verso il basso e attraverso l'organizzazione stessa.

18. **Utilizzo dell'IT**: utilizzare i sistemi informativi e tecnologici per supportare la gestione del rischio aziendale.
19. **Comunicazione dei rischi**: comunicazione dei rischi individuati e delle attività intraprese per affrontarli agli *stakeholder* interni ed esterni, i quali possono trarne vantaggio per il loro operato.
20. **Reporting su rischio, cultura e performance**: fornire report sul rischio, sulla cultura e sulle performance ai vari livelli dell'organizzazione per supportare il loro processo di *decision-making* e per garantire allineamento con la strategia ai vari livelli aziendali.

3.2 ISO 31000:2018

ISO (*International Organization for Standardization*) è un'organizzazione internazionale indipendente, non governativa, fondata nel 1947, composta dai rappresentanti degli enti di normazione nazionali di oltre 160 paesi. Si occupa di sviluppare *standard* internazionali per garantire qualità, sicurezza, efficienza e sostenibilità in vari settori. Questi sono volontari ma spesso vengono adottati come requisiti per accedere ai mercati finanziari o ottenere certificazioni.

ISO 31000:2018 è uno standard elaborato dalla ISO in materia di Enterprise Risk Management e fornire linee guida per costruire ed integrare all'interno della struttura aziendale un sistema di gestione del rischio. La revisione del 2018 si basa sulla versione originale pubblicata nel 2009 ma si propone di: evidenziare il ruolo di leadership che è in capo al top management, integrare il sistema di gestione del rischio in tutti i livelli e le attività aziendali, enfatizzare la natura iterativa e di sviluppare un framework adattabile alle specifiche esigenze aziendali. Il documento è suddiviso in **tre parti**, ognuna delle quali rappresenta un componente del sistema ERM.

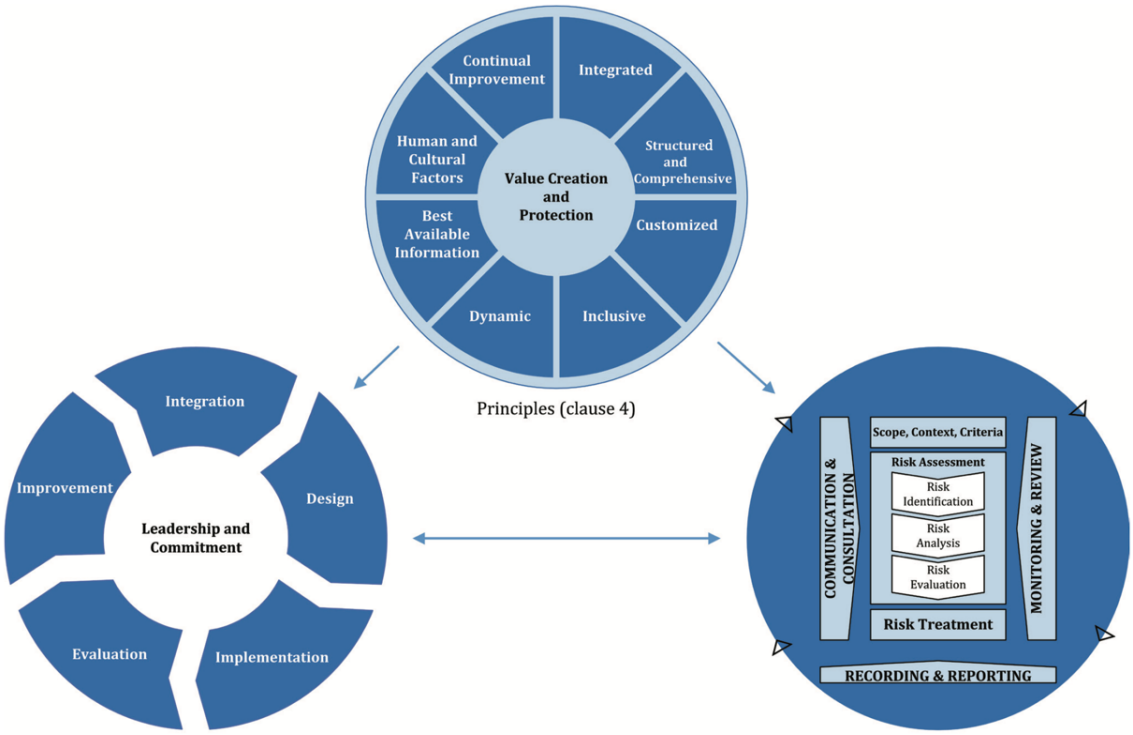

Figura 7: Componenti processo ERM. Fonte: ISO. (2018). ISO 31000:2018

Il **primo componente** presentato dallo standard sono i **principi**, questi rappresentano le fondamenta di tutto il sistema e devono essere tenuti in considerazione sia nella costruzione del sistema che nello svolgimento delle relative funzioni. Secondo la ISO un efficace sistema ERM deve essere:

- **Integrato**: deve essere parte integrante di tutte le attività aziendali.
- **Strutturato ed esauriente**: deve utilizzare un approccio strutturato ed olistico al fine di poter fornire concreto supporto al processo decisionale.
- **Personalizzato**: il *framework* ed il processo di *risk management* devono essere adattati alle specifiche necessità aziendali derivanti dal proprio contesto esterno ed interno.
- **Inclusivo**: il coinvolgimento degli *stakeholder* interessati, siano essi interni o esterni, è di fondamentale importanza per ottenere *insights* basati sulla loro conoscenza, le loro visioni e percezioni.
- **Dinamico**: essendo i rischi variabili di natura dinamica, il sistema di gestione degli stessi deve essere in grado di gestire questa dinamicità.

Deve inoltre prevedere e considerare:

- **Migliori informazioni disponibili**: la base informativa su cui i processi di gestione del rischio si basa sia su dati storici che su previsioni future. I primi devono essere validati, mentre le seconde devono essere il più possibile attendibili, in ogni caso le informazioni devono essere rese disponibili ai soggetti interessati in maniera chiara ed in tempi adatti.
- **Fattori umani e culturali**: deve tenere in considerazione la componente umana in quanto fattore capace di influenzare la gestione del rischio
- **Miglioramento continuo**: il sistema di gestione del rischio deve essere una fonte di apprendimento che conduce a un continuo processo di perfezionamento.

Il **secondo componente** è il **framework**, ossia la struttura fondamentale da seguire per strutturare un efficace sistema ERM che possa operare in modo integrato e permanente all'interno dell'organizzazione. La struttura del *framework* ha natura circolare e sottolinea la natura iterativa dell'ERM fondata sul principio del miglioramento continuo. Le sue componenti sono:

- **Leadership ed impegno**: il *top management* e gli organi di controllo sono corresponsabili di supervisionare la corretta integrazione del sistema ERM, devono inoltre mostrare il loro impegno nelle attività di gestione del rischio.
- **Integrazione**: il *risk management* non è un'attività eseguita da un'unica funzione ma è svolto in ogni parte dell'organizzazione ed ognuno ha la propria responsabilità. In quest'ottica il *risk management* deve essere parte integrate dei sistemi di governo, controllo, pianificazione, finanza e *operations*.
- **Design**: nella progettazione di un sistema ERM è di fondamentale importanza tenere presente il principio della personalizzazione, di conseguenza bisogna partire da un'analisi del contesto interno ed esterno dell'impresa. Si procede, quindi, con la definizione dei ruoli, autorità e responsabilità, in modo tale da individuare i soggetti che possiedono l'autorità di gestire il rischio (*Risk Owners*). Successivamente il *top management* provvede all'allocazione delle risorse necessarie, non solo in termini strettamente economici ma anche da un punto di vista di capitale umano, di processi, di procedure e informativo. Infine, è indispensabile strutturare approcci di consultazione e comunicazione tra i vari *stakeholder* interessati al fine di consentire alle informazioni di circolare correttamente.

- **Implementazione**: nell'implementazione del sistema l'organizzazione deve prestare attenzione allo sviluppo di piani coerenti con quanto sopra descritto, analizzare il processo di *decision-making* e adattarlo a quanto pianificato.
- **Valutazione**: al fine di valutare l'efficacia del sistema sviluppato l'organizzazione deve procedere a misurazioni periodiche delle *performance* prodotte mediante la predisposizione di *feedback*, *audit* interni e KPI.
- **Miglioramento**: l'organizzazione dopo aver monitorato il sistema deve apportare le modifiche necessarie per un suo perfezionamento e per adattarlo a cambiamenti del contesto sia esterno che interno.

Terzo componente dello *standard* è rappresentato dal **processo**, questo riguarda l'applicazione sistematica dei principi e del *framework* a livello strategico, operativo, di controllo e progettuale. Le varie fasi individuate sono:

- **Comunicazione e consultazione**: consiste nel coinvolgimento di *stakeholder* esterni ed interni per promuovere la comprensione del rischio e ottenere informazioni per sostenere il processo decisionale.
- **Scopo, contesto e criteri**: la definizione dello scopo, analisi del contesto e definizione dei criteri di valutazione del rischio sono attività necessarie al fine di consentire una corretta valutazione e gestione del rischio.
- **Risk assessment**: consiste nel processo di identificazione, analisi e valutazione dei rischi. È un'attività che necessita di essere effettuata in maniera sistematica e di coinvolgere i diversi *stakeholder* interessati.
- **Trattamento del rischio**: fase di elaborazione delle strategie per gestire il rischio (evitare, ridurre, condividere, accettare)
- **Monitoraggio e revisione**: fase di verifica della corretta applicazione delle strategie elaborate e individuazione delle migliorie da poter apportare.
- **Registrazione e reporting**: quanto prodotto dal sistema ERM, in termini di attività effettuate ed effetti sull'organizzazione, deve essere raccolto, elaborato e successivamente condiviso con i soggetti che possono trarne il massimo valore.

3.3 Altri Standard e Linee Guida per il Risk Management

3.3.1 Normative ISO

L’attività dell’ISO in materia di *standard* connessi al *risk management* non si ferma al *framework* presentato nel documento 31000:2018, ma è incentrata a sviluppare un’intera famiglia di normative volte a definire principi e linee guida. Tra le principali possiamo identificare:

- **ISO/IEC 31010:2019 - Risk management - Risk assessment techniques**: propone metodi di analisi e valutazione dei rischi adatti a diversi contesti.
- **ISO 31022:2020 - Risk management - Guidelines for the management of legal risk**: sviluppa linee guida per la gestione dei rischi legati a questioni di origine legale.
- **ISO/TS 31050:2023 - Risk management - Guidelines for managing an emerging risk to enhance resilience**: elaborazione di principi per affrontare e gestire i rischi emergenti per migliorare la resilienza dell’organizzazione.
- **ISO 31073:2022 - Risk management - Vocabulary**: definisce termini e concetti chiave per una comunicazione uniforme.

Tuttavia, come precedentemente indicato, la gestione dei rischi a livello aziendale è un’attività olistica che, quindi, per sua stessa natura ricomprende diverse aree organizzative. Per questo motivo possiamo trovare *standard* ISO riferibili a settori specifici che integrano al loro interno principi di valutazione e gestione del rischio.

- **ISO 9001:2015 - Quality management systems - Requirements**: include il *risk-based thinking*, richiedendo all'organizzazione di determinare i rischi e le opportunità da affrontare per garantire i risultati previsti del sistema di gestione della qualità.
- **ISO 14001:2015 - Environmental management systems - Requirements with guidance for use**: richiede l'identificazione degli aspetti ambientali e la valutazione dei rischi associati, considerando un approccio di ciclo di vita.
- **ISO 21502:2020 - Project, programme and portfolio management - Guidance on project management**: include la gestione del rischio di progetto, rilevante per pianificazione ed esecuzione, applicabile a gestione progetti.
- **ISO 22301:2019 - Security and resilience - Business continuity management systems - Requirements**: include la valutazione del rischio per identificare minacce alla continuità operativa, elemento essenziale per la pianificazione.

- **ISO 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements**: richiede un processo di valutazione del rischio per la sicurezza delle informazioni, integrandolo nel sistema di gestione.
- **ISO 28000:2022 - Security management systems for the supply chain**: include la valutazione del rischio per la sicurezza della catena di approvvigionamento, componente rilevante del sistema di logistica.
- **ISO 37301:2021 - Compliance management systems - Requirements with guidance for use**: include la valutazione del rischio per i rischi di conformità, supportando la gestione etica e legale.

3.3.2 Codice di Corporate Governance

Facendo riferimento alle criticità del sistema economico-finanziario mostrate dalle crisi dei primi anni del 2000, possiamo individuare come componente in grado di influenzare la fiducia nei mercati la corporate governance. Questo periodo è stato caratterizzato da crisi aziendali e dissesti finanziari che possono essere ricondotti a due tipologie di cause. "La prima fa riferimento ad episodi di frode e di corruzione che hanno visto soggetti perseguire in modo illecito benefici personali, in conflitto di interessi con le organizzazioni di riferimento (ad esempio, casi WorldCom 2003 ed Enron 2005)[30]". La seconda è da "ricondurre a quegli organi di governo e gestione che, inseguendo finalità inadeguate (o insostenibili), hanno prodotto danni così rilevanti alle economie delle imprese interessate, da portarle all'insolvenza (casi Arthur Andersen 2003 e Lehman Brothers 2007)".[31] A questi fallimenti i regolatori hanno risposto emanando nuovi regolamenti volti a rafforzare il controllo societario e rendendo il *risk management* una responsabilità della *corporate governance*[32].

In Italia documentazione di fondamentale importanza è il **Codice di Corporate Governance** (2020), che indica le *best practice* in materia di governo societario. Promosso da Borsa Italiana S.p.A., il codice, è rivolto a tutte le società quotate su

[30] Accardi, F. (2024). *Governo e Controllo dei Rischi, manuale per scelte consapevoli e sostenibili.* Franco Angeli.

[31] Di Carlo, E. (2017). *Interesse primario dell'azienda come principio guida e bene comune.* Giappichelli.

[32] Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. *Accounting, Organization and Society, 35*, 659-675.

Euronext Milan – ex Mercato Telematico Azionario[33] (MTA), l'adesione allo stesso è di natura volontaria e deve essere esplicitata nella relazione sul governo societario.

Il codice è organizzato in articoli ed ognuno di questi è suddiviso a sua volta "in principi, che definiscono gli obiettivi di una buona governance, e in raccomandazioni, che indicano i comportamenti che il Codice reputa adeguati a realizzare gli obiettivi indicati nei principi"[34].

- **Art. 1 –** Ruolo dell'organo di amministrazione
- **Art. 2** – Composizione degli organi sociali
- **Art. 3** – Funzionamento dell'organo di amministrazione e ruolo del presidente
- **Art. 4** – Nomina degli amministratori e autovalutazione dell'organo di amministrazione
- **Art. 5** – Remunerazione
- **Art. 6** – Sistema di controllo interno e di gestione dei rischi

Il codice stesso prescrive che debba essere adottato facendo prevalere la sostanza del contenuto rispetto all'aspetto della forma. Viene così introdotto il criterio del *comply or explain* (**applicazione discrezionale**) secondo il quale le aziende possono discostarsi da quanto prescritto dagli articoli qualificando e giustificando tali deviazioni. Viene, sempre dallo stesso codice, inoltre illustrato l'**obbligo di *disclosure*** (informativa), secondo il quale le informazioni vanno comunicate al mercato mediante la relazione del governo societario. Questa informativa non sostituisce quella prescritta dal dettato civilistico ma la integra, andando così a fornire agli *stakeholder* un'informativa più completa e trasparente su come l'organo di governo societario sia composto ed operi.

4. Enterprise Risk Management

L'Enterprise Risk Management (ERM) costituisce un **processo integrato** che coinvolge Consiglio di Amministrazione, management e strutture operative, finalizzato a identificare e gestire i rischi in coerenza con la strategia e gli obiettivi aziendali, così da garantire la creazione e la protezione del valore nel lungo periodo. A differenza degli approcci tradizionali, spesso caratterizzati da una visione settoriale e frammentata, l'ERM

[33] Euronext Milano. (s.d.). *Euronext Milan*. Tratto da Borsa Italiana: https://www.borsaitaliana.it/azioni/mercati/euronext-milan/home/caratteristiche.htm

[34] Comitato per la Corporate Governance. (2020). Codice di Corporate Governance.

supera la logica “a silos” attraverso un **coordinamento a livello di impresa** che permette di cogliere le interrelazioni tra rischi eterogenei e di valutarne congiuntamente l’impatto sulle performance.

L’ERM, pur incorporando i concetti tipici dei **controlli interni**, se ne distingue per l’orientamento più ampio: non si limita alla mitigazione dei rischi operativi e alla conformità normativa, ma integra elementi quali la **propensione al rischio, la tolleranza, la definizione degli obiettivi e il legame con la strategia**. In tal modo diventa uno strumento di governo aziendale, che consente di bilanciare rischi e opportunità e di rafforzare la resilienza organizzativa.

L’efficacia di questo processo dipende tuttavia non solo dai modelli adottati, ma anche dall’**ambiente organizzativo** in cui esso si inserisce: la **cultura del rischio**, che plasma i comportamenti individuali, e la **corporate governance**, che definisce ruoli e responsabilità formali, rappresentano due pilastri fondamentali.

È da questa base che il capitolo si sviluppa, analizzando dapprima i **profili culturali e di governance** (paragrafo 4.1), per poi evidenziare il legame con **strategia, obiettivi e performance** (paragrafo 4.2), approfondire gli **elementi fondamentali del processo ERM** (paragrafo 4.3) ed infine mostrare l’**integrazione con il sistema di controllo interno** (paragrafo 4.4).

4.1 Corporate Governance e Cultura Aziendale

L'efficacia di un sistema di Enterprise Risk Management non dipende unicamente dall’adozione di modelli metodologici strutturati, necessita anche di un **contesto organizzativo** che ne consenta l’attuazione in modo coerente e sistematico. In tal senso la cultura organizzativa e la *corporate governance* costituiscono due pilastri fondamentali per garantire l’efficacia e l’integrazione del sistema di Enterprise Risk Management all’interno dell’impresa.

La prima plasma i comportamenti, le percezioni e le modalità con cui gli individui si rapportano al concetto di rischio, influenzando in maniera diretta l’adozione di decisioni consapevoli e coerenti con i valori aziendali. La *corporate governance*, invece, definisce ruoli, responsabilità e processi decisionali connessi alla gestione del rischio, disegnando la struttura formale del sistema ed i meccanismi di supervisione e controllo.

Queste due dimensioni, pur operando su piani diversi – uno più informale e valoriale, mentre l'altro più strutturato e normativo – si influenzano reciprocamente e devono essere allineate affinché il processo ERM sia realmente integrato e funzionale al perseguimento della strategia, degli obiettivi strategici e alla creazione di valore sostenibile nel lungo termine.

4.1.1 Cultura

La **cultura organizzativa** è l'insieme di valori, abitudini e comportamenti condivisi che si sviluppano nel tempo all'interno di un'organizzazione. Nasce dall'esperienza comune nel risolvere problemi, si trasmette ai nuovi membri, guida il modo in cui le persone pensano e agiscono[35]. ***Mission*** **e** ***vision*** ne sono il principale mezzo comunicativo, tuttavia, questa influenza in maniera pervasiva anche altri aspetti, come: i valori aziendali fondamentali, le modalità di agire dei soggetti, il processo decisionale.

Questi aspetti sono in grado di influenzare in maniera diretta come i vari attori aziendali si rapportano rispetto al concetto di rischio e, siccome sono le persone ad operare il sistema di *risk management*, contribuiscono a definire anche l'orientamento dell'impresa nei confronti del rischio. L'Institute of Risk Management definisce la **cultura del rischio** come "i valori, le convinzioni, le conoscenze e la comprensione del rischio condivisi da un gruppo di persone con uno scopo comune, in particolare i dipendenti di un'organizzazione"[36]. In relazione a ciò, il COSO individua uno "**spettro culturale**", all'interno del quale la cultura aziendale può posizionarsi da un estremo di avversità al rischio, ad un altro di propensione. A seconda di dove l'impresa è posizionata in questo spettro la definizione di rischi ed opportunità potrà variare, e quello che per la prima organizzazione può costituire un evento negativo da evitare, per la seconda può rappresentare una potenziale occasione da provare a sfruttare.

È **responsabilità del** ***board*** **e del** ***management*** definire una cultura aziendale in linea alla strategia ed agli obiettivi strategici (3° Principio COSO). Questa è una scelta di primaria importanza, poiché la cultura organizzativa influenza profondamente il modo in cui l'impresa identifica, valuta e gestisce i rischi. Inoltre, poiché il sistema di Enterprise Risk

[35] Sackmann, S. A. (2022). *Culture in Organizations: Development, Impact and Culture-Mindful Leadership.* Springer International Publishing.
[36] IRM. (2012). *Risk Culture: Resources for practitioners.* London: Institute of Risk Management.

Management è concepito anche come strumento di supporto al processo di *decision-making*, questo contribuisce ad orientare le decisioni in modo coerente con i valori e gli obiettivi dell'impresa.

È inoltre **responsabilità del *management*** promuovere attivamente la cultura aziendale definita e dimostrare coerenza rispetto ad essa, come indicato dal 4° Principio del COSO Framework. A tal fine, è fondamentale che il management eserciti una *leadership* solida e adotti uno stile comunicativo coerente, in grado di favorire l'allineamento tra tutti gli attori coinvolti rispetto ai valori aziendali, alle priorità strategiche e ai comportamenti attesi da dipendenti e partner. Ciò deve essere supportato mediante lo sviluppo di un sistema comunicativo aperto e trasparente, che da un lato incoraggi il personale a partecipare attivamente alle discussioni inerenti ai rischi, e dall'altro garantisca una risposta tempestiva e adeguata a eventuali comportamenti non coerenti con i valori condivisi.

In definitiva, lo scopo di tutto ciò è quindi sviluppare una **cultura aziendale** consapevole del rischio (***risk-aware***), che integri considerazioni riguardanti il rischio a tutti i livelli decisionali ed alla quale siano allineati i comportamenti individuali. In questo contesto "il personale sa gli obiettivi dell'entità e quali sono i limiti entro i quali può operare. Può discutere e confrontarsi apertamente sui rischi da assumere per raggiungere la strategia e gli obiettivi aziendali, con il risultato che i comportamenti dei dipendenti e dei dirigenti sono più coerentemente allineati con la propensione al rischio dell'entità."[37] A supporto di ciò, nei tempi più recenti, è stata registrata una tendenza diffusa all'adozione di sistemi ERM, anche su base volontaria, principalmente ancorabili ad una cultura del rischio fortemente radicata all'interno dell'organizzazione e condivisa a tutti i livelli.[38]

4.1.2 Corporate Governance

La ***corporate governance*** può essere definita come "l'insieme delle regole, delle procedure, degli organi sociali e delle strutture organizzative volte a consentire attraverso un adeguato processo di identificazione, misurazione, gestione e monitoraggio dei principali rischi, una conduzione dell'impresa sana, corretta e coerente con gli obiettivi

[37] COSO. (2017). *Enterprise Risk Management: Integrating with Strategy and Performance.* COSO.
[38] Beasley, M. S., & Branson, B. C. (2024). *The State of Risk Oversight: An Overview of Enterprise Risk Management Practices.* Raleigh: NC State University, AICPA, CIMA.

prefissati"[39]. Rappresenta quindi il sistema di governo societario, le sue varie componenti e le modalità attraverso cui queste interagiscono tra loro. Per sua stessa natura è una caratteristica distintiva di ogni impresa e, la sua configurazione, è in grado di influenzare in modo significativo il comportamento dei vari attori aziendali e l'approccio alla gestione del rischio. Ogni soggetto coinvolto nella *governance* ricopre un ruolo specifico all'interno dell'ERM, ed è pertanto chiamato a partecipare attivamente affinché questo processo sia realmente integrato e possa, quindi, generare tutti i benefici connessi alla protezione ed alla creazione di valore.

Il **framework COSO** fornisce alcune linee guida – nello specifico all'interno dei principi uno e due – per supportare le imprese nella fase di sviluppo di una *corporate governance* che sia in grado di supportare il processo di gestione dei rischi, andando a definire ruoli e responsabilità specifici al processo ERM e indicando come gli attori o istituzioni preesistenti possano contribuirvi. Un ulteriore contributo alla definizione di linee guida è rinvenibile nel **Codice di Corporate Governance**[40] promosso da Borsa Italiana S.p.A. – precedentemente introdotto nel paragrafo 3.3.2 – che, mediante la definizione di principi e raccomandazioni, fornisce la struttura fondamentale sulla quale costruire un sistema di governo societario che sia funzionale al perseguimento del successo sostenibile dell'impresa, garantendo un equilibrio tra la gestione efficace dei rischi, la trasparenza dei processi decisionali e la tutela degli interessi di tutti gli *stakeholder*.

Mentre il Codice mantiene un'impostazione neutra rispetto al modello societario adottato, il *framework* elaborato dal COSO utilizza il **modello monistico (*one-tier*)**. Di conseguenza, per mantenere un'impostazione coerente e semplificare la spiegazione di ruoli, responsabilità e linee di comunicazione, l'elaborato adotterà come modello di *corporate governance* quello monistico, applicabile anche dalle società italiane ai sensi del D. lgs. 6/2003.

[39] De Nicola, A. (2018). *Il Diritto dei Controlli Societari.* Giappichelli.
[40] Da qui in avanti verrà indicato esclusivamente come "il Codice"

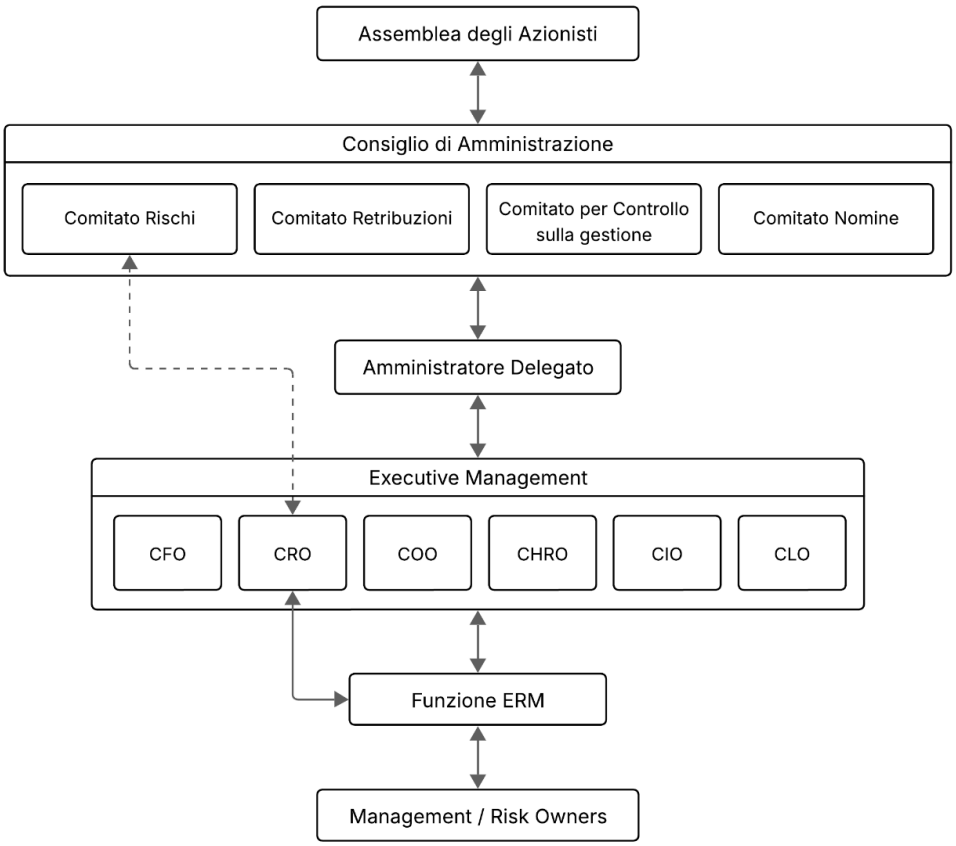

Figura 8. Struttura di Corporate Governance di una società che applica il modello Monistico o One-Tier

L'**assemblea degli azionisti** è l'organo collegiale composto dalle persone degli azionisti (*shareholder*), questi possono essere suddivisi in due principali categorie: **azionisti di controllo**, soggetti che possono direttamente o indirettamente influenzare in maniera significativa le decisioni del collegio, ed **azionisti di minoranza**. L'assemblea delibera sulla base delle disposizioni di legge (in Italia: CC e TUF) ed è chiamata a prendere le decisioni di primaria importanza per la società, ad esempio: approvare bilancio, nominare e revocare amministratori e modificare lo statuto societario.

All'**organo di amministrazione** (consiglio di amministrazione), i cui componenti sono nominati dall'assemblea degli azionisti, spetta il ruolo di guidare la società. Il Codice attribuisce a questo organo il compito di: definire le strategie della società prendendo anche in analisi i temi rilevanti per la generazione di valore nel lungo periodo, disegnare un sistema di governo societario in linea con l'attività dell'impresa e definire la natura ed il livello di rischio compatibile con gli obiettivi strategici. I componenti di quest'organo si distinguono in **amministratori esecutivi**, muniti di deleghe gestionali; **amministratori non esecutivi**, che non possedendo deleghe gestionali ricoprono esclusivamente un ruolo

di supervisione; ed in **amministratori indipendenti**, privi di incarichi operativi e scelti in modo da garantire autonomia di giudizio e imparzialità nelle decisioni del consiglio. Il COSO attribuisce al board, nella sua dimensione collegiale, la primaria responsabilità di supervisionare il rischio da un punto di vista strategico lasciando al management le attività di natura quotidiana. Nell'espletare le proprie funzioni il CdA si dota di **comitati costituiti al suo interno**. Mentre alcuni hanno natura obbligatoria (es. comitato per il controllo sulla gestione), altri possono essere liberamente formati. Tra questi rientra il Comitato Rischi, composto da soli amministratori non esecutivi, in maggioranza indipendenti e presieduto da un amministratore indipendente. A questo organo viene delegato il compito raccogliere informazioni su come i rischi possano impattare la strategia e supportare le valutazioni ed il processo decisionale dell'organo di governo.

L'**amministratore delegato** (*chief executive officer*), che può rivestire anche la carica di presidente del consiglio di amministrazione, ha il ruolo di raccordo tra il board ed i manager. Con riferimento al processo di gestione dei rischi, a questo spetta il compito di supervisionare l'implementazione del sistema di *risk management* e di sottoporre i rischi identificati all'organo di amministrazione.

I **manager esecutivi** (CFO, COO…) rivestono un ruolo apicale all'interno dell'organizzazione e sono posti a capo di dipartimenti aziendali. Hanno la principale funzione di collegare la visione strategica del *board*, del quale possono anche essere membri, con quella operativa del resto della struttura manageriale a loro sottoposta. Tra questi è ricompreso anche il **CRO** (*chief risk officer*), il quale si occupa di supervisionare il processo di *risk management* ed è responsabile di coordinare i risultati del flusso informativo riguardante i rischi. La relazione intercorrente tra i diversi manager esecutivi ed il CRO è di fondamentale importanza per il buon funzionamento del processo di *risk management*[41] e deve essere basata su interazione, collaborazione e reporting costanti. Il CRO, nell'esercizio delle proprie funzioni, può anche avere una linea di reporting diretta con il comitato rischi interno al board al fine di garantire una più rapida e completa

[41] Liebenberg, A. P., & Hoyt, R. E. (2003). The Determinants of Enterprise Risk Management: Evidence From the Appointment of Chief Risk Officers. *Risk Management and Insurance Review*, 37-52.

panoramica ed informativa sui rischi ai quali l'impresa è esposta da parte del consiglio di amministrazione[42].

La **funzione ERM**, al quale vertice è collocato il CRO, è responsabile della coordinazione e del corretto funzionamento del sistema di *risk management*. Si occupa di "supportare il management nel governo dei rischi (…), sovraintende tutto il processo"[43] elabora e consolida i risultati ottenuti. Ha una linea di *reporting* diretta con il CRO, tuttavia può interfacciarsi a monte con i vari *executive managers* e a valle con il management delle altre divisioni e funzioni aziendali, al fine di aumentare la circolazione dell'informativa riguardante i rischi e supportare i *decision-maker* posti ai diversi livelli aziendali.

Il processo di gestione dei rischi aziendali, tuttavia, non è un'attività di esclusiva responsabilità dell'alta amministrazione o della funzione ERM. Come lo stesso COSO sostiene, il sistema ERM funziona in maniera ottimale quando è integrato nell'intera organizzazione e diviene componente fondamentale del processo decisionale ad ogni livello. I *manager* collettivamente sono responsabili del rischio aziendale, tuttavia, "spesso viene individuato un ***risk-owner*** quale persona di riferimento con la responsabilità di garantire che i rischi specifici siano gestiti in modo appropriato"[44].

4.2 Strategia, Obiettivi e Performance

Il Framework COSO ERM posiziona chiaramente il **processo di gestione dei rischi al centro della catena del valore** tra la mission, 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 aziendali.

[42] Bailey, C. (2022). The Relationship Between Chief Risk Officer Expertise, ERM Quality, and Firm Performance. *Journal of Accounting, Auditing & Finance*, 205-228.
[43] Accardi, F. (2024). *Governo e Controllo dei Rischi, manuale per scelte consapevoli e sostenibili.* Franco Angeli.
[44] COSO, WBCSD. (2018). *Enterprise Risk Management: Applying enterprise risk management to environmental, social and governance-related risks.* COSO, WBCSD.

Figura 9. Processo ERM. Fonte: COSO. (2017). ERM Framework – Integrating with Strategy and Performance

***Mission, vision* e valori fondamentali** sono la dichiarazione dell'impresa mediante la quale essa definisce il proprio scopo, le proprie aspirazioni ed i principi etici che guidano il proprio operato. Come precedentemente indicato nel paragrafo sulla cultura aziendale, sono i mezzi mediante i quali l'impresa esplicita il proprio rapporto con il concetto di rischio ed una prima dichiarazione della propria propensione al rischio.

La **strategia aziendale**, espressa mediante la redazione di un documento di sintesi denominato piano industriale, costituisce l'insieme di scelte ed azioni che l'impresa prevede di prendere per conseguire i propri obiettivi di lungo periodo. Per supportare la maggior richiesta di trasparenza alle imprese da parte degli *stakeholder*, negli ultimi anni si è assistito ad una declinazione della stessa in una molteplicità di documenti pubblici tra cui: relazione sulla gestione, relazione sul governo societario, bilanci di sostenibilità e documenti di sintesi elaborati durante le presentazioni dedicate ad investitori ed analisti. La strategia aziendale rappresenta quindi "il posizionamento dell'impresa nell'ambiente, conseguente alle scelte e ai comportamenti del management"[45]. L'adozione di una strategia è una scelta di vitale importanza per l'impresa, questa infatti, implica la predisposizione di investimenti ed allocazione di risorse per permettere il raggiungimento dei risultati attesi. Inoltre, essendo questa espressione degli orientamenti interni all'azienda, per massimizzare le possibilità di successo è necessario che la strategia sia in linea con *mission*, *vision* e valori fondamentali aziendali.

Il COSO framework (2017) nasce proprio dalla comprensione della **necessità di integrare il processo di ERM con quello di pianificazione strategica**, e non essere più applicato a compartimenti stagni. Questa visione è sostenuta da Frigo, il quale sostiene

[45] Mazzola, P. (2013). *Il Piano Industriale: Progettare e Comunicare le Strategie di Impresa.* Egea.

che "per essere efficaci, la valutazione del rischio, la gestione del rischio e l'ERM dovrebbero essere integrate nei piani e nei budget strategici, nei piani di esecuzione e nelle misure di performance"[46]. Tuttavia "l'Enterprise Risk Management non crea la strategia dell'entità, ma influenza il suo sviluppo. (…) Fornisce al management le informazioni sui rischi di cui necessita per considerare le strategie alternative e, infine, per adottare la strategia scelta."[47]

In quest'ottica un processo ERM veramente integrato può supportare il management nella definizione del piano industriale guidando il management verso **l'analisi di tre criticità che possono affliggere la strategia**: la possibilità che questa non sia allineata con *mission*, *vision* e valori aziendali, le implicazioni che scaturiscono dalla strategia scelta ed i **rischi insiti** in essa. Per quanto riguarda la prima criticità – **mancato allineamento dei piani di lungo periodo con *mission*, *vision* e valori aziendali** – la stessa COSO, nel framework del 2017, introduce un componente del processo denominato *strategy and objective setting* che si focalizza sulla necessità di allineare queste componenti, sottolineando che una mancato allineamento possa minare la capacità di raggiungere quanto preventivato e incrementare il rischio per gli stakeholder. Un approccio ERM integrato consente di individuare *early warning signals* di disallineamento e supporta il management nella selezione di alternative strategiche coerenti con l'identità aziendale. In riferimento alla seconda criticità – **implicazioni della strategia scelta** – bisogna tener presente che ogni decisione strategica comporta dei *trade-off* e rischi specifici. Il processo ERM, in tal senso, fornisce un supporto analitico nel valutare tali implicazioni permettendo così al management di "considerare il tipo e l'ammontare di rischio che incontrerà nel perseguire quella specifica strategia"[48]

Definita la strategia, un'organizzazione sviluppa **obiettivi strategici** che, in linea con il principio 9 del framework COSO ERM 2017, rappresentano il collegamento logico tra il piano industriale e le performance. Questi permettono di individuare, misurare ed osservare come e se le azioni intraprese dall'azienda stanno dirigendo la stessa verso la direzione di lungo periodo definita. Un processo ERM integrato consente di tradurre tali obiettivi in indicatori di performance chiave (KPI), fornendo al management strumenti

[46] Frigo, M. L. (2008). When Strategy and ERM Meet. *Strategic Finance*, 45-49.
[47] COSO. (2017). *Enterprise Risk Management: Integrating with Strategy and Performance.* COSO.
[48] COSO. (2017). *Enterprise Risk Management: Integrating with Strategy and Performance.* COSO.

per valutare i risultati raggiunti rispetto alle aspettative e identificare tempestivamente eventuali scostamenti. Attraverso l'integrazione tra la gestione del rischio e la definizione degli obiettivi, l'ERM supporta il processo decisionale, permettendo di bilanciare rischi e opportunità e di ottimizzare le performance aziendali.

L'integrazione tra ERM, strategia ed obiettivi strategici supporta, quindi, il management dell'impresa mediante il miglioramento del processo decisionale, fornendo una visione più completa dello scenario in cui questa opera ed i vari *trade-off* ai quali si espone. Questo conduce, in definitiva, ad un **miglioramento delle performance** e ad una maggior capacità non solo di **proteggere il valore** ma anche di **generarlo** in maniera sostenibile nel lungo periodo. Questo importante beneficio al sistema azienda dato dal legame indissolubile di questi componenti è espresso in maniera chiara dal *King IV Report of Corporate Governance for South Africa* (2016) nel quale è espresso che "lo scopo dell'organizzazione [n.d.r.: *mission* e *vision*], i suoi rischi e opportunità, la strategia, il *business model*, le *performance* e lo sviluppo sostenibile sono tutti elementi inseparabili del processo di creazione del valore"[49]

4.3 Elementi Fondamentali del Processo ERM

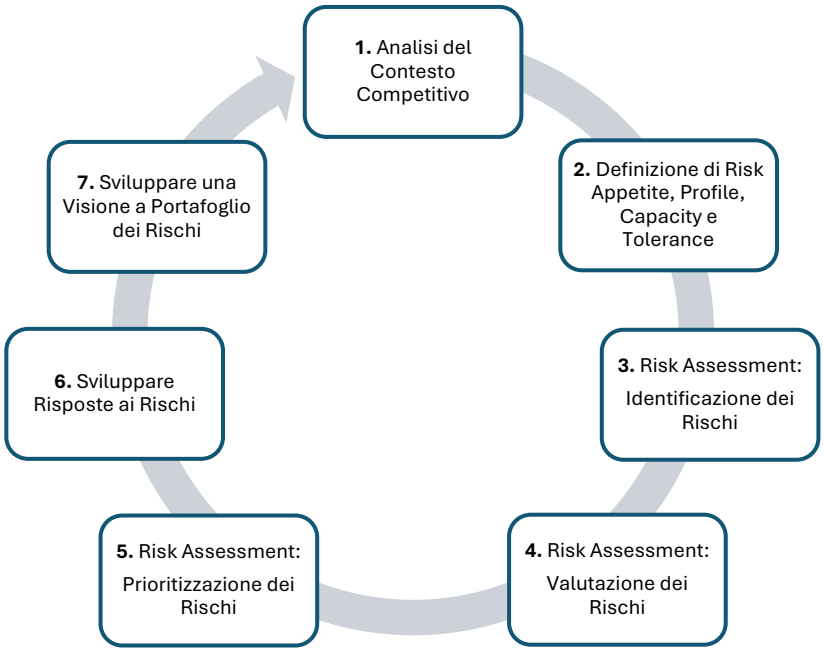

Figura 10. Elementi fondamentali del processo ERM

[49] The Institute of Directors in Southern Africa. (2016). *King IV Report of Corporate Governance for South Africa 2016.* The Institute of Directors in Southern Africa.

L'Enterprise Risk Management si configura come un processo strutturato, continuo e integrato, il cui scopo è supportare il raggiungimento degli obiettivi aziendali attraverso l'identificazione, la valutazione e la gestione dei rischi in modo sistemico e coerente con le decisioni strategiche definite dal management. Il presente capitolo si propone quindi di approfondire i **principali elementi che costituiscono il processo di ERM**, seguendo l'articolazione proposta dal framework COSO ERM 2017, e di illustrare le principali metodologie di analisi e decisionali applicabili in ciascuna fase individuate dalla normativa ISO 31010:2019.

La prima fase illustrata riguarda **l'analisi del contesto competitivo**, volta a comprendere l'ambiente interno ed esterno in cui opera l'organizzazione. A partire da questa base informativa vengono **definiti i principali parametri di rischio**: *risk appetite*, *risk profile*, *risk capacity* e *risk tolerance*, mediante i quali il management allinea l'approccio al rischio dell'impresa con la propensione della stessa derivante dalla strategia. Successivamente si affronta il sotto-processo di ***risk assessment***, il quale è articolato in tre fasi distinte: l'identificazione dei rischi, la loro valutazione in termini di impatto e probabilità e la successiva prioritizzazione. Questa fase aiuta l'organizzazione ad approfondire la propria conoscenza e consapevolezza riguardo i rischi che la interessano e fornisce informazioni necessarie alla definizione delle strategie di gestione e risposta ai rischi. Infine, l'adozione di una **visione a portafoglio dei rischi** consente di superare un approccio frammentato, integrando le diverse esposizioni in un'ottica strategica e trasversale.

4.3.1 Analisi del Contesto Competitivo

Punto di partenza per lo sviluppo di un efficace strategia di *risk management* è quella dell'**analisi del contesto competitivo**, definita dal COSO come lo studio dei "trend, delle relazioni e degli altri fattori che influenzano l'attuale e futura strategia dell'impresa ed i suoi obiettivi"[50]. Comprendere l'ambiente in cui un'organizzazione opera – sia interno che esterno – è essenziale per progettare un processo ERM in grado di identificare e valutare i rischi in maniera olistica e di porre in essere adeguate misure di gestione anche utilizzando un'ottica proattiva.

[50] COSO. (2017). *Enterprise Risk Management: Integrating with Strategy and Performance.* COSO.

L'**ambiente esterno** (*external environment*) "comprende tutti i fattori che esulano dai confini di un'impresa e che possono potenzialmente influenzare la redditività e la *performance* dell'impresa, delle sue parti costitutive e della sua strategia"[51]. Diverse metodologie sono state sviluppate sia in letteratura accademica che nella prassi aziendale per effettuare l'analisi del contesto competitivo esterno, tra queste le principali – citate anche dal COSO nelle sue documentazioni – sono: analisi SWOT, analisi delle cinque forze di Porter e l'analisi PASTEL. L'**analisi SWOT** (*Strengths, Weaknesses, Opportunities,* e *Threats*) costituisce un metodo semplice e veloce per mettere in relazione i punti di forza e debolezza di una strategia e di far emergere eventuali pericoli ed opportunità che l'impresa può trovarsi ad affrontare, restituendo una matrice 2x2 che mostra graficamente il posizionamento dei fattori individuati e la loro posizione relativa. Benché parte della letteratura accademica la consideri già da tempo uno strumento incompleto, meramente descrittivo e privo del necessario rigore analitico[52], la SWOT rimane comunque uno strumento estremamente utilizzato ed utile per analizzare sistematicamente il contesto competitivo, soprattutto se accompagnato da metodologie più rigorose ed analitiche[53]. Il Modello delle **cinque forze di Porter** è una metodologia di analisi del contesto competitivo esterno che consente di comprendere la struttura del settore di riferimento e le dinamiche che ne influenzano la redditività. Le cinque forze individuate da Porter sono: la minaccia di nuovi entranti, il potere contrattuale dei fornitori, il potere contrattuale dei clienti, la minaccia di prodotti sostitutivi e l'intensità della rivalità tra imprese esistenti[54]. A queste, lo stesso Porter, in una sua revisione del 2008 aggiunge una sesta dimensione: i beni complementari[55], ovvero quei prodotti o servizi che, pur appartenendo ad altri settori, influenzano in modo significativo la domanda e la competitività del settore analizzato. Ulteriore strumento di analisi del contesto competitivo esterno è l'**analisi PASTEL**, questa esplora i fattori ambientali di più ampia portata che possono influenzare le imprese indipendentemente dal settore in

[51] Auguer, M., & Teece, D. J. (2018). *The Palgrave Encyclopedia of Strategic Management.* Palgrave Macmillan.
[52] Hill, T., & Westbrook, R. (1997). SWOT analysis: It's time for a product recall. *Long Range Planning, 30*, 46-52.
[53] Auguer, M., & Teece, D. J. (2018). *The Palgrave Encyclopedia of Strategic Management.* Palgrave Macmillan.
[54] Porter, M. E. (1980). *Competitive strategy: Techniques for analyzing industries and competitors.* New York: Free Press.
[55] Porter, M. E. (2008). The five competitive forces that shape strategy. *Harvard Business Review, 86*, 78-95.

cui operano. Le sei dimensioni chiave sulle quali l'analisi si concentra sono: politica, legata alla stabilità istituzionale e alle normative; ambiente, riguardante la sostenibilità ecologica e vincoli normativi in materia; società, che include tendenze demografiche, culturali e valoriali; tecnologia, in relazione al progresso tecnologico; economia, considera il quadro macroeconomico generale; e legge, con attenzione al sistema normativo e regolamentare. L'analisi del contesto competitivo esterno è un passaggio fondamentale per un corretto processo ERM; infatti, permette di studiare e comprendere in maniera approfondita l'ambiente nel quale l'impresa si trova ad operare e mette il management in "una miglior posizione per anticipare ed affrontare il cambiamento"[56].

L'**ambiente interno** (*internal environment*) ricomprende "tutto ciò che all'interno dell'entità può influire sulla sua capacità di raggiungere la strategia e gli obiettivi aziendali"[57]. L'analisi dell'ambiente interno è quindi orientata ad approfondire la comprensione dell'impresa sui suoi punti di forza e debolezza, su come questi possono incidere sulla performance aziendale e sull'approccio dell'azienda nei confronti del rischio. Diversi sono i **fattori oggetto di studio**, tra questi possiamo riscontrare come primo elemento l'organizzazione interna e il sistema di governance, i quali ricoprono un ruolo cruciale nel determinare l'efficienza del processo decisionale e di quello di controllo di gestione. Un secondo aspetto è rappresentato dalla solidità finanziaria e l'adeguatezza patrimoniale, elementi che riflettono la capacità dell'impresa di sostenere economicamente le proprie strategie e di resistere a eventuali *shock*. Ulteriore fattore è il capitale umano, valutato non solo in termini di competenze dei dipendenti, ma anche come espressione della cultura aziendale e dei valori condivisi. Ulteriori fattori determinanti sono anche la tecnologia adottata, le infrastrutture aziendali ed i processi interni, tutti elementi in grado di influenzare direttamente la performance operativa e la competitività dell'organizzazione. Infine, ulteriore elemento è costituito dalla reputazione dell'impresa, la quale è strettamente legata al valore del marchio e alla fiducia instaurata con gli stakeholder.

Ulteriore elemento da prendere in considerazione per effettuare un'esaustiva analisi del contesto competitivo riguarda **l'identificazione degli *stakeholder***; questi sono definiti come "ogni gruppo o individuo che può influenzare o è influenzato dal raggiungimento

[56] COSO. (2017). *Enterprise Risk Management: Integrating with Strategy and Performance.* COSO.
[57] COSO. (2017). *Enterprise Risk Management: Integrating with Strategy and Performance.* COSO.

degli obiettivi dell'organizzazione"[58]. **Freeman** propone una prima ma importante distinzione degli *stakeholder* in due gruppi: ***stakeholder* interni**, soggetti compresi all'interno dell'impresa in grado di influenzarla in maniera diretta; e ***stakeholder* esterni**, entità non facenti parte dell'azienda in senso stretto ma in grado di condizionare ed essere condizionati da essa. Un secondo metodo di classificazione degli *stakeholder* è quello proposto da **Max B.E. Clarkson**[59], il quale propone una distinzione in due categorie: ***stakeholder* primari**, essenziali per la sopravvivenza dell'impresa, il ritiro di anche solo uno di questi può comportare l'interruzione della regolare operatività aziendale; e ***stakeholder* secondari**, i quali hanno un potere di influenza, ma non sono vitali per la sopravvivenza dell'impresa e non sono in relazione transazionale diretta con essa. Ulteriore metodo di classificazione, tra i più influenti, è quello proposto da **Mitchell, Agle e Wood** (1997)[60], i quali propongono una distinzione basata su tre attributi: **potere**, "una relazione tra attori sociali nella quale un attore sociale, A, può indurre un altro attore sociale, B, a fare qualcosa che B non avrebbe altrimenti fatto"[61]; **legittimità**, "percezione o ipotesi generalizzata che le azioni di un'entità sono desiderabili, corrette o appropriate rispetto ad un sistema socialmente costruito di norme, valori, credenze, definizioni"[62]; e **urgenza**, "il grado in cui le rivendicazioni degli *stakeholder* richiedono attenzione immediata"[63]. Basandosi su questi attributi, gli ***stakeholder*** vengono classificati in tre diverse macrocategorie: **latenti**, presentano un solo attributo e sono poco rilevanti per l'impresa; **aspettativi**, con due attributi e di media rilevanza per l'azienda; **definitivi**, caratterizzati dalla contemporanea presenza dei tre attributi ed un elevata rilevanza per l'impresa.

[58] Freeman, E. R. (1984). *Strategic Management: A Stakeholder Approach.* Boston: Pitman.
[59] Clarckson, M. B. (1995). A Stakeholder Framework for Analyzing and Evaluating Corporate Social Performance. *Academy of Management Review, 20*, 92–117.
[60] Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts. *Academy of Management Review, 22*(4), 853-886.
[61] Pfeffer, J. (1981). *Power in Organizations.* Pitman Publishing.
[62] Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review, 20*(3), 571–610.
[63] Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts. *Academy of Management Review, 22*(4), 853-886.

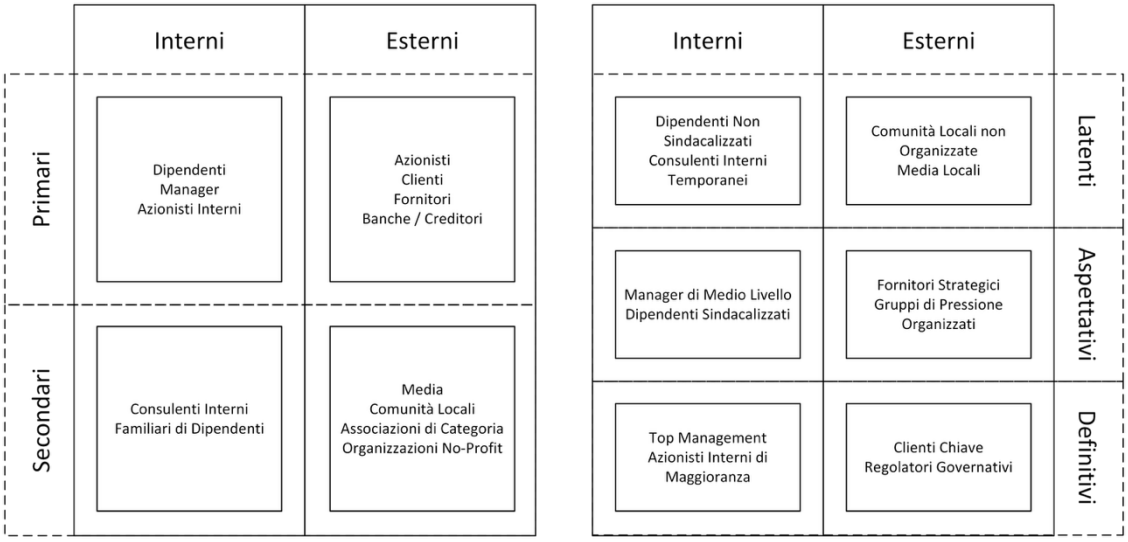

Figura 11. Matrici di Classificazione Stakeholders

4.3.2 Risk Profile, Risk Appetite, Risk Capacity, Risk Tolerance

A valle dell'analisi del contesto competitivo risulta essenziale, al fine di sviluppare un sistema ERM veramente integrato, approfondire la consapevolezza che l'azienda ha circa il proprio posizionamento rispetto al rischio e la capacità di gestirlo in modo coerente con gli obiettivi strategici. In questo contesto comprendere i principi che guidano la propensione al rischio, la capacità di assunzione dello stesso, i limiti tollerabili e il profilo di esposizione attuale rappresentano un passaggio cruciale per garantire coerenza tra strategia, obiettivi e *performance*.

Come introdotto in precedenza, un processo ERM integrato supporta il management nella fase di sviluppo e scelta della strategia aziendale fornendo informazioni sui rischi. Lo strumento che consente di illustrare in maniera chiara la relazione che intercorre tra rischio e *performance* associate ad una data strategia è il ***risk profile***. Questo è definito dallo stesso COSO come un modello in grado di "fornire una visione composta del livello di rischio ad un particolare livello dell'entità (es. livello complessivo, livello di business unit, livello funzionale) o aspetto del modello di business (es. prodotto, servizio, geografia)"[64]. La costruzione di un profilo di rischio implica l'analisi della relazione tra il livello atteso di performance – di una strategia o di un obiettivo aziendale – e l'esposizione al rischio ad essa associata, analisi che può essere condotta a seconda del caso sia mediante metodologie quantitative che qualitative. Il legame risultante viene

[64] COSO. (2017). *Enterprise Risk Management: Integrating with Strategy and Performance.* COSO.

generalmente rappresentato attraverso una linea (curva o profilo di rischio) su un grafico in cui la *performance* è posizionata sull'asse delle ascisse (x), mentre il livello di rischio sull'asse delle ordinate (y). Non esiste un'unica forma di *risk profile*, questa infatti è influenzata da una serie di fattori tra cui: assunzioni del management, confidenza e qualità delle analisi svolte, contesto competitivo, obiettivi e dalla strategia stessa. Tuttavia, in ambito accademico è comune usare una curva di tipo esponenziale al fine di sottolineare una relazione più che crescente tra rischio e livello di *performance* associato.

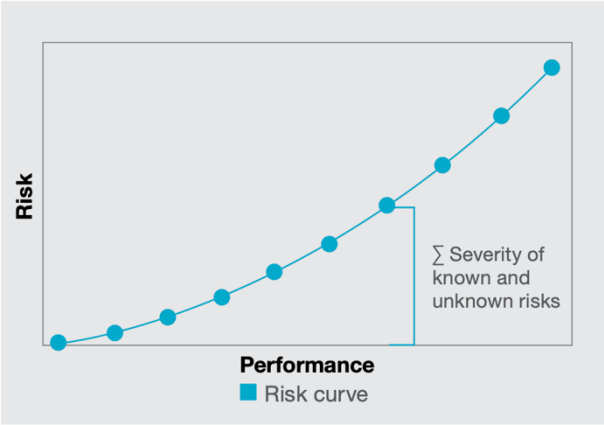

Figura 12. Risk Profile. Fonte: COSO. (2017). Enterprise Risk Management: Integrating with Strategy and Performance - Appendices

Ulteriore fattore di vitale importanza per il corretto funzionamento del sistema ERM è la definizione del ***risk appetite***, il quale rappresenta "i tipi e la quantità di rischio, a livello di *board*, che un'organizzazione è disposta ad accettare per perseguire il valore"[65]. Definire questa metrica è un fattore critico per sostenere un'organizzazione di successo, in quanto: fornisce al *management* importanti *insight* che permettono supportare il processo di definizione della strategia ed orienta le varie analisi effettuate durante il processo di ERM. Inoltre, costituisce anche un utile strumento comunicativo sia interno all'organizzazione – favorendo l'allineamento dei comportamenti dei vari attori aziendali – sia all'esterno della stessa nei confronti dei diversi *stakeholder*. Quest'importante funzione che il *risk appetite* riveste all'interno del processo ERM è dovuta al processo mediante il quale viene definita. Questo, infatti, prende avvio dai valori fondanti dell'organizzazione – *mission*, *vision* e *core values* – che rappresentano la base per la formulazione della strategia aziendale, in funzione della quale il management stabilisce il risk appetite a livello di entità (*entity-level appetite*). Questo viene successivamente declinato rispetto ai singoli obiettivi aziendali, identificando un *risk appetite* specifico per ciascuno di essi, assicurando così coerenza tra strategia, *performance* e gestione del rischio.

[65] Martens, F., & Rittenberg, L. (2020). *Risk Appetite Critical to Success: Using Risk Appetite to Thrive in a Changing World.* COSO.

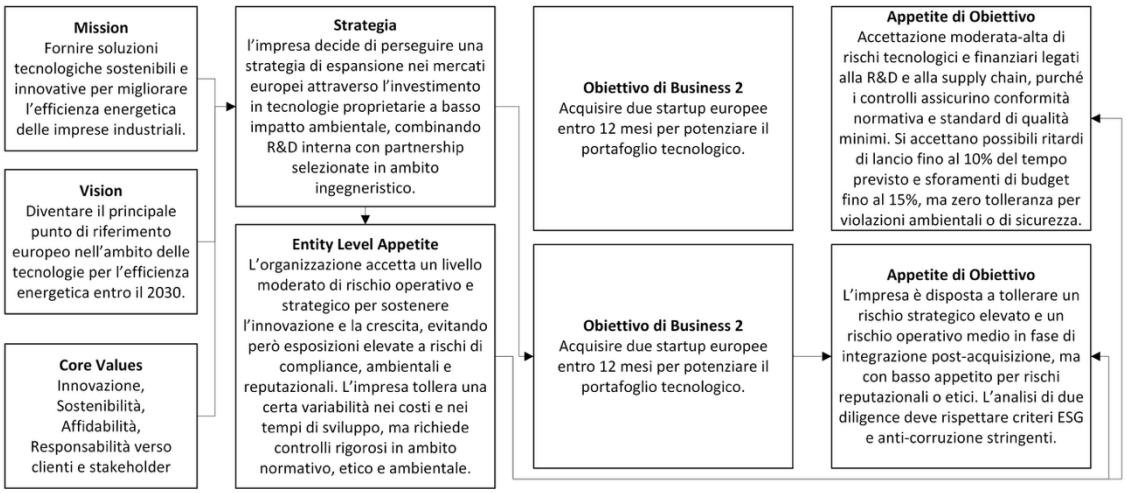

Figura 13. Esempio di processo di definizione del risk appetite

Con il termine ***risk tolerance*** (tolleranza al rischio) si fa riferimento "ai limiti di variazione accettabile delle prestazioni rispetto agli obiettivi."[66]. Questa definizione individua la tolleranza non attraverso il concetto di rischio, bensì attraverso le *performance*, permettendone così l'allineamento diretto con gli obiettivi quantitativi, sia a livello strategico che a quello operativo. Al contrario del *risk appetite*, la *risk tollerance* è una misura che va definita precisamente ed in maniera specifica all'obiettivo a cui si riferisce ed a seconda della relativa importanza. Infatti, minore sarà il livello di tolleranza definito dall'organizzazione – e di conseguenza più è importante raggiungere la *performance target* di quel dato obiettivo – maggiori saranno le risorse che il management dovrà allocare per ridurre il rischio che la *performance* si discosti dal *range* prestabilito.

La ***risk capacity*** (capacità di rischio) rappresenta, invece, la massima quantità di rischio che un'impresa può sopportare, nel perseguimento della propria strategia, tenendo contro della propria struttura, delle disponibilità di capitale, e del contesto in cui opera. "Non è solito per un'organizzazione fissare la propensione al rischio al di sopra della propria capacità di rischio, ma in rare situazioni può scegliere di farlo. Questo potrebbe accadere, ad esempio, nel caso di un'organizzazione che accetti il pericolo di insolvenza, comprendendo che il successo può creare un valore considerevole."[67] Prendere questa decisione da parte del *management* è estremamente pericoloso in quanto, se l'evento negativo associato si manifestasse, potrebbe risultare distruttivo per l'organizzazione.

[66] Martens, F., & Rittenberg, L. (2020). *Risk Appetite Critical to Success: Using Risk Appetite to Thrive in a Changing World.* COSO.
[67] COSO. (2017). *Enterprise Risk Management: Integrating with Strategy and Performance.* COSO.

Questi elementi possono essere messi tra loro in relazione, permettendo così la **costruzione di un grafico** in grado di visualizzare chiaramente il legame tra il livello di rischio e la performance attesa, evidenziando al contempo la soglia di risk appetite, la capacità massima di rischio (*risk capacity*), il livello target di performance e l'intervallo di tolleranza associato. Questa visualizzazione aiuta a valutare *trade-off* tra ambizione strategica e accettabilità del rischio, supportando decisioni informate sull'allocazione delle risorse e sulla definizione di soglie operative coerenti con gli obiettivi di lungo termine.

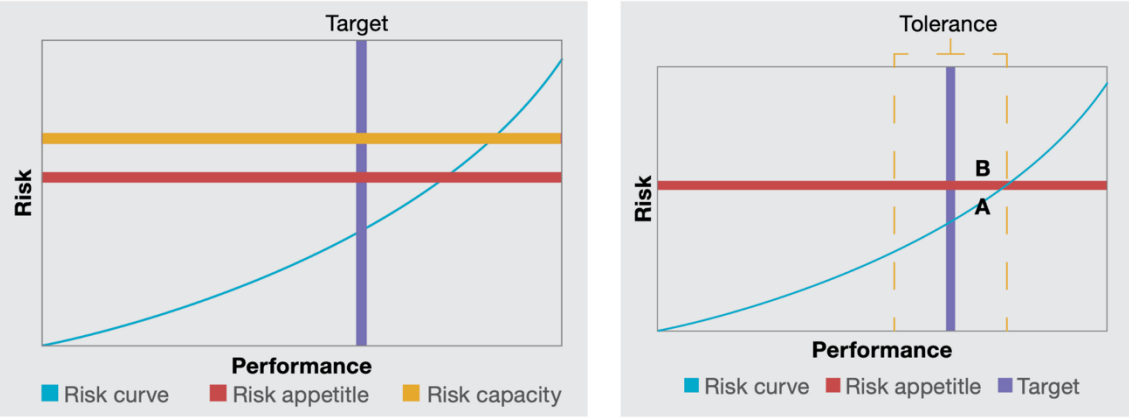

Figura 14. Grafico di risk profile, risk appetite, risk capacity e risk tolerance. Fonte: COSO. (2017). Enterprise Risk Management: Integrating with Strategy and Performance – Appendices. COSO.

4.3.3 Risk Assessment - Identification

Passaggio fondamentale di ogni processo ERM è la fase di identificazione dei rischi, la quale costituisce anche il punto di partenza per l'attività di ***risk assessment***, ossia quel procedimento volto all'individuazione, analisi e valutazione sistematica dei rischi. Durante la **fase di *risk identification***, quindi, l'impresa si concentra nell'individuazione di quegli eventi che potrebbero influenzare negativamente, oppure positivamente, la capacità di perseguire la propria strategia e di raggiungere gli obiettivi fissati.

Partendo dalla consapevolezza che il *management* ha sviluppato riguardo la cultura aziendale, la propria struttura di governance, il proprio *risk appetite* e l'ambiente competitivo in cui opera, l'attività di identificazione dei rischi richiede un'ulteriore analisi, ampia e sistematica, di una molteplicità di fattori. In primo luogo, è necessario comprendere quali circostanze o condizioni, siano esse tangibili (come una variazione normativa) o intangibili (quali un cambiamento reputazionale), possano generare conseguenze significative in futuro. In secondo luogo, sono oggetto di analisi sia le fonti

di rischio già note che quelle che potrebbero emergere nel tempo, con lo scopo di mappare in modo esaustivo le esposizioni potenziali. Ulteriore elemento analizzato è il sistema dei controlli esistenti, valutando non solo la loro presenza, ma anche la loro effettiva efficacia nel mitigare i rischi identificati. Infine, ulteriore ed imprescindibile oggetto di analisi è costituito dalle cause ed i *driver* degli eventi di rischio.

Il risultato di questa fase consiste nella redazione di un documento, denominato ***risk inventory* o *risk universe***, consistente in una raccolta sistematica di tutti i rischi individuati, i quali vengono classificati secondo criteri predefiniti (come categoria, fonte, livello organizzativo, impatto potenziale, probabilità di accadimento, controlli esistenti, ecc.) e collegati agli obiettivi strategici e operativi. Questo strumento fornisce una visione integrata e dinamica del profilo di rischio dell'organizzazione e rappresenta un supporto di fondamentale importanza per il resto del processo di *risk assessment*.

Rischio	Categoria	Descrizione	Fonte	Prob (1-5)	Imp (1-5)	Liv	Controlli esistenti	Owner	Obiettivi Impattati
Interruzione IT	Operativo	Possibile blackout dei sistemi aziendali critici	Interna	4	5	20	Parziali	CIO	Continuità operativa, affidabilità dei servizi IT
Perdita di talenti chiave	Strategico	Turnover di risorse strategiche difficili da sostituire	Interna	3	4	12	Limitati	HR Manager	Capacità innovativa, continuità gestionale
Variazione normativa	Normativo	Cambiamenti legislativi che impattano i requisiti di conformità	Esterna	2	3	6	Avanzati	Legal Dept	Compliance normativa, reputazione aziendale
Violazione dati sensibili	Reputazio-nale	Data breach o accessi non autorizzati a dati personali	Interna	5	5	25	Assenti	DPO	Tutela della privacy, fiducia degli stakeholder
Ritardi nella supply chain	Operativo	Interruzioni nelle forniture di materie prime essenziali	Esterna	3	4	12	Parziali	Supply Chain Mgr	Efficienza produttiva, soddisfazione del cliente

Tabella 1. Esempio di Risk Inventory

Nell'esecuzione di questa fase è quindi necessario sviluppare ed applicare diverse tecniche di raccolta delle informazioni e di analisi dei dati, al fine di restituire una fotografia dell'esposizione al rischio dell'impresa il più completa e vicina alla realtà. L'ISO, nel suo standard 31010:2019, propone una serie di **metodologie** per effettuare questa analisi, le quali sono principalmente volte a raccogliere informazioni dagli stakeholders, identificare i rischi e individuare fonti, cause e *driver* di rischio.

Una prima metodologia frequentemente adottata per coinvolgere gli *stakeholder* nella fase di identificazione dei rischi è il ***brainstorming***, una tecnica qualitativa volta a

generare idee e pareri su temi specifici. Benché questa sia una metodologia che trova applicazioni in numerose aree, è in grado di fornire numerosi spunti di riflessione anche in ambito ERM. Il brainstorming è condotto mediante una discussione strutturata, e spesso guidata da un esperto nel ruolo di facilitatore, dove un gruppo selezionato di partecipanti – scelti in base alla loro funzione, competenza o esposizione al rischio – viene stimolato a proporre eventi potenzialmente rilevanti per il raggiungimento degli obiettivi aziendali. Sebbene questa metodologia sia efficace nel generare una prima mappatura dei rischi, essa richiede di essere affiancata da tecniche più strutturate al fine di generare informazioni utili a supportare il processo di gestione dei rischi aziendali.

Una secondo metodo per il coinvolgimento degli *stakeholders* nel processo di *risk identification*, e che può anche essere impiegato come prima analisi dei risultati emersi da precedenti sessioni di *brainstorming*, è costituito dal **Metodo Delphi**, una procedura usata per affrontare problemi complessi dove è necessario il parere incondizionato di un gruppo di esperti. Il metodo consiste nel sottoporre a un gruppo di esperti uno o più questionari strutturati relativi a una tematica specifica (nel nostro caso, i rischi potenziali per l'organizzazione), i quali risultati saranno analizzati in forma aggregata, e sulla base di essi verrà predisposta una nuova iterazione. Il processo così composto si ripete più volte fino al raggiungimento di un consenso condiviso. Risulta di fondamentale importanza che i singoli soggetti partecipanti possano esprimersi in maniera anonima, ma che al contempo abbiano comunque accesso alle sintesi dei contributi espressi nei round precedenti. Benché lo scopo di questa analisi sia il raggiungimento di un consenso comune, il modello permette di individuare esperti con opinioni divergenti i cui punti di vista possono essere successivamente approfonditi attraverso interviste individuali, arricchendo così l'analisi dei rischi in modo più articolato.

Tra le metodologie di identificazione dei rischi a orientamento più quantitativo, l'ISO 31010:2019 suggerisce l'utilizzo del **modello FMEA** (*failure modes and effects analysis*). Nata in ambito industriale, per identificare punti di criticità nel funzionamento di macchinari, ha progressivamente trovato ampia applicazione anche nell'identificazione di rischi aziendali, soprattutto riguardanti processi e procedure operative. Il procedimento viene portato avanti da un *team* di esperti – provenienti da diverse funzioni aziendali – guidati da un facilitatore, i quali come primo passo si occupano di suddividere il processo oggetto di analisi in singole attività o elementi. Ognuno di questi viene quindi studiato

approfonditamente al fine di evidenziare: le modalità in cui può fallire (*failure mode*), le cause che possono generare queste criticità, le conseguenze che queste comportano sugli obiettivi aziendali ed i controlli esistenti. Ogni *failure mode* viene successivamente analizzata mediante l'uso di tre parametri: gravità dell'impatto, probabilità dell'accadimento e capacità di rilevamento preventivo. La combinazione di questi tre fattori consente di calcolare un **indice** sintetico noto come **RPN** (*risk priority number*), utilizzato per classificare in maniera quantitativa l'importanza del rischio e supportare le future fasi di *risk assessment*. In ottica ERM, la FMEA si configura quindi come una tecnica particolarmente utile per la costruzione del *risk inventory* legato ai processi operativi, fornendo un supporto quantitativo e strutturato per le successive fasi di analisi, valutazione e trattamento del rischio.

Un ultimo aspetto da prendere in considerazione in sede di identificazione dei rischi riguarda l'**individuazione di fonti, cause e *driver* dei rischi**, elementi fondamentali per comprendere le dinamiche alla base degli eventi potenzialmente avversi. In relazione a questo aspetto, l'ISO 31010:2019 suggerisce due **modelli di analisi** con approcci differenti ma complementari: il **Diagramma di Ishikawa** (*fishbone method*) e il *cindynic approach*. Il primo modello si basa su un'analisi sistematica, effettuata mediante un panel di esperti, delle cause da cui scaturiscono eventi positivi o negativi. Il risultato di questo processo viene poi rappresentato mediante un diagramma a lisca di pesce sul quale vengono mostrate le cause primarie e secondarie dell'evento attenzionato. Il ***cindynic approach***, invece, si concentra su una dimensione più profonda e qualitativa dell'analisi del rischio, basandosi su interviste semi-strutturate volte a esplorare i fattori sistemici, percettivi e culturali che possono contribuire alla manifestazione di situazioni critiche nonostante la presenza di controlli formali. L'obiettivo è quello di comprendere le motivazioni per cui alcune vulnerabilità restano latenti o non vengono percepite, evidenziando così l'importanza della cultura organizzativa, della comunicazione e della governance nella gestione del rischio.

4.3.4 Risk Assessment - Valuation

Identificati i rischi che possono influenzare la capacità dell'impresa di perseguire la propria strategia, il processo di *risk assessment* prosegue con una fase di analisi volta ad

approfondire la conoscenza da parte del *management* riguardo gli impatti, la probabilità e livello dei rischi.

Concetto di fondamentale importanza, che rappresenta l'obiettivo della **fase di *risk valuation***, e che costituisce anche un importante supporto al successivo processo di prioritizzazione, è quello di livello di rischio definito dalla ISO come "**magnitudo di un rischio** [n.d.r. *magnitude of a risk*] o di una combinazione di rischi, espressa in termini di combinazione di conseguenze [n.d.r. *impact*] e di probabilità delle stesse"[68]. I due fattori identificati da tale definizione – impatto e probabilità – costituiscono quindi il *focus* analitico di questa fase, e devono essere valutati adottando un orizzonte temporale coerente con quello impiegato nella formulazione della strategia e nella definizione degli obiettivi aziendali. Tuttavia, è fondamentale che il management mantenga consapevolezza anche dei rischi che si proiettano su un arco temporale di più lungo termine, al fine di non trascurare minacce od opportunità legate a trasformazioni strutturali del sistema economico e competitivo, la cui manifestazione, per loro stessa natura, avviene nel lungo periodo.

Per effettuare un'analisi strutturata dei due principali parametri di rischio – impatto e probabilità – e poter ottenere misurazioni coerenti del livello dei rischi identificati e raccolti nel *risk inventory*, l'ISO, nel documento 31010:2019, propone diverse **metodologie e modelli**. Tra questi: la *business impact analysis* (BIA) consente di stimare gli impatti organizzati, operati ed economici derivanti da eventi critici, individuando i processi più vulnerabili e i limiti temporali entro cui è necessario ripristinarli; la *cause-consequence analysis* (CCA) amplia l'analisi integrando sia le cause che gli effetti di un evento critico; infine, il modello bayesiano, consente di stimare la probabilità condizionata del verificarsi di uno scenario di rischio e di aggiornarla dinamicamente in seguito all'ottenimento di nuove informazioni o di cambiamenti del contesto competitivo.

La ***business impact analysis*** (BIA) è una tecnica di analisi qualitativa finalizzata ad individuare i processi essenziali per il raggiungimento degli obiettivi aziendali, gli effetti di eventi critici su di essi e le risorse necessarie – in termini di personale, immobilizzazioni e sistemi IT – per prevenire, o permettere il recupero da, eventi *disruptive*. All'interno di un *framework* ERM, la BIA rappresenta uno strumento

[68] ISO. (2022). *ISO 31073:2022 Risk management - Vocabulary.* ISO.

fondamentale per collegare le informazioni riguardanti i processi aziendali, il profilo di rischio dell'organizzazione e il raggiungimento delle performance preventivate. Questa metodologia prende in ingresso informazioni riguardanti strategia, ambiente competitivo e processi interni mediante l'utilizzo di questionari, interviste e *workshops* che coinvolgono *stakeholder* provenienti da diverse aree aziendali; mentre, attraverso la stima di indicatori come il *recovery time objective* (RTO) e il *maximum tolerable period of disruption* (MTPD), supporta la definizione delle priorità di risposta e la costruzione di strategie di continuità operativa. La BIA, pur non fornendo misure di probabilità riguardo l'accadimento degli eventi critici, contribuisce in modo determinante alla determinazione del livello di rischio e fornisce informazioni che possono essere utilizzate per strutturare la CCA.

La ***cause–consequence analysis*** (CCA) è una tecnica di analisi derivante dall'integrazione di due metodi classici: il *fault tree analysis* e l'*event tree analysis*. Il modello viene costruito da un *team* composto da attori interni all'organizzazione, esperti nelle diverse aree coinvolte, supportato da un facilitatore, ed è alimentato da informazioni ottenute mediante le analisi precedentemente eseguite (es. BIA, analisi del contesto competitivo, FMEA ecc.). La CCA permette di rappresentare graficamente, mediante la predisposizione di un diagramma ad albero verticale, sia le cause che le conseguenze associate ad un evento centrale (*initiating event*) prendendo in considerazione gli effetti che scaturiscono dagli attuali sistemi di controllo. Il diagramma si sviluppa a partire dall'*initiating event* (solitamente posto in posizione centrale) ed a questo sono collegati a monte gli scenari conseguenti e verso il basso le situazioni causali. Tra i diversi nodi sono inserite delle condizioni di controllo, tipicamente binarie (si/no), influenzate da fattori derivanti da *fault tree analysis* complementari. Questa rappresentazione consente, quindi, di visualizzare l'intera catena causale che collega un evento critico ai suoi potenziali impatti ed alle sue cause, permettendo la comprensione di ipotetici punti di vulnerabilità e gli effetti delle possibili misure di mitigazione dei rischi. All'interno del processo di *risk assessment*, questa metodologia si rivela particolarmente utile per analizzare in profondità gli eventi ad alto impatto potenziale, approfondire la comprensione delle interdipendenze tra elementi tecnici, organizzativi e decisionali ed infine fornire un solido supporto alla valutazione del livello di rischio.

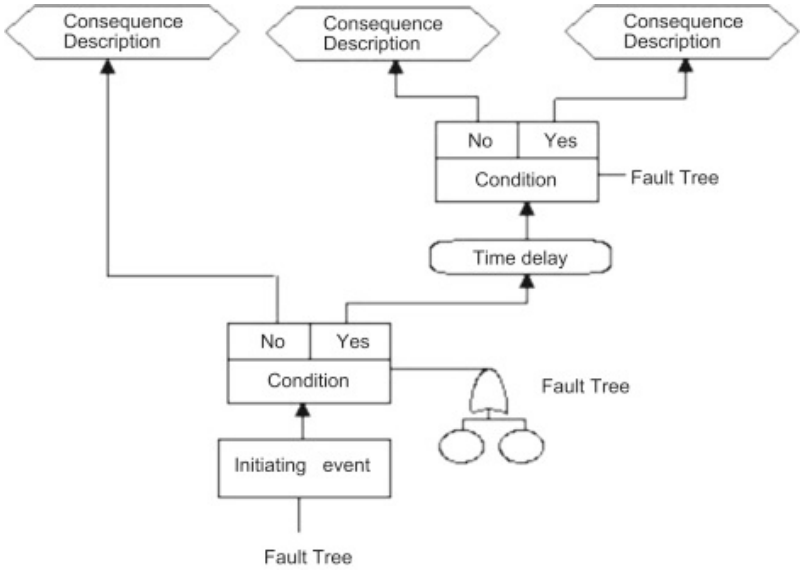

Figura 15. Esempio di diagramma CCA. Fonte: Woodward, J. L. (2012). LNG safety and security aspects. In S. Mokhatab, J. Y. Mak, J. V. Valappil & D. A. Wood (Eds.), Handbook of Liquefied Natural Gas (pp. 359–435). Elsevier.

L'**analisi bayesiana** è una metodologia quantitativa che permette di stimare, tramite tecniche di inferenza statistica, la probabilità condizionata di accadimento di eventi incerti, integrando informazioni pregresse con nuovi dati osservati. Il modello si basa sul teorema di Bayes, il quale permette di calcolare la probabilità a posteriori di un'ipotesi (H) data un'evidenza (E), e può essere espresso mediante la seguente formula:

$$P(H|E) = \frac{P(E|H) \times P(H)}{P(E)}$$

Il teorema può essere ulteriormente esteso al fine di ricomprendere una moltitudine di ipotesi (N) mutualmente esclusive, tra le quali bisogna selezionare l'ipotesi i-esima data l'osservazione effettuata:

$$P(H_i|D) = P(H_i) \times \left[\frac{P(D|H_i)}{\sum P(H_n)\, P(D|H_n)}\right]$$

Il modello consente, quindi, di formalizzare in un parametro stima, $P(H_i)$, le conoscenze esperte in termini probabilistici (*priors*), per poi raffinarle man mano che emergono nuove informazioni (posteriors). In fase di *risk assessment*, l'analisi bayesiana si configura come uno strumento prezioso per la valutazione della *likelihood* del rischio, soprattutto in situazioni in cui i dati storici siano limitati, incerti o parziali. Questa flessibilità rende l'approccio particolarmente utile per la gestione di rischi emergenti.

Il *framework* ERM proposto dal COSO – nel principio 11 – indica che **l'analisi del livello di rischio deve essere condotta a più livelli dell'organizzazione** (divisioni, funzioni, unità operative). Questo consente di comprendere i livelli aziendali impattati dai diversi rischi identificati e come i rischi evolvano attraverso l'organizzazione, permettendo di identificare il livello più adatto ad implementare misure di gestione degli stessi. Ad esempio, un rischio potrebbe impattare in maniera equivalente gli obiettivi aziendali a differenti livelli (prima illustrazione); oppure, due obiettivi di livello divisionale impattati da rischi in maniera lieve possono influenzare in maniera aggravata un obiettivo di livello strategico e quindi la capacità dell'impresa di raggiungere la strategia (seconda illustrazione). Un terzo caso esemplificativo (terza illustrazione) può essere invece rappresentato da rischi che hanno un impatto irrilevante a livello divisionale ma che aumenta in maniera significativa lungo la struttura dell'organizzazione.

Figura 16. Livello di rischio a diversi livelli aziendali

4.3.5 Risk Assessment – Prioritization

Valutati i rischi precedentemente identificati, il passo successivo del processo di *risk assessment* consiste nel **definirne la priorità** – principio 12 COSO –, al fine di fornire *insights* rilevanti a quei soggetti incaricati di sviluppare dei piani di risposta adeguati. In questo contesto l'impresa è interessata a conoscere le tipologie di azioni più adatte a portare il livello di rischio verso il *risk appetite*, l'urgenza richiesta nell'implementare le modalità di risposta e l'investimento necessario per garantire un efficace funzionamento delle azioni correttive.

Per svolgere efficacemente questa fase, il management deve stabilire **criteri di prioritizzazione**, tra i quali il più rilevante è rappresentato dal **livello di rischio** (*level of risk*) definito come funzione congiunta di impatto (*impact*) e probabilità (*likelihood*). Tuttavia, come sottolineato dallo stesso COSO nel framework ERM (2017), alcune imprese stanno ampliando la definizione di livello di rischio, introducendo ulteriori criteri

di valutazione in grado di arricchire l'analisi e renderla più adatta a comprenderne la natura multidimensionale. Un primo criterio è l'**adattabilità** (*adaptability*), intesa come la capacità dell'organizzazione di rispondere e adattarsi alla mutevolezza dello scenario competitivo. Si pensi, ad esempio, a un'azienda che deve riconfigurare le proprie strategie di prodotto in risposta all'evoluzione dei gusti dei consumatori o all'ingresso di nuove tecnologie sul mercato. Un secondo criterio è rappresentato dalla **complessità** (*complexity*), la quale identifica l'ampiezza degli impatti, la natura dei rischi e le loro interconnessioni. Alcuni rischi, infatti, possono impattare in maniera simultanea su più obiettivi aziendali, generando effetti a catena difficili da gestire. Si può considerare, a tal proposito, il caso di un'impresa tecnologica che, nel tentativo di mantenere la *leadership* di mercato, affronta rischi connessi allo sviluppo rapido dei prodotti, alla pressione competitiva e all'aspettativa costante di innovazione da parte dei clienti. La **velocità** (*velocity*), invece, riguarda la rapidità con cui un rischio può produrre effetti negativi. Un esempio potrebbe essere un'interruzione improvvisa nelle attività logistiche dovuta a eventi esterni in grado di compromettere la regolare catena distributiva e di approvvigionamento. La **persistenza** (*persistence*), misura la durata dell'impatto del rischio. Alcuni eventi, infatti, possono avere effetti prolungati nel tempo, influenzando la reputazione, la fiducia dei clienti o la performance finanziaria anche dopo la loro risoluzione. Un caso esemplificativo può essere quello di un'azienda che subisce un attacco informatico, i cui effetti in termini di credibilità e perdita di dati sensibili si protraggono ben oltre il contenimento tecnico dell'evento. Infine, **la capacità di ripresa** (*recovery*) rappresenta l'abilità dell'organizzazione di ritornare entro i livelli di performance accettabili, una volta che il rischio si è concretizzato. È importante sottolineare che questo criterio si riferisce alla capacità effettiva di ripresa, mentre il tempo necessario per raggiungere il ripristino è considerato parte della persistenza, non della *recovery*.

Il ***value at risk*** (VaR) è una tecnica di analisi quantitativa particolarmente diffusa in ambito finanziario che, se applicata all'interno di un framework ERM, diventa un utile strumento per quantificare il livello di rischio in maniera tale da renderlo facilmente confrontabile con la soglia di *risk appetite* definita dal management. Il modello, basato su un approccio probabilistico, elabora informazioni derivanti da altri metodi di analisi (es. simulazione Monte Carlo per derivare la forma della distribuzione di probabilità) e

da dati storici, al fine di stimare il livello massimo di perdita attesa che un'organizzazione può subire su un determinato portafoglio, in un dato orizzonte temporale e con un certo livello di confidenza statistica. L'output del sistema assume solitamente la seguente forma "con una probabilità del 95%, la perdita non supererà X euro nei prossimi N giorni". Nel processo di *risk assessment* risulta particolarmente utile in quanto consente di stimare una misura monetaria riguardante i rischi ed il periodo temporale all'interno del quale potrebbe verificarsi, facilitando considerevolmente il confronto tra i vari rischi soprattutto in sede di prioritizzazione.

4.3.6 Risk Response

Una volta aver individuato, analizzato e prioritizzato i rischi, l'impresa giunge ad una fase critica del processo di risk management: **decidere come rispondere ai rischi**. Lo scopo di questa fase è identificare le misure da mettere in atto per ricondurre il livello di rischio ottenuto e ricondurlo il più possibile al livello definito dal *risk appetite*, o per lo meno portarlo all'interno del *range* di tollerabilità.

Le **risposte al rischio** (*risk response*) che l'impresa può mettere in atto vengono classificate all'interno del framework proposto dal COSO nelle seguenti categorie:

- **Accettare**: non intraprende alcuna azione per modificare il livello di rischio, in quanto questo è già considerato accettabile o tollerabile.
- **Evitare**: l'impresa decide di rimuovere completamente il rischio. Questa tipologia di risposta viene applicata quando non è possibile ridurre il rischio ad un livello considerato accettabile.
- **Perseguire**: l'azienda decide consapevolmente di aumentare il rischio in quanto interessata ad aumentare le proprie performance. Può avvenire o perché il rischio è inferiore al risk appetite e quindi l'impresa è in grado di sopportarne di più, oppure la decisione da intraprendere è così strategicamente rilevante non farlo può esporre a rischi maggiori.
- **Ridurre**: vengono intraprese azioni per diminuire il rischio.
- **Condividere**: il rischio viene condiviso attraverso strumenti quali assicurazioni, *outsourcing*, o accordi di collaborazione, che permettono di trasferirlo anche su altri attori.

In alcuni casi, tuttavia, l'impresa può trovarsi nell'impossibilità di portare il rischio ad un livello accettabile; in questo caso dovrà prendere in considerazione altre **strategie di gestione più "invadenti"** nei confronti della strategia aziendale. La prima tra queste è la **possibilità di rivedere l'obiettivo aziendale**, questa opzione si rende necessaria proprio nel caso in cui nessuna delle strategie di gestione del rischio precedentemente indicate sia in grado di influenzare il rischio nella maniera desiderata. La seconda, consiste nel **rivedere la strategia oppure optare per un'altra** che sia più in linea con il *risk appetite* dell'azienda. La terza, invece, si rende necessaria nel momento in cui l'impresa si trova a dover prendere sistematicamente la decisione di violare *risk appetite*, oppure il rispettare questo "limite" comporta esporsi a rischi ancora più elevati. In questo caso l'organizzazione dovrà **rivedere la definizione della sua propensione al rischio**.

Una volta applicate queste misure, ed aver valutato il loro impatto, è importante tenere presente che queste non eliminano completamente il rischio: una sua componente residuale sarà sempre presente (***residual risk***). Inoltre, è importante considerare che l'implementazione delle misure di gestione può portare con sé ulteriori rischi, questi sono noti come rischi secondari (***secondary risk***[69]) e devono essere sottoposti allo stesso processo di identificazione e valutazione dei primari. In questo contesto assume particolare importanza la **comunicazione verso gli *stakeholder*** interessati dei rischi residuali e secondari, in maniera tale che possano essere monitorati consapevolmente ed integrati nel processo decisionale. La mancata gestione o comunicazione dei rischi residui e secondari può infatti generare falsi livelli di sicurezza, sottostimando il rischio reale residuo[70] ed esponendo l'organizzazione a vulnerabilità non percepite.

Tra i **modelli decisionali** a supporto della selezione delle strategie di risposta al rischio, l'approccio ALARP (*as low as reasonably practicable*) e l'analisi costi-benefici (CBA) rappresentano strumenti complementari per valutare la sostenibilità e l'adeguatezza degli interventi di gestione. Entrambi i metodi consentono supportare i *decision-maker* nel processo di creazione di piani di risposta ai rischi introducendo variabili di natura economica, tecnica e sociale.

---

[69] Hillson, D. (1999). Developing Effective Risk Responses. *Proceedings of the 30th Annual Project Management Institute Seminars & Symposium.* Philadelphia: Project Management Institute.

[70] Ewertowski, T., Berlik, M., & Sławinska, M. (2024). The Effectiveness of Operational Residual Risk Assessment: The Case of General Aviation Organizations in Enhancing Flight Safety in Alignment with Sustainability. *Sustainability*.

Il **modello ALARP** costituisce un fondamentale criterio decisionale che guida i *manager* nello stabilire se un rischio possa essere tollerato oppure debba essere ridotto. Questo modello si basa sull'idea che non tutti i rischi possono, o devono, essere eliminati completamente, ma che il loro livello dovrebbe essere mantenuto il più basso possibile, compatibilmente con ciò che è "ragionevolmente praticabile". La rappresentazione tipica del modello prevede un triangolo rovesciato sul quale vengono individuate **tre aree**: una **zona accettabile**, in cui il rischio è sufficientemente basso da non richiedere ulteriori azioni; una **zona intermedia** (ALARP), in cui il rischio può essere tollerato solo se i benefici derivanti da sua ulteriore riduzione ulteriore non sono considerati ragionevoli rispetto ai costi da dover sostenere; una **zona intollerabile**, in cui il rischio deve essere necessariamente ridotto. Inserito all'interno del processo di prioritizzazione, il modello ALARP aiuta il management a giustificare razionalmente l'accettazione di alcuni rischi residui, in linea con i livelli di *risk tolerance*.

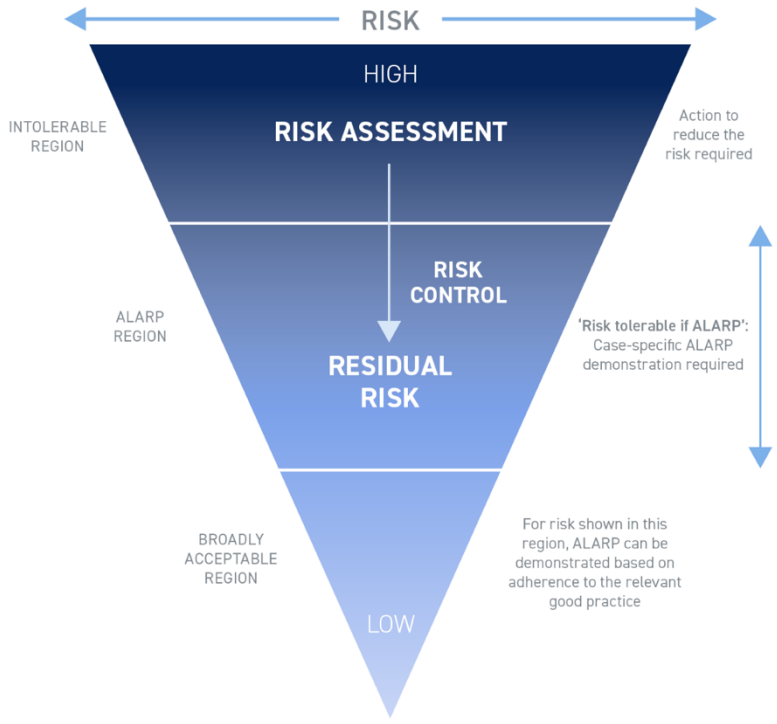

Figura 17. Esempio del diagramma ALARP. Fonte: https://britanniapandi.com/2024/08/understanding-effective-risk-assessment/

La ***cost-benefit analysis*** (CBA) è una tecnica di valutazione economica che consente di confrontare i costi associati all'implementazione di una misura di risposta al rischio con i benefici da essa generati. Questa metodologia prevede una stima quantitativa dei costi diretti (es. investimenti, costi operativi), dei costi indiretti (es. impatti reputazionali, interruzioni) e dei benefici attesi (es. riduzione delle perdite finanziarie, miglioramento

della resilienza). Il risultato viene normalmente espresso attraverso lo sviluppo di diversi indicatori, tra i quali i principali sono: il ***net present value***, che misura il valore netto attualizzato dei benefici al netto dei costi; il ***benefit-cost ratio***, che rappresenta il rapporto tra i benefici attesi e i costi sostenuti; e la ***payback period analysis***, che indica il tempo necessario per recuperare l'investimento. In ambito ERM, la CBA costituisce uno strumento di supporto al processo decisionale, consentendo la comparazione tra diverse alternative di trattamento del rischio al fine di selezionare l'opzione che meglio garantisca un adeguata ed efficiente allocazione delle risorse aziendali.

4.3.7 Portfolio View

Una criticità da evitare in fase di implementazione del sistema di ERM è quella di gestire i rischi a compartimenti stagni, ignorando così le loro interazioni e come queste possano modificare l'esposizione complessiva al rischio da parte dell'impresa. Il COSO, per sopperire a questa situazione e migliorare l'integrazione del processo ERM, suggerisce – nel principio numero 14 – di **adottare una visione a portafoglio dei rischi** (*portfolio view*), ossia una visione aggregata e trasversale del profilo di rischio dell'organizzazione rispetto alla sua propensione al rischio.

In fase di sviluppo del piano riguardante le misure di gestione del rischio – come discusso nel paragrafo precedente – non è quindi sufficiente tenere presente l'esistenza di rischi residuali e di rischi secondari per permettere al processo ERM di adempiere la propria funzione di protezione e creazione del valore aziendale; è necessario fornire al *management* ed al *board* strumenti in grado di supportare il processo decisionale che permettano di considerare "la tipologia, la gravità e le interdipendenze dei rischi e come questi possano impattare sulle performance"[71]. Adottare una visione a portafoglio garantisce quindi che le risposte ai rischi non sia applicate in maniera isolata, ma che queste siano predisposte in maniera coerente e coordinata, riducendo sovrapposizioni, inefficienze e lacune nella copertura complessiva dei rischi.

Il COSO, nel suo framework ERM del 2017, individua **4 livelli di sviluppo ed integrazione della visione a portafoglio**:

[71] COSO. (2017). *Enterprise Risk Management: Integrating with Strategy and Performance.* COSO.

- ***Risk view*** (integrazione minima): i rischi vengono individuati ed analizzati in maniera discreta e le risposte vengono applicate singolarmente senza considerare le relazioni intercorrenti. L'attenzione del *management* è quindi posta esclusivamente nella riduzione dei singoli rischi e non sugli obiettivi ad essi associati.
- ***Risk category view*** (integrazione limitata): il *management* sfrutta le informazioni ottenute nel processo di identificazione dei rischi per raggrupparli in categorie. Le misure di gestione vengono applicate prendendo in considerazione il loro impatto nella riduzione del rischio associato ad una determinata categoria.
- ***Risk profile view*** (integrazione parziale): l'organizzazione sposta la propria attenzione dai rischi al loro impatto sugli obiettivi di *business*. Nel processo di sviluppo del piano di gestione dei rischi il *management* prende in considerazione le relazioni tra i rischi che impattano su specifici obiettivi di *business*.
- ***Portfolio view*** (integrazione completa): l'attenzione dell'organizzazione si concentra sulla strategia e sul conseguimento degli obiettivi di *business*. Questo approccio consente di identificare, valutare, rispondere e monitorare i rischi ai livelli più appropriati per supportare il processo decisionale. Il *management* ed il *board* supervisionano la strategia ed i rischi ad essa correlati, mentre la responsabilità riguardante gli obiettivi di business e dei rischi specifici viene distribuita lungo tutta la struttura organizzativa.

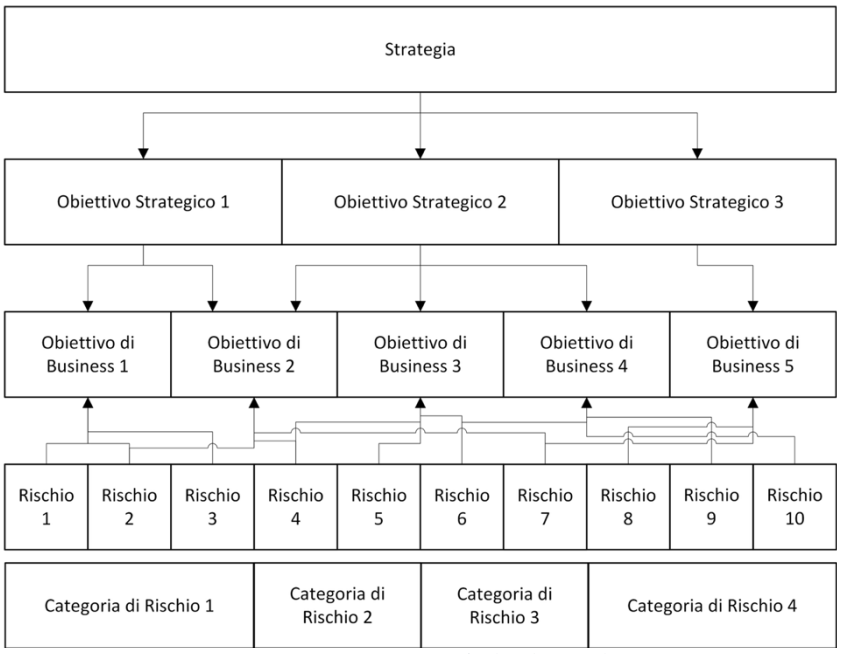

Figura 18. Vista a Portafoglio dei Rischi

Richard Adler – nel suo libro *Bending the Law of Unintended Consequences* – sviluppa un **modello di visione a portafoglio** dei rischi come strumento di supporto al processo decisionale. Partendo dal concetto di portafoglio in ambito finanziario, inteso come una combinazione di attività finanziarie detenute da un investitore (quali azioni, obbligazioni, strumenti monetari, ecc.) con l'obiettivo di massimizzare il rendimento atteso a fronte di un determinato livello di rischio; Adler propone un ribaltamento di prospettiva, definendo il **portafoglio dei rischi** come uno strumento mediante il quale l'impresa "cerca di massimizzare la quantità di riduzione del rischio che può essere ottenuta con un insieme fisso di risorse"[72]. Questa impostazione teorica si concretizza in un modello decisionale, simulativo e dinamico, in grado di supportare le imprese nella selezione ed allocazione delle misure di gestione dei rischi in maniera coordinata ed integrata.

Il modello prevede una struttura composta da **tre elementi fondamentali**: le **minacce** (*threats*), le quali costituiscono eventi in grado di avere un impatto sul raggiungimento degli obiettivi; i ***target* vulnerabili** (*target sets*), ossia *asset*, *business unit*, o *stakeholders* esposti alle minacce; e le **misure di riduzione del rischio** (*risk reduction measures*). Ogni combinazione di minaccia e *target* costituisce un segmento di esposizione al rischio che deve essere oggetto di un'azione di gestione. Adler, paragonando questa struttura ad un tavolo da gioco, identifica ogni segmento di rischio come una "casella" dello stesso, ed ogni misura di mitigazione come un "gettone" da posizionare su una o più caselle a seconda della sua efficacia. In quest'ottica, le decisioni aziendali assumono la forma di "scommesse" consapevoli su specifici segmenti del portafoglio, vincolate dalla disponibilità limitata di risorse economiche e operative.

Adler prosegue individuando un insieme di **metriche di *performance*** finalizzate a supportare il processo decisionale mediante un'analisi strutturata del *trade-off* che intercorre tra rischio e costi. Particolare attenzione è prestata alla metrica del **ROI** (*Return On Investment*), inteso come indicatore di efficienza economica delle misure di *risk reduction*. Calcolato come rapporto tra l'impatto economico ottenuto dalla riduzione del rischio ed il costo sostenuto per l'implementazione delle relative le misure di gestione, la sua applicazione nel contesto dell'ERM incontra una serie di limitazioni. Questo perché un mero confronto tra il livello di rischio prima e dopo l'implementazione della misura

[72] Adler, R. M. (2020). *Bending the Law of Unintended Consequences: A Test-Drive Method for Critical Decision-Making in Organizations.* Cham: Springer.

tende a produrre risultati distorti, in quanto ignora la dinamica temporale dei costi e dei benefici.

Per superare questa limitazione, l'autore propone una metrica più robusta e realistica: il **CROI** (*Cumulative Return On Investment*), indicatore che tiene conto sia dell'accumulo progressivo dei benefici (ossia della quantità di rischio evitato lungo l'intero arco temporale di simulazione), sia dell'evoluzione dei costi nel tempo, articolati in costi di avviamento e ricorrenti.

$$\text{CROI} = \frac{\text{Riduzione del Rischio Totale Cumulata}}{(\text{Costo Totale di Riduzione del Rischio nel Tempo}) \times (\text{Rischio Iniziale} \times \text{Durata})}$$

Il CROI viene calcolato come il rapporto tra il rischio cumulativamente ridotto in ciascun intervallo temporale e il costo totale sostenuto, normalizzato per la durata e il livello di rischio iniziale. Tale approccio consente di rappresentare con maggiore fedeltà l'effettiva efficacia economica delle strategie alternative, evitando le sovrastime legate all'utilizzo di indicatori statici. Inoltre, il CROI consente di mettere a confronto strategie implementate su orizzonti temporali diversi o caratterizzate da dinamiche di spesa disomogenee, rendendolo uno strumento particolarmente utile nel contesto delle decisioni complesse e di lungo periodo.

Il modello decisionale richiede un set minimo di **dati in *input*** distinti da Adler stesso in **tre categorie**: **componenti del rischio** (*risk components*), **misure di gestione del rischio** (*risk management*) ed un **insieme di ipotesi generali** ("*what-if*") che rappresentano possibili scenari evolutivi nel tempo. Queste informazioni in ingresso del modello sono direttamente provenienti dalle diverse fasi del modello ERM e la loro qualità influenza in maniera diretta l'attendibilità ed accuratezza dell'*output* del modello.

Adler arriva così alla definizione del cuore operativo del proprio modello, una **fase simulativa** che consente di effettuare *stress test* sulle misure di gestione del rischio implementate e proiettare così nel tempo gli effetti al fine di monitorarne l'efficacia. Il processo di test del modello si sviluppa mediante una sequenza ciclica di azioni raggruppate in **cinque fasi**: (1) l'introduzione di eventi o cambiamenti contestuali rilevanti (es. nuove normative, crisi economiche, incidenti), (2) l'aggiornamento degli scenari in base a trend e forze esterne, (3) il calcolo dei costi accumulati e della riduzione di rischio ottenuta nell'intervallo precedente, (4) l'applicazione delle nuove unità delle

misure previste dal piano di *roll-out* e (5) l'aggiornamento delle metriche aggregate a livello di portafoglio.

Il modello sviluppato da Adler consente di rappresentare con precisione la complessità delle scelte di gestione del rischio, tenendo conto della natura mutevole dei rischi, delle trasformazioni del contesto competitivo, delle implicazioni delle misure di gestione. Di particolare rilevanza è la capacità del modello di prendere in considerazione l'interazione tra le misure di gestione e il contesto competitivo, soprattutto mediante la definizione del modello di adattamento strategico delle minacce (*threat shifting*), permettendo al modello di rappresentare non solo l'efficacia iniziale di una misura, ma anche la sua sostenibilità nel tempo in funzione all'evoluzione del contesto. Ciò rende questa simulazione uno strumento strategico in grado di sostenere un processo decisionale proattivo volto ad anticipare il cambiamento ed a favorire l'adattamento del sistema aziendale

4.4 Integrazione tra ERM e Sistema di Controllo Interno

Come mostrato in diversi punti del presente elaborato, affinché il sistema di Enterprise Risk Management possa adempiere nella maniera più efficace alla sua funzione di protezione e creazione di valore per l'azienda ed i propri *stakeholder*, è necessario che sia integrato all'interno dei processi aziendali e che quindi non operi come una funzione a sé stante. L'integrazione, tuttavia non deve avvenire solo a livello strategico, decisionale e di *performance*, ma deve abbracciare anche il sistema di controlli endosocietari. Come lo stesso COSO sostiene: "i professionisti della gestione del rischio dovrebbero lavorare in tandem con la struttura di controllo interno di un'entità. (…) L'integrazione di solidi controlli interni può supportare l'efficacia dell'ERM"[73]. Infatti, in mancanza di un adeguato sistema di controllo interno non si può avere sicurezza riguardo l'applicazione delle prassi, dei principi e delle modalità di gestione dei rischi all'interno dell'entità. In quest'ottica di profondo legame che intercorre, quindi, tra SCI (sistema di controllo interno) ed Enterprise Risk Management si può arrivare a delineare un unico grande, e omnicomprensivo, sistema interno all'organizzazione definito **SCIGR** (sistema di controllo interno e gestione dei rischi). In questo contesto ERM e SCI possono essere

[73] COSO, WBCSD. (2018). *Enterprise Risk Management: Applying enterprise risk management to environmental, social and governance-related risks.* COSO, WBCSD.

considerati come "gli strumenti operativi ed i pilastri del governo societario"[74] ed in quanto tali forniscono ai manager di vertice i mezzi per adempiere al proprio compito di supervisione strategica dell'operato societario.

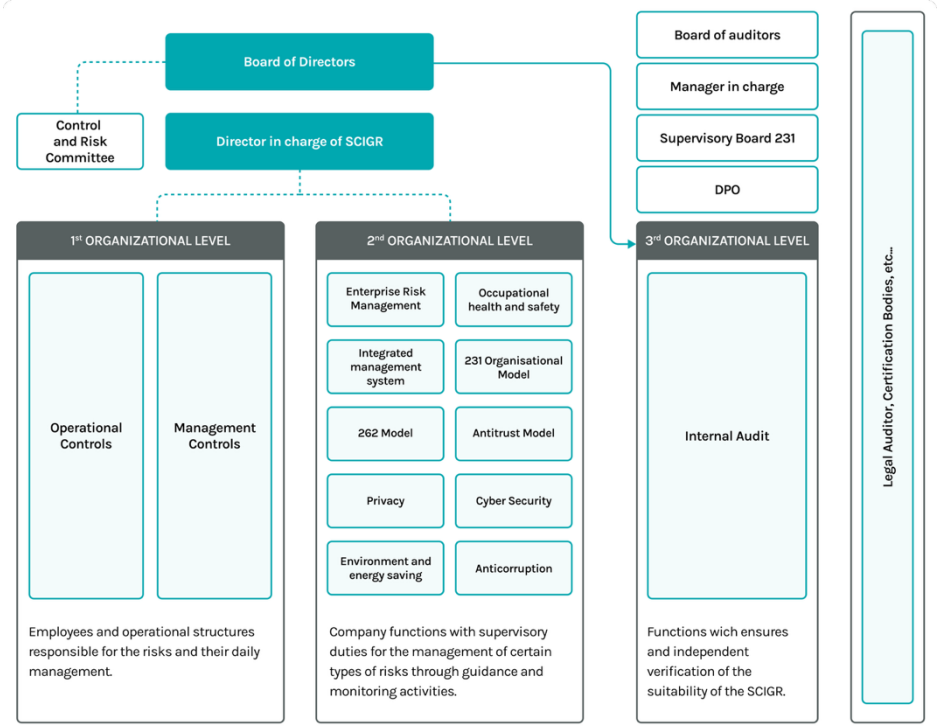

Figura 19. Struttura Sistema SCIGR di Acea. Fonte:https://www.gruppoacea.it/en/governance/internal-control-and-risk-management-system

L'**architettura del sistema di controlli** segue un modello articolato in tre livelli di natura endosocietaria, ed un quarto di natura esosocietaria. Il **primo livello** di controllo, noto anche come "controlli di linea", è portato avanti dai dipendenti che svolgono un ruolo operativo, questi controlli mirano a garantire a corretta esecuzione dei processi aziendali al fine di prevenire i rischi. Il **secondo livello** di controllo è affidato alle funzioni aziendali che ricoprono un ruolo di supervisione, questi controlli riguardano il monitoraggio continuo del corretto funzionamento e dell'adeguatezza dei controlli posti in essere a livello aziendale. Il **terzo livello** di controllo invece è presidiato dalla funzione di *internal audit*, la quale si occupa di effettuare valutazioni indipendenti riguardo l'adeguatezza strutturale e di funzionamento del sistema di controllo interno. Il **quarto livello**, quello riguardante i controlli effettuati da *auditor* esterni la società, riguarda la validazione delle informazioni prodotte internamente alla società. Questo quarto livello – per le S.p.A. – può essere suddiviso in diverse categorie di controlli: revisione legale dei conti, affidata

[74] Dittmeier, C. A. (2007). *Internal Auditing. Chiave per la Corporate Governance.* Egea.

ad un revisore esterno o società di revisione; controllo della Consob, per le società quotate; controllo giudiziario sulla gestione; controlli effettuati da autorità indipendenti (es. AGCM), riguardanti ambiti normativi specifici; e controlli effettuati da enti certificatori indipendenti, i quali verificano il rispetto di norme volontarie alle quali le imprese decidono di aderire (es. ISO).

5. ERM e Obiettivi ESG

Da quando il modello *triple bottom line* – trattato nel paragrafo 2.3.2 – è stato elaborato, l'attenzione sia da parte delle imprese che di enti di natura pubblica ed internazionale nei confronti delle tre dimensioni delle performance è cresciuta significativamente. Questa visione multidimensionale permea **l'Agenda 2030** dell'ONU, un piano d'azione comune sottoscritto da 193 paesi membri nel 2015, contenente l'impegno di affrontare le sfide globali promuovendo un modello di sviluppo sostenibile basato su tre dimensioni: economica, sociale ed ambientale. Il cuore dell'agenda è rappresentato dai 17 obiettivi di sviluppo sostenibile (SDGs – *Sustainable Development Goals*), a loro volta suddivisi in 169 target, che rappresentano le principali tematiche da affrontare per creare le condizioni di una crescita economica inclusiva e sostenibile. Questi obiettivi, oltre che indicare la strada da prendere ai vari legislatori, costituiscono per le imprese dei fondamentali punti di riferimento per valutare l'impatto che le loro politiche di sostenibilità generano.

Figura 20. Sustainable Development Goals - SDGs

Diverse sono le **motivazioni** che hanno spinto le organizzazioni a focalizzarsi in maniera estremamente attenta sugli aspetti ESG, ma tra queste possiamo evidenziare in maniera

particolare: l'evoluzione del panorama dei rischi globali, crescenti pressioni da parte dei consumatori e della collettività, maggior interesse da parte degli investitori, aumento di regolamentazione in materia.

Per quanto riguarda la prima motivazione individuata, **l'evoluzione del panorama dei rischi globali**, possiamo prendere in analisi il *Global Risk Report* del WEF e studiare come la percezione dei rischi globali sia cambiata nel tempo. Nel 2007, tra i cinque principali rischi in termini di impatto, solamente uno era riconducibile a temi ESG (Pandemie), nel 2015 tre su cinque rischi globali in termini di impatto sono legati a tematiche ESG (crisi dell'acqua, pandemie e crisi climatica)[75]. Nel report del 2025, invece, dei cinque principali rischi in termini di impatto nel lugo periodo, ben quattro sono legati a tematiche ESG (condizioni climatiche estreme, perdita di biodiversità, cambiamenti critici al sistema Terra, scarsità di risorse naturali)[76].

Le **crescenti pressioni da parte dei consumatori** sono un ulteriore elemento che contribuisce a indirizzare le imprese verso comportamenti più consapevoli e una visione più sostenibile del loro business. A titolo esemplificativo può essere preso uno studio svolto annualmente da YouGov – *Who Cares? Who Does? Sustainability Report* – in cui viene analizzata l'attenzione dei consumatori *retail* nei confronti della sostenibilità elaborando dati raccolti mediante un'indagine svolta in quindici paesi europei. Nell'edizione del 2024 individua come il 24% della popolazione intervistata sia costituita da consumatori *eco-actives*, ossia soggetti fortemente impegnati nel ridurre l'impatto ambientale, mentre un altro 37%, costituito dagli *eco-considers*, presta attenzione alla sostenibilità ma ritiene che apportare un cambiamento spetti prevalentemente a governi e aziende[77]. Ad ulteriore sostegno di questa dinamica di pressione sociale nei confronti delle società, KPMG in un suo report del 2022 conclude che i "cambiamenti sistemici negli atteggiamenti dei consumatori e nei comportamenti d'acquisto, rilevati inizialmente tra i millennials, si stanno ora diffondendo in tutte le fasce demografiche. Le aziende devono assicurarsi che i loro impegni siano autentici e permeino le esperienze dei clienti, il che richiede un approccio integrato al cliente e all'ESG."[78]

[75] WEF. (2015). *Global Risk Report 2015.* World Economic Forum.
[76] WEF. (2025). *Global Risks Report 2025.* World Economic Forum.
[77] YouGov. (2024). *Who Cares? Who Does? Sustainability Report - 6th Edition.* YouGov.
[78] KPMG. (2022). *Me, my life, my wallet.* KPMG.

Anche da parte degli **investitori** si osserva una crescente attenzione alle tematiche ESG. Negli ultimi anni, infatti, si è registrato un *trend* in costante crescita nelle proposte legate ad attività ESG da parte degli azionisti di aziende statunitensi, che nel 2018 rappresentavano circa il 50% del totale[79]. Larry Fink, CEO di BlackRock, nella sua lettera annuale ai CEO del 2018 adotta pienamente questa nuova visione della realtà economica. In questo documento sostiene che "Senza *sense of purpose*, nessuna azienda, pubblica o privata, può raggiungere il proprio pieno potenziale. Alla fine, perderà la licenza di operare da parte dei principali *stakeholder*. Soccomberà alle pressioni a breve termine per distribuire gli utili e, nel processo, sacrificherà gli investimenti nello sviluppo dei dipendenti, nell'innovazione e nelle spese in conto capitale necessari per la crescita a lungo termine. (…) La capacità di un'azienda di gestire le questioni ambientali, sociali e di *governance* dimostra la *leadership* e il buon governo che sono essenziali per una crescita sostenibile."[80] Questo crescente interesse degli investitori è chiaro anche nel caso dell'emissione degli *European Green Bond* da parte di A2A nel gennaio del 2025. Il livello di attenzione da parte degli investitori è stato tale che l'emissione ha registrato una domanda pari a 4,4 volte l'ammontare offerto. Inoltre, il rendimento annuo si è attestato a un livello inferiore di 125 punti base rispetto al tasso di riferimento[81].

5.1 Normativa ESG in UE

Negli ultimi anni diversi *policy-maker* a livello globale hanno elaborato ed approvato normative che impongono alle organizzazioni di considerare nel loro operato anche tematiche riguardanti gli obiettivi ESG.

L'Unione Europea è il soggetto internazionale che si è dotato di un più avanzato e pervasivo impianto normativo riguardante la sostenibilità, figlio di un progetto politico che adotta una visione di lungo periodo e basato sull'agenda 2030 elaborata dall'ONU. Il punto di partenza di questo processo normativo è rinvenibile nella redazione da parte della commissione europea del **piano d'azione per la finanza sostenibile del 2018**. In tale documento strategico l'Unione esprime l'intenzione di voler riformare profondamente il

[79] COSO, WBCSD. (2018). *Enterprise Risk Management: Applying enterprise risk management to environmental, social and governance-related risks.* COSO, WBCSD.
[80] Fink, L. (2018). *Larry Fink's 2018 Letter to CEOs: A sense of Purpose.* Tratto da BlackRock: https://www.blackrock.com/corporate/investor-relations/2018-larry-fink-ceo-letter
[81] A2A. (2025, Gennaio 23). *A2A, primo european Green Bond collocato sul mercato.* Tratto da A2A: https://www.gruppoa2a.it/it/media/comunicati-stampa/a2a-primo-european-green-bond-mercato

sistema finanziario per allinearlo agli obiettivi di sostenibilità ambientale, sociale e di *governance*. Tuttavia, il vero punto di svolta in ambito normativo si ha nel 2020 con l'approvazione da parte del consiglio europeo del **Green Deal**, definito dagli stessi atti ufficiali come la "nuova strategia di crescita che mira a trasformare l'UE in una società equa e prospera, con un'economia moderna, efficiente sotto il profilo delle risorse e competitiva, nella quale non vi siano emissioni nette di gas a effetto serra entro il 2050 e la crescita economica sia disaccoppiata dall'uso delle risorse"[82].

Da questo primo atto ne discende a cascata, negli anni successivi, una serie di normative volte a raggiungere gli obiettivi proposti:

- **EU Environmental Taxonomy (Reg. 2020/852)**: stabilisce criteri condivisi per determinare se un'attività economica può definirsi ecosostenibile e impone obblighi di rendicontazione per alcune imprese e partecipanti a mercati finanziari. Nello specifico, definisce i criteri per cui un'attività economica possa essere considerata ammissibile alla tassonomia ed i criteri per essere definita allineata: vaglio tecnico, *do not significant harm* e garanzie minime sociali.
- **Climate DA e Disclosure DA (Reg. 2021/2139 e 2021/2178)**: precisano il contenuto e la presentazione delle informazioni che le imprese devono comunicare in merito alle attività economiche ecosostenibili mediante la definizione di tre KPI (Fatturato, CapEx, OpEx).
- **Corporate Sustainability Reporting Directive – CSRD (Dir. 2022/2464)**: in vigore dal 2024 per le grandi imprese. Prevede criteri di rendicontazione delle *performance* ESG trasparenti e facilmente confrontabili (*European Sustainability Reporting Standars* - ESRS).
- **CBAM – Carbon Border Adjustment Mechanism (Reg. 2023/956)**: introduce un sistema che prezza le emissioni incorporate nei prodotti altamente inquinanti.
- **Corporate Sustainability Due Diligence Directive – CS3D (Dir. 2024/1760)**: introduce obblighi di *due diligence* in materia ESG per le imprese lungo la catena di fornitura.

[82] European Commission. (2019). The European Green Deal.

Tuttavia, questa linea politica tenuta dall'Unione Europea ha riscontrato nel tempo delle **criticità** e diversi autori e studi hanno mosso **critiche** nei suoi confronti. Uno studio[83] condotto da CFA Institute – Research & Policy Center – mediante un sondaggio rivolto ad operatori del settore dell'*asset and wealth management* in Europa, ha evidenziato la complessità dell'attuale impianto normativo ed i costi associati alla raccolta di dati in ambito ESG; riconoscendo, tuttavia, il merito all'attuale regolamentazione di spingere gli investitori verso prodotti finanziari che abbiano un *focus* su questa tematica ed il suo contributo nel guidare l'agenda globale verso una finanza sostenibile. Alcune critiche alle normative ESG europee provengono anche dal mondo imprenditoriale, in particolare, "la European Round Table for Industry, che rappresenta aziende con un fatturato annuo complessivo di 2.000 miliardi di euro, ha dichiarato che le normative severe stanno accelerando la perdita di competitività e suggerisce che le opportunità potrebbero essere migliori al di fuori dell'Europa"[84]. A queste critiche viene fornita maggior rilevanza da Mario Draghi nel suo rapporto "il futuro della competitività europea"[85] pubblicato nel settembre del 2024, dove evidenzia che, sebbene queste normative mirino a promuovere la sostenibilità, generano anche significative criticità, in particolare legate al peso regolamentare e alla complessità, che potrebbero ostacolare la competitività europea.

Muovendo da queste critiche la commissione europea ha presentato il **pacchetto omnibus**, una proposta di iniziative volte a ridurre il carico amministrativo per le imprese e promuovere la competitività. La prima parte del pacchetto, approvata nell'aprile del 2025, ha posticipato l'entrata in vigore degli obblighi di rendicontazione della CSRD e della CS3D, così che le imprese della seconda e terza ondata previste dalla CSRD dovranno pubblicare il bilancio di sostenibilità dal 2028 e 2029 anziché dal 2026 e 2027. Tali rinvii sono stati recepiti a livello nazionale con il **Decreto-Legge n. 95/2025**, convertito nella **Legge n. 118/2025**, che ha modificato il calendario di attuazione italiano stabilito dal D.lgs. 125/2024. In particolare, il decreto ha confermato:

- per le grandi imprese già soggette alla Non Financial Reporting Directive (NFRD), l'obbligo a partire dall'esercizio 2024, con pubblicazione nel 2025;

[83] Silvestri, R., & Kamerling, J. (2024). *CFA Institute Survey Report on the ESG Regulatory Framework in the EU.* CFA Institute.
[84] ESG Post. (2024, 9 9). *EU's ESG rules face criticism from European businesses*. Tratto da ESG Post: https://esgpost.com/eus-esg-rules-face-criticism-from-european-businesses/
[85] Draghi, M. (2024). *The future of European competitiveness.* European Commission.

- per le altre grandi imprese (oltre 250 dipendenti o determinate soglie di fatturato e bilancio), lo slittamento all'esercizio 2027 (con pubblicazione nel 2028);
- per le PMI quotate non microimprese, l'entrata in vigore dal 2028 (con prima pubblicazione nel 2029).

Contestualmente, anche l'obbligo di *due diligence* in materia di sostenibilità previsto dalla Corporate Sustainability Due Diligence Directive (CSDDD, o CS3D) è stato differito, con slittamenti al 2028 per le imprese di maggiori dimensioni e al 2029 per le altre categorie.

Questo intervento normativo, se da un lato concede alle imprese un margine temporale più ampio per predisporre sistemi di raccolta e rendicontazione dei dati ESG, dall'altro rappresenta un segnale della volontà del legislatore Europeo e Nazionale di garantire un'applicazione graduale e sostenibile degli obblighi, lasciando tuttavia impregiudicato il ruolo strategico della sostenibilità quale fattore di *governance* e competitività.

5.2 Rischi Collegati agli Obiettivi ESG

Con l'evoluzione del concetto di *performance* aziendale, dalla mera dimensione economica ad una visione più globale ed orientata al concetto di sostenibilità, l'impresa amplia la propria consapevolezza riguardo il contesto nel quale è inserita ed opera. I **rischi collegati agli obiettivi ESG** riguardano, quindi, minacce o opportunità che un'impresa affronta, o potrebbe affrontare, riguardo le tre dimensioni che definiscono il concetto di sostenibilità.

Benché il concetto di rischi associati agli obiettivi ESG non presenti una formulazione univoca, diversi enti di normazione hanno intrapreso un percorso di **definizione e classificazione**. In tal senso, **MSCI** ha sviluppato una metodologia finalizzata alla valutazione di questa tipologia di rischi[86], identificando i principali temi relativi a ciascuno dei tre *pillar* della sostenibilità, nonché le problematiche chiave che possono avere un impatto finanziario sulle performance aziendali e che, pertanto, devono essere oggetto di monitoraggio.

[86] MSCI. (2024). *ESG Ratings Methodology.* MSCI ESG Research LLC.

3 Pilastri	10 Temi	33 Temi Chiave ESG
Ambiente	Cambiamento Climatico	Emissioni di CO_2; Vulnerabilità ai cambiamenti climatici; Finanziamento dell'impatto ambientale; Impronta carbonica dei prodotti
	Capitale Naturale	Biodiversità e uso del suolo; Approvvigionamento di materie prime; Stress Idrico
	Inquinamento e Rifiuti	Rifiuti elettronici; Materiali da imballaggio e rifiuti; Emissioni tossiche e rifiuti
	Opportunità Ambientali	Opportunità in: Tecnologie pulite, Edilizia sostenibile, Energie rinnovabili
Sociale	Capitale Umano	Salute e sicurezza; Sviluppo del capitale umano; Gestione del lavoro; Standard lavorativi lungo la catena di fornitura
	Responsabilità di Prodotto	Sicurezza chimica; Protezione finanziaria dei consumatori; Privacy e sicurezza dei dati; Sicurezza e qualità dei prodotti; Investimenti responsabili
	Opposizioni degli Stakeholders	Relazioni con la comunità; Approvvigionamento controverso
	Opportunità Sociali	Accesso alla finanza; Accesso a servizi sanitari; Opportunità in salute e nutrizione
Governance	Corporate Governance	Consiglio di amministrazione; Retribuzioni; Proprietà e controllo; Contabilità
	Comportamento Aziendale	Etica di impresa; Trasparenza fiscale

Society for Corporate Governance e BrownFlynn, in un loro report del 2018[87], hanno evidenziato che i **rischi associati a tematiche ESG** hanno delle **caratteristiche in comune**: sono legati all'operatività o prodotti *core* di un'azienda, sono in grado di impattare in maniera rilevante sul suo valore intangibile, la sua reputazione o la sua capacità di operare, infine, sono solitamente oggetto di interesse mediatico. Queste caratteristiche rendono questa tipologia di rischi strettamente legata a quelli tradizionalmente associati all'operatività aziendale. Risulta perciò necessario, ed estremamente utile, applicare un approccio di tipo olistico che consenta di integrarli correttamente all'interno del *risk universe,* al fine di un loro trattamento coerente con le strategie di risk management dell'impresa.

Come introdotto nel paragrafo 2.3.2, il processo di adozione da parte delle imprese di una visione di sostenibilità di lungo periodo conduce necessariamente ad un processo di *business model innovation*. Tuttavia, nel momento in cui l'impresa si accinge a questo processo di profondo cambiamento, si trova nel doversi confrontare con un'ulteriore tipologia di rischi: i ***transition risks***. Questi sono solitamente "associati al passaggio a un'economia a basse emissioni di carbonio, compresi i cambiamenti politici, i progressi

[87] Society for Corporate Governance, BrownFlynn. (2018). *ESG Roadmap: Observations and Practical Advice for Boards, Corporate Secretaries and Governance Professionals.*

tecnologici e i mutamenti del mercato, che possono influire sul valore delle attività e sulla stabilità finanziaria delle istituzioni. (…) Possono richiedere una gestione proattiva e strategie di adattamento per mitigarne l'impatto."[88]

5.3 Applicazione Framework ERM ad Obiettivi ESG

Come precedentemente introdotto, la sostenibilità è un, se non il più importante, *driver* di cambiamento che sta spingendo le aziende ad innovare il proprio *business model*; processo che porta con sé la necessità di sviluppare nuove competenze e di ripensare il modo in cui l'operatività aziendale impatta l'ambiente in cui essa è inserita e le interdipendenze presenti. In questo contesto appare quindi imprescindibile l'integrazione delle tematiche ESG all'interno del sistema ERM, al fine di sviluppare un processo "*ESG-ready*" che costituisca una leva strategica a supporto del *management* per individuare ed orientare il processo decisionale attraverso gli impatti, rischi ed opportunità legati ai cambiamenti climatici e ad una crescente responsabilità sociale da parte delle imprese.

Lo sviluppo di processo ERM "*ESG-ready*" richiede **l'introduzione di numerosi cambiamenti** che impattano l'intero sistema aziendale, tra cui: una riorganizzazione dell'assetto di *governance*, un nuovo modo di approcciare al processo di creazione di valore, una ridefinizione della strategia aziendale, un l'adozione di un processo di *risk assessment* che valuti i rischi non solo in termini finanziari ma anche in relazioni agli impatti ambientali ed un processo di *reporting* delle informative aziendali che superi il semplice concetto di bilancio di esercizio, favorendo una comunicazione più ampia e trasparente verso gli *stakeholder*.

5.3.1 Governance e Sistemi di Controllo Interno

Lo sviluppo di un'organizzazione *ESG-ready* comporta l'integrazione all'interno della struttura di *governance* **di nuovi ruoli e funzioni aziendali**. All'interno del *board*, che riveste un ruolo di supervisione generale dell'operato societario, viene creato un **comitato ESG** chiamato a supportare il consiglio di amministrazione nelle responsabilità in ambito di gestione delle tematiche ESG e della loro rendicontazione. All'interno della struttura di governance viene poi istituita una nuova **funzione ESG**, a capo della quale viene posto

[88] Cardenas, V. (2024). *Financial climate risk: A review of recent advances and key challenges.* Institute for Resources, Environment and Sustainability, University of British Columbia (UBC).

un manager esecutivo – il **CSO** (*Chief Sustainability Officer*) –, con la responsabilità di implementare le strategie in ambito di sostenibilità elaborate dal board.

In questo contesto, al fine di **integrare** correttamente la funzione **ESG** quella **ERM** ed il resto delle operazioni aziendali, è importante strutturare sistemi e processi che permettano di comunicare ed operare in maniera coordinata e coerente. La stessa COSO sostiene che il "direttore della sostenibilità dovrebbe mantenere una stretta relazione con il direttore del ERM"[89] e strutturare linee di *reporting* dirette con il CFO, CSO e COO al fine di supportare l'operato delle funzioni a loro affidate in direzione degli obiettivi ESG.

In relazione al sistema di controlli interni il WBCSD e l'IIA[90], ridefiniscono le **responsabilità dei diversi livelli di presidii aziendali**. In particolare: al **primo livello** sono affidati i controlli riguardati tematiche e rischi ESG che possano influenzare le *operatons*, mentre al **secondo livello** sono affidate responsabilità di supporto al processo ERM riguardante rischi ESG (*compliance*, *assurance*…).

5.3.2 Multidimensionalità del Valore Aziendale e Definizione della Strategia

La capacità di creare, preservare o erodere valore da parte di un'azienda è determinata dal proprio **modello di *business***, ossia l'insieme di processi sviluppati dall'impresa e volti a trasformare gli *input* della produzione in *output*. In questo contesto, un efficace sistema ERM contribuisce a supportare il management nel proprio processo decisionale, permettendo di sviluppare una strategia in grado ottimizzare la propria capacità di creare e proteggere valore mediante un'analisi e valutazione sistematica ed integrata di tutti quei fattori, interni od esterni all'organizzazione, capaci di impedire il conseguimento della strategia.

Tuttavia, in ambito ESG una definizione di valore limitata al solo aspetto finanziario non è sufficiente per strutturare un processo ERM che sia in grado di analizzare in maniera approfondita la **multidimensionalità del valore** associato al concetto di sostenibilità. Per questo motivo l'IIRC (*international integrated reporting council*) ha sviluppato il concetto di ***multi-capital approach*** definito dalla stessa organizzazione come "la

[89] COSO, WBCSD. (2018). *Enterprise Risk Management: Applying enterprise risk management to environmental, social and governance-related risks.* COSO, WBCSD.
[90] WBCSD, IIA. (2022). *Embedding ESG and sustainability considerations into the Three Lines Model.* WBCSD.

considerazione attiva da parte di un'organizzazione delle relazioni tra le sue varie unità operative e funzionali e i capitali che l'organizzazione utilizza o influenza"[91]. La stessa IIRC ha sviluppato l'**<IR>** (*Integrated Reporting Framework*), un modello di *reporting* progettato per fornire alle organizzazioni uno standard comune per la redazione di rapporti che illustrino in maniera chiara la relazione che intercorre tra gli aspetti ESG ed il loro modello di business in un'ottica di creazione di valore di lungo periodo. Le due caratteristiche fondamentali del reporting integrato riguardano il ciclo di creazione di valore e la definizione dei diversi "capitali".

L'*integrated report* espande il concetto di **capitale aziendale**, definito in origine esclusivamente secondo un'accezione finanziaria, ed arriva a individuarne **6 tipologie** differenti:

- **Capitale finanziario**: l'insieme di disponibilità economiche che l'organizzazione può usare per la produzione e sono ottenute mediante finanziamenti o generate attraverso l'operatività aziendale
- **Capitale produttivo**: capitale fisico che l'impresa può usare per svolgere il proprio processo produttivo (es. edifici, macchinari, infrastrutture ecc.)
- **Capitale intellettuale**: beni immateriali corrispondenti al capitale organizzativo e al valore della conoscenza (es. proprietà intellettuale, know-how, sistemi, ecc.)
- **Capitale umano**: competenze, capacità ed esperienza del personale
- **Capitale sociale e relazionale**: istituzioni o relazioni tra i soggetti interni all'azienda, o tra l'azienda ed altre realtà, e la capacità di condividere informazioni
- **Capitale naturale**: tutti i processi e le risorse ambientali, rinnovabili e non rinnovabili, che forniscono beni o servizi per il successo passato, presente e futuro di un'organizzazione.

Il **ciclo di creazione del valore**, fa invece riferimento a quel processo dinamico attraverso il quale le organizzazioni convertono i capitali in ingresso mediante le attività trasformative definite nel proprio modello di *business* in *outcome,* generando così nuovo valore. Nello schema presentato dalla IIRC individuiamo **tre componenti** che influenzano questo processo: l'ambiente esterno, la *governance* ed il *business model*. Il primo componente, l'**ambiente esterno**, "include le condizioni economiche, i

[91] IIRC. (2021). *Il Framework <IR> Internazionale.* International Integrated Reporting Council.

cambiamenti tecnologici, le questioni sociali e le sfide ambientali e rappresenta il contesto in cui opera l'organizzazione". La **struttura di *governance***, predisposta dal management, supporta l'organizzazione nel proprio processo di creazione di valore. Il fulcro di questo modello, tuttavia, risiede nell'ultimo elemento: il ***business model***, il quale utilizzando i capitali in input li converte mediante le attività aziendali in output (prodotti, servizi, sottoprodotti e scarti).

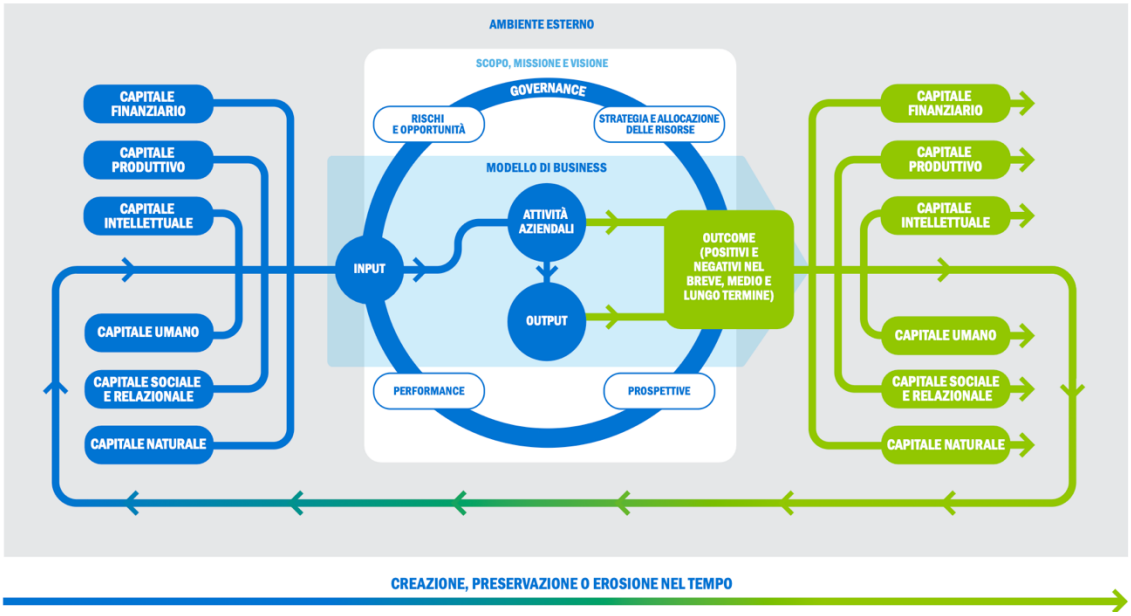

Figura 21. Ciclo di creazione del valore. Fonte: IIRC. (2021). Il framework <IR> Internazionale

5.3.3 Risk Assessment

Il **processo di *risk assessment*** viene profondamente influenzato dall'integrazione dei rischi ESG all'interno del sistema ERM, infatti, l'applicazione di questa nuova visione aziendale comporta la **modifica di diverse caratteristiche chiave** del processo. In primis, la funzione ERM è tenuta a **revisione della definizione dei rischi** precedentemente mappati, questo per far si che chi si occupi di effettuare le analisi richieste includa la prospettiva ESG al fine di favorire l'identificazione di rischi che in precedenza erano trascurati. Successivamente, risulta necessario condurre un **nuovo processo di identificazione** dei rischi in modo tale da poter sviluppare, attraverso la combinazione di un approccio *bottom-up* e *top-down*, un nuovo *risk inventory*. In seguito, è fondamentale definire **nuovi criteri di valutazione** dei rischi e selezionare metodologie di analisi e prioritizzazione che siano in grado di valutare la multidimensionalità introdotta nel sistema dall'adozione dell'approccio ESG. Infine, sarà necessario **ampliare la prospettiva temporale** presa in considerazione nel processo di analisi, infatti, mentre

i rischi strategici e operativi tendono a manifestarsi nel medio-breve periodo, i rischi ESG, data la loro natura strutturale e di lungo termine, possono manifestarsi e produrre i loro impatti in un orizzonte temporale più esteso.

5.3.4 Comunicazione e Reporting – IRO e Doppia Materialità

La **comunicazione ed il *reporting* dei rischi**, fase fondamentale di qualsiasi processo ERM, accresce di rilevanza nel momento in cui l'impresa adotta una prospettiva ESG. Mentre le modalità di comunicazione con soggetti interni all'impresa non subiscono importanti modifiche, la comunicazione ed il *reporting* dei rischi ESG sono oggetto di una serie di normative sia obbligatorie che volontarie. In questo contesto le **comunicazioni riguardanti i temi ESG**, contenute nel report di sostenibilità, diventano uno strumento di posizionamento strategico da parte dell'impresa, la quale mediante l'informativa condivisa al pubblico riesce a ottenere un sostanziale **vantaggio competitivo**. Questo dipende da **due differenti *driver***: **maggiore trasparenza e coinvolgimento degli stakeholder**, che comporta il miglioramento del dialogo con questi attori chiave, ottenimento di informazioni utili anche nel processo ERM e contribuisce a costruire fiducia; ed una **migliore gestione e monitoraggio degli impatti** dell'impresa, i quali consentono all'organizzazione di avere maggior consapevolezza delle tematiche ESG ed essere meglio posizionata nell'implementare misure di risposta ai rischi o di sfruttare le opportunità.

Come precedentemente introdotto, in ambito di *reporting* di sostenibilità sono diverse le norme elaborate, sia di natura obbligatoria che volontaria. Tra gli **standard di natura volontaria** possiamo individuare gli **standard GRI**, i quali forniscono indicazioni per la stesura del report di sostenibilità, individuano criteri per la definizione del concetto di materialità ed aiutano a integrare i rischi ESG nella gestione complessiva dei rischi, favorendo trasparenza e sostenibilità di lungo periodo. Altra normativa di carattere volontario è il sopracitato **<IR> *framework***, il quale elabora un sistema rendicontazione che integra il bilancio di esercizio ed il report di sostenibilità. Passando invece alle **normative di natura obbligatoria** l'ISSB (*international sustainability standards board*) nel 2023 ha approvato due standard volti a fornire una base omogenea a livello globale riguardo le informazioni di sostenibilità. Nello specifico: l'**IFRS S1**, stabilisce i requisiti generali per la divulgazione delle informazioni relative ai rischi e alle opportunità legati

alla sostenibilità, inclusi aspetti ambientali, sociali e di governance.; mentre l'**IFRS S2** si focalizza sull'informativa specifica ai cambiamenti climatici. L'Europa, invece, nel 2023 approva e adotta gli **ESRS** (*european sustainability reporting standards*), i quali costituiscono una base normativa volta a rendere coerente e maggiormente trasparente l'informativa legata alla sostenibilità.

Gli **ESRS** definiscono, quindi, le **informazioni che devono essere rendicontate** da parte delle aziende nel contesto della sostenibilità, queste possono essere suddivise in due macro-famiglie: **IRO** (impatti, rischi ed opportunità), ossia i processi mediante i quali le imprese identificano e valutano gli impatti, i rischi e le opportunità; e **metriche ed obiettivi**, ossia come l'impresa misura le performance, gli obiettivi in ambito ESG ed i progressi compiuti per raggiungerli.

Riguardo gli **IRO**, concetto di fondamentale importanza è quello della "**doppia materialità**" che rappresenta il criterio mediante il quale vengono individuate le informazioni oggetto di rendicontazione. La materialità, infatti, ha una doppia accezione: una prima, di **natura finanziaria**, secondo la quale un'informazione è considerata materiale se la sua omissione o errata presentazione può influenzare le decisioni economiche degli stakeholder interessati; ed una seconda, definita **materialità d'impatto** – standard GRI 101 e 3 –, che individua la soglia di impatto oltre la quale una questione risulta essere sufficientemente rilevante da essere inclusa nel report. Secondo il principio della doppia materialità, quindi, un'informazione diventa oggetto di rendicontazione se è contemporaneamente rilevante sia sotto un punto di vista finanziario che dell'impatto.

Per quanto riguarda le **metriche e gli obiettivi**, la normativa europea - **Regolamento Taxonomy** (2020/852/UE) e **Atto Delegato del 6 luglio 2021** – fornisce indicazioni uniformi al fine di coordinare le misure utilizzate dalle imprese in ambito di rendicontazione ESG. Come primi elementi vengono individuate le **definizioni di attività economica ammissibile ed allineata alla tassonomia** e successivamente le misure mediante le quali le imprese comunicano le loro performance in tali ambiti. L'Articolo 1 dell'atto delegato del 6 luglio 2021 definisce che un'attività economica è ammissibile alla tassonomia se questa à "identificata e descritta negli atti delegati"; mentre è considerabile come allineata un'attività economica che "oltre a risultare ammissibile, soddisfa i criteri di vaglio tecnico ad essa associati, non arreca danno a

nessuno degli altri obiettivi ambientali e rispetta le garanzie minime di salvaguardia sociale". Per quanto riguarda le misure per valutare le performance raggiunte dalle imprese, l'atto delegato, **individua 3 principali KPI** riguardanti: la **quota di fatturato** proveniente da prodotti o servizi associati ad attività economiche allineate, la **quota di spese in conto capitale** (CapEx) relativa ad attività economiche allineate e la **quota di spese operative** (OpEx) relativa ad attività economiche allineate.

6. Barometro: Applicazione ERM nelle Principali Aziende Quotate Italiane

Il presente capitolo costruisce e applica un *barometro di maturità dell'Enterprise Risk Management* per valutare in che misura le società quotate integrano il rischio nei processi decisionali (strategia, pianificazione/*budget*, allocazione del capitale) e come raccordano l'ERM con i fattori ESG. **L'approccio** utilizzato dall'analisi è di tipo compilativo, prende ad oggetto le principali aziende quotate su Euronext Milan ed è basato sullo studio della documentazione pubblica fornita dalle imprese interessate – in maniera preponderante la relazione annuale integrata – riguardante l'anno fiscale 2024.

Obiettivi e valutazione. L'obiettivo è stimare in maniera chiara e replicabile il grado di maturità dell'ERM, osservando sei dimensioni: (i) *Governance* dei rischi, (ii) *Risk Appetite*, (iii) *Portfolio View* e valutazione, (iv) Integrazione con pianificazione/capex, (v) ESG e doppia materialità, (vi) dati e *reporting*. Ciascuna dimensione è valutata su una scala 0–4 e contribuisce a un punteggio complessivo 0–100 tramite pesi predefiniti (Governance 20; Risk Appetite 20; Portfolio & Valutazione 20; Pianificazione/Capex 20; ESG & Doppia Materialità 15; Dati & Reporting 5). Il punteggio complessivo si ottiene sommando, per ciascuna dimensione, la quota pari a (punteggio/4 × peso). I risultati sono letti come: basso 0–39; intermedio 40–59; buono 60–79; avanzato 80–100.

Livello (0–4)	Descrizione sintetica
0 – Assente	Non ci sono riferimenti sostanziali a ruoli/processi di ERM, metriche o collegamenti ai processi aziendali.
1 – Dichiarativo	Sono presenti affermazioni o policy, ma senza evidenze operative (responsabilità, frequenze, soglie/limiti, metriche).
2 – Parziale	Processi descritti e qualche applicazione, ma non sistematica; esempi puntuali o copertura limitata di rischi/aree.
3 – Integrato/Operativo	Processi standardizzati con responsabilità chiare, collegamenti a piani/KPI/KRI e reporting periodico utilizzato dal management.
4 – Avanzato/Quantitativo	Evidenze robuste (soglie/limiti, scenari/stress test, indicatori tracciati) con impatti su budget/capex o riallocazioni/decisioni documentate.

6.1 UniCredit

A – Governance dei rischi e sostenibilità

- **Modello**: sistema **monistico** (CdA + Comitato per il Controllo sulla Gestione, CCG/Audit Committee).
- **Comitati CdA**: CCG; Comitato Rischi; Comitato Governance & Sostenibilità; Nomine; Remunerazioni; Parti Correlate.
- **Coordinamento**: CCG ↔ Comitato Rischi (scambio agende/*joint meeting*); CCG svolge anche funzioni OdV 231/2001.
- **Comitati manageriali**: GFRC (Financial & Credit Risk) e GNFRC (Non-Financial Risks & Controls, incl. ICT/Cyber/Third-party; Reputational). GEC – Risk session di coordinamento.

Lettura: governance formalizzata e coerente con un impianto RAF/ICAAP maturo; chiara attribuzione di ruoli e frequenze di *reporting*.

B – ERM

Componente	Evidenza/Prassi	Implicazione
Identificazione / Mappa rischi	Mappatura enterprise (finanziari e NFR)	Base per priorità e reporting integrato
Misurazione	Capitale economico (inter/intra-diversificazione), calcolo trimestrale	Allineamento con ICAAP e comitati
Stress test	Scenari almeno bi-annuali	Test di resilienza su capitale/liquidità
Risk Appetite	RAS qualitativo + Dashboard KPI (regolatori/manageriali/climate)	Propensione al rischio esplicitata
Budget / Remunerazione	RAF integrato nel budget; coerenza con policy retributiva	Steering rischio–rendimento e pay-for-risk
Monitoring e Reporting	RAF Monitoring & Integrated Risk – trimestrale	Escalation e azioni correttive

---

C – Principali rischi 2024 (cluster)

- **Macro/Geopolitici**: conflitti e contesto regolatorio.
- **Cyber/ICT & Terze Parti**: presidio in GNFRC; business continuity.
- **Finanziari**: credito, liquidità, tasso, mercato, sovrano;

- **Operativi**: condotta/compliance, frodi, processi, danni a beni;
- **Climatici & Ambientali**: rischio di transizione e fisico (KPI dedicati, integrazione IFRS9 e ICAAP).

D – ESG ed ERM

Tema	Come è trattato	Effetto su ERM
Doppia materialità / IRO	Processo integrato in governance e reporting	Collegamento IRO, rischi, KPI
KPI Net Zero	Settori prioritari (energia, *oil&gas*, auto) + estensioni *real estate*	Inclusi in Dashboard RAF con soglie
Integrazione nei processi	Impatti su *budget* e verifica RAF	*Escalation* e *remediation*
Controlli	Controlli interni su *reporting* sostenibilità	Qualità/consistenza dati

---

E – Valutazione

Dimensione	Punteggio	Nota
Governance e ruoli	**4**	Forte assetto CdA/CCG; coordinamento comitati; linee di difesa chiare
Risk Appetite	**4**	Integrazione in *budget*/remunerazione; *Dashboard* KPI ampia incl. *climate*
Portfolio view e valutazione	**3**	Capitale economico, stress test, reporting integrato; meno evidenze "*capex gating*"
Integrazione con pianificazione/capex	**3**	Chiaro su *budget*/*pay*; non emergono *gate capex* esemplificati
ESG e doppia materialità	**4**	KPI *climate* in RAF, IRO integrati, *target*/monitoraggi
Dati e reporting	**3**	*Reporting* regolare; controlli interni; *assurance* da verificare

Totale indicativo: **88.8/100**

6.2 Intesa San Paolo

A – Governance dei rischi e sostenibilità

- **Modello**: sistema **monistico** (CdA + Comitato per il Controllo sulla Gestione – CCG).

- **Comitati CdA**: Comitato Rischi e Sostenibilità (supporto a CdA su RAF/politiche di rischio); CCG con funzioni di controllo.
- **Linee di difesa**: sistema di controlli interni su tre livelli.
- **Comitati manageriali**: Comitato di Direzione (Sessione *Analisi Rischi di Gruppo*; esamina proposta RAF, pacchetti ICAAP/ILAAP, *Tableau de Bord* dei rischi); Comitato Rischi Finanziari di Gruppo (sessioni su rischi di mercato, banking book, liquidità e assicurativi).

Lettura: governance formalizzata; chiara ripartizione tra supervisione (CdA), controllo (CCG) e gestione (CEO), con comitati manageriali a supporto della vista portfolio dei rischi.

B – ERM

Componente	Evidenza/Prassi	Implicazione
Identificazione / Mappa rischi	Mappatura enterprise su famiglie finanziarie e non-finanziarie	Base per priorità e reporting integrato
Misurazione	Capitale interno / economico; ICAAP; *Tableau de Bord*	Allineamento capitale-rischio
Stress test	Analisi di scenario incl. climate/ESG	Test di resilienza su capitale/liquidità
Risk Appetite	RAS + KRI/Limiti (anche ESG/climate)	Propensione al rischio esplicitata
Pianificazione / Capitale	RAF e capital management indirizzano pianificazione e allocazione	Steering rischio–rendimento
Monitoring e Reporting	Comitato di Direzione/Comitato Rischi Finanziari di Gruppo; *Tableau de Bord*	Escalation e azioni correttive

---

C – Principali rischi 2024 (cluster)

- **Macro/Regolatori/Geopolitici**.
- **Finanziari**: credito, liquidità, tasso, mercato, sovrano; assicurativi.
- **Cyber/ICT & Terze Parti**: continuità operativa e rafforzamento difese.
- **Operativi**: condotta/compliance, frodi, processi, dati, outsourcing.
- **Climatici & Ambientali**: rischio di transizione e fisico (integrazione in RAF/ICAAP).

D – ESG ed ERM

Tema	Come è trattato	Effetto su ERM
Doppia materialità (ESRS)	Analisi strutturata, stakeholder engagement	Mappa IRO ↔ rischi ↔ KRI
KRI / Limiti ESG	Presidi nel RAF, per settori più esposti; collegati a strategie creditizie	Escalation e remediation
Scenario analysis	Climate scenario su portafogli/aree vulnerabili	Evidenze quantitative per ICAAP/RAF
Due diligence	Processi integrati in strategia e modello di business	Qualità dei presidi e priorità d'azione
Assurance	*Limited assurance* su rendicontazione di sostenibilità	Maggior affidabilità del reporting

E – Valutazione

Dimensione	Punteggio	Nota
Governance e ruoli	**4**	Modello monistico; CCG; comitato Rischi e Sostenibilità; 3 linee di controllo
Risk Appetite	**4**	RAS + KRI/Limiti incl. ESG/climate; ruolo nei comitati
Portfolio view e valutazione	**3**	Capitale interno, *Tableau de Bord*, stress test; meno evidenze di "capex gating"
Integrazione con pianificazione / capex	**3**	RAF e capital management indirizzano pianificazione/capitale
ESG e doppia materialità	**4**	Analisi ESRS-based, KRI/limiti, scenario analysis
Dati e reporting	**4**	3 linee di difesa; *limited assurance* sulla sostenibilità

Totale indicativo: **90/100**

6.3 ENEL

A – Governance dei rischi e sostenibilità

- **Modello**: sistema **tradizionale** (Consiglio di Amministrazione + Collegio Sindacale; società di revisione esterna).
- **Comitati CdA**: Comitato Controllo e Rischi (CCR); Comitato per la Corporate Governance e la Sostenibilità (CGS); Comitato Nomine e Remunerazioni (CNR); Comitato Parti Correlate.

- **Coordinamento**: sedute congiunte CCR ↔ Collegio Sindacale su SCIGR; flussi periodici su rischi, segnalazioni etiche, sostenibilità.
- **Controlli e assurance**: sistema di controllo interno su corporate reporting esteso alla sostenibilità (metodologia univoca; testing di Audit); assurance esterna sulla Rendicontazione di Sostenibilità (limited assurance).

Lettura: assetto formalizzato, linee di difesa chiare e presidio board-level su rischi e sostenibilità; frequenze e flussi indicano una governance matura.

B – ERM

Componente	Evidenza/Prassi	Implicazione
Identificazione / Risk catalogue	Tassonomia omogenea di Gruppo e mappatura enterprise, con vista per Linee di Business/Paesi	Base per priorità e reporting integrato
Valutazione	Matrici likelihood × impatto e vista dinamica tramite e-Risk Landscape©	Comparabilità e aggiornamento continuo
Modelli	Open Country Risk (quantitativo) e Cyber Value-at-Risk	Misura più robusta per rischi Paese e cyber
Risk Appetite	Risk Appetite Framework (RAF) con Risk Appetite Statement (indicatori/limiti per rischio)	Propensione formalizzata; limiti operativi
Comitati manageriali	Group Risk Committee (CEO-chaired, ~trimestrale) + comitati rischi locali	Allineamento top-down & bottom-up
Investimenti / Capex	Comitato Investimenti di Gruppo in matrice organizzativa	Presidio sui gate decisionali; integrazione potenziale
Monitoring e Reporting	Flussi regolari verso top management e organi sociali; controlli interni su reporting	Escalation e azioni correttive

---

C – Principali rischi 2024 (cluster)

- **Regolatori/Legali & Compliance**: forte concentrazione tra top risks (contenzioso fiscale, evoluzioni normative e regolatorie).
- **Strategici/Macroeconomici**: Paesi, geopolitica, mercati energia.
- **Digital/IT**: trasformazione digitale, CERT interno, metodologia Cyber VaR.
- **Operativi**: continuità del servizio, supply chain, sicurezza.

D – ESG ed ERM

Tema	Come è trattato	Effetto su ERM
Doppia materialità (IRO)	Processo aggiornato a CSRD/ESRS, catena del valore inclusa; CGS supervisiona	IRO → priorità e reporting rischi
Clima	Temi climatici discussi regolarmente in CdA/CCR/CGS; Piano di Sostenibilità	Integrazione dei rischi clima nei flussi decisionali
Incentivi	Obiettivi di sostenibilità nelle policy retributive (CEO & LTI)	Allineamento pay-for-sustainability
Controlli dati	SCIGR esteso alla sostenibilità con testing Audit e assurance esterna	Maggior affidabilità informativa

---

E – Valutazione

Dimensione	Punteggio	Nota
Governance e ruoli	**4**	Comitati attivi; sedute congiunte; linee di difesa chiare
Risk Appetite	**3**	RAF/RAS con limiti; integrazione implicita, casi d'uso da approfondire
Portfolio view e valutazione	**3**	Risk catalogue + e-Risk Landscape; modelli Paese/Cyber
Integrazione con pianificazione / capex	**3**	Comitato Investimenti; evidenze operative non dettagliate
ESG e doppia materialità	**4**	Oversight board-level; processo DM conforme ESRS; clima in agenda
Dati e reporting	**4**	SCIGR esteso a sostenibilità; testing Audit; limited assurance

Totale indicativo: **85/100**

6.4 Ferrari

A – Governance dei rischi & sostenibilità

- **Modello**: Board unico (N.V. olandese) con Comitato Audit, Comitato ESG, Comitato Remunerazioni; ruolo di indirizzo e supervisione del CdA.
- **Tre linee di controllo**: funzioni operative (1ª), funzioni di controllo/Compliance/ERM (2ª), Internal Audit (3ª).
- **Struttura manageriale**: Internal Audit, Risk & Compliance Department (dal 12/2023) che riporta al CEO; Internal Control Committee (trimestrale) guidato dal CFO; Ferrari Leadership Team (FLT) per coordinamento rischi.

- **Comitati ESG**: ESG Strategic Committee (a guida CFO), comitati operativi su Carbon Neutrality e Diversity & Inclusion.

Lettura: assetto di governance strutturato e integrato (CdA-Comitati-FLT) con chiara attribuzione di ruoli, frequenze di reporting e raccordo tra rischi finanziari, operativi ed ESG.

B – ERM

Componente	Evidenza/Prassi	Implicazione
Identificazione / Mappa rischi	Integrated Risk Assessment annuale e risk map presentata al Comitato Audit	Priorità e reporting strutturati
Misurazione	Valutazione con likelihood, impact, preparedness, velocity; KRI con frequenze differenziate	Vista comparabile dei rischi e trend
Risk Appetite	Risk Appetite Framework con categorie (Strategici, Operativi, Finanziari, Compliance, Reputazionali, HSE) e livelli di appetito	Confini e limiti espliciti per il management
Stress / Scenari	Scenario analysis climatica (fisico e transizione) su impianti e supply-chain	Test di resilienza e piani di mitigazione
Risk Response	Strategie Reduce/Avoid/Share/Accept con monitoraggio periodico	Azioni e escalation codificate
Monitoring e Reporting	Flussi informativi verso FLT, Internal Control Committee e Comitato Audit	Allineamento decisionale e tempestività

C – Principali rischi 2024 (cluster)

- **Strategici/di mercato**: evoluzione domanda lusso, posizionamento brand, concorrenza, M&A.
- **Operativi & Supply-chain**: qualità/prodotto, disponibilità materiali critici, business continuity, sicurezza sul lavoro.
- **Finanziari**: tasso/cambio, liquidità, commodity.
- **Compliance & Condotta**: regolazione auto, privacy, 231/anticorruzione, sanzioni.
- **Reputazionali**: tutela brand ed esclusività, canali/partner.
- **Climatici & Ambientali (HSE)**: fisici (alluvioni, grandine, siccità) e di transizione (normativa, percezione cliente, materiali critici).

D – ESG ed ERM

Tema	Come è trattato	Effetto su ERM
Doppia materialità (ESRS)	Processo annuale con approvazione Comitato Audit; integrazione delle IRO nel sistema ERM	Allineamento IRO ↔ rischi ↔ piani
Governance ESG	ESG Committee del CdA; ESG Strategic Committee (FLT, guida CFO)	Supervisione CdA e coordinamento manageriale
Clima	Scenario analysis impianti/supply-chain; due rischi di transizione materiali con piani di resilienza	Mitigazioni e priorità nella risk map
Target 2030	Carbon neutrality operativa; riduzioni Scope 3 per auto	KPI ambientali a supporto delle decisioni
Assurance	Limited assurance esterna su Sustainability Statement (ESRS)	Maggiore affidabilità dei dati/report

E – Valutazione

Dimensione	Punteggio	Nota
Governance e ruoli	**4**	Board-Comitati strutturati; 3 linee; dip. Risk & Compliance al CEO
Risk Appetite	**3**	RAF formale per categorie/limiti; uso trasversale, non esplicitato su budget/capex
Portfolio view e valutazione	**3**	Valutazioni omogenee (likelihood/impact/…); KRI; reporting a comitati
Integrazione con pianificazione / capex	**2**	Collegamento a decisioni e resilienza; non evidenziati "capex-gates" dedicati
ESG e doppia materialità	**4**	DM integrata in ERM; governance ESG; scenari e target 2030
Dati e reporting	**4**	Flussi strutturati a FLT/Comitati; limited assurance ESRS

Totale indicativo: **80.0/100**

6.5 Generali

A – Governance dei rischi e sostenibilità

- **Modello**: **tradizionale** italiano (Assemblea, Consiglio di Amministrazione, Collegio Sindacale).
- **Comitati CdA**: Comitato Controllo e Rischi; Comitato Nomine e Corporate Governance; Comitato Innovazione e Sostenibilità Sociale e Ambientale.

- **Organi manageriali**: Group Management Committee (coordinamento esecutivo).

Lettura: governance allineata alle migliori prassi e al quadro Solvency II; responsabilità e flussi decisionali formalizzati.

B – ERM

Componente	Evidenza/Prassi	Implicazione
Identificazione / Profilo di rischio	Processo enterprise su rischi assicurativi, finanziari, di credito, operativi	Base per priorità e reporting integrato
Misurazione	SCR/GOF (Solvency II) e sensitività su tassi, spread, equity	Vista portfolio rischio-capitale
Stress test / Scenari	Analisi climatica annuale con metodologia proprietaria *Clim@risk* su investimenti e portafogli assicurativi	Resilienza prospettica e input a strategia di rischio
Risk Appetite	RAF di Gruppo con operating target range su solvibilità e monitoraggio periodico	Propensione al rischio esplicitata e monitorata
Pianificazione	ORSA collegato a Piano Strategico e Group Capital Management Plan	Allineamento risk-planning e allocazione capitale
Monitoring e Reporting	Report ricorrenti su solvibilità e profilo di rischio; disclosure regolatoria (es. SFCR)	Escalation e azioni correttive

---

C – Principali rischi 2024 (cluster)

- **Finanziari & di Credito**: quota prevalente del profilo (pre-diversificazione) legata a mercato, tassi, spread.
- **Sottoscrizione**: Vita e Danni su rischi tariffari/tecnici; sensitività a riscatti e sinistri estremi.
- **Operativi**: processi, compliance/condotta, IT.
- **Liquidità**: presidi e piano di gestione dedicato.
- **Climatici**: rischio fisico (eventi naturali) e transizione; valutati anche effetti di contenzioso.

D – ESG ed ERM

Tema	Come è trattato	Effetto su ERM
Doppia materialità (ESRS)	Rendicontazione 2024 conforme ESRS; attestatezza CEO/CFO e assurance limitata del revisore	Qualità informativa e tracciabilità IRO
Clima	Scenari Net-Zero/Delayed/Fragmented; rischio fisico via modelli climatici regionali	Integrazione in ORSA e strategia di rischio
Biodiversità e natura	Valutazioni in ottica TNFD sul portafoglio investimenti	Individuazione esposizioni settoriali rilevanti
Governance ESG	Comitato consiliare dedicato a innovazione e sostenibilità	Collegamento top-down con processi di rischio

---

E – Valutazione

Dimensione	Punteggio	Nota
Governance e ruoli	**4**	Modello tradizionale con comitati dedicati; responsabilità chiare
Risk Appetite	**4**	RAF di Gruppo, target range su solvibilità, monitoraggi periodici
Portfolio view e valutazione	**4**	SCR/GOF, sensibilità multi-fattore, scenari climatici
Integrazione con pianificazione / capex	**3**	Forte su ORSA ↔ Piano/Capital; capex-gating non pertinente
ESG e doppia materialità	**3**	ESRS, scenari clima integrati; target/limiti operativi da esplicitare
Dati e reporting	**4**	Reporting ricorrente e assurance sulla sostenibilità

Totale indicativo: **91,3/100**

6.6 Riepilogo dei Risultati

Il barometro è stato applicato a cinque casi riferiti all'esercizio 2024 (UniCredit, Intesa Sanpaolo, Enel, Ferrari, Generali). Nel complesso emerge un livello di **maturità ERM elevato** (media intorno a 87/100), trainato da assetti di *governance* solidi, da una buona qualità informativa e da un'integrazione ESG ormai stabilizzata nei documenti pubblici. La coerenza dei presidi a livello di consiglio e comitati, l'adozione delle tre linee di controllo e la cadenza dei flussi di *reporting* costituiscono un tratto comune dell'intero campione.

Sul piano della **propensione al rischio (*Risk Appetite*)**, i risultati sono particolarmente robusti nei settori regolati. Banche e assicurazioni presentano *framework* completi, con *statement*, limiti e indicatori diffusi e un chiaro raccordo con i processi di budget, capitale e remunerazione; negli emittenti industriali lo *statement* è presente e strutturato, ma la traduzione operativa dei limiti risulta meno pervasiva. La ***portfolio view*** dei rischi è buona in tutti i casi, con l'assicurativo che eccelle per profondità di misure; negli altri settori la vista aggregata esiste, ma il suo uso decisionale è meno esplicito.

L'**integrazione ESG** ha compiuto un salto di qualità grazie all'adozione della doppia materialità (ESRS/CSRD), all'inclusione di KPI climatici e alle analisi di scenario: elementi che vengono progressivamente inglobati nei *framework* di rischio e nel processo di pianificazione. Rimane tuttavia eterogenea la **traduzione in limiti operativi** e in ***trigger*** gestionali, soprattutto al di fuori dei settori regolati. In parallelo, **dati e *reporting*** mostrano un consolidamento: la *limited assurance* sulle *disclosure* di sostenibilità è ormai prassi diffusa e i sistemi di controllo interno sono estesi alle metriche non finanziarie, con benefici sulla qualità delle informazioni.

Nel complesso, il barometro suggerisce che la **maturità ERM** del campione è **alta** e sufficientemente omogenea nelle dimensioni di governance, ESG e dati. La **priorità** per una fase successiva è rendere più tracciabile l'impatto del profilo di rischio sulle **scelte allocative** (CapEx, portafoglio iniziative), introducendo soglie, *trigger* e responsabilità chiare.

7. Conclusione

Il presente elaborato ha ricostruito in modo organico i principali contributi dottrinali e professionali sull'Enterprise Risk Management, mostrando come, in un contesto segnato da incertezza strutturale, il rischio debba essere trattato come informazione per decidere e non come semplice anomalia da eliminare. Dalla letteratura emerge una convergenza sostanziale: sia il *framework* COSO ERM 2017 sia la norma ISO 31000:2018 concepiscono l'ERM come architettura organizzativa che allinea strategia, obiettivi e *performance*.

Il contributo dell'elaborato, di natura compilativa, è duplice. Primo: mettere ordine nel lessico e nei concetti, evidenziando complementarità e differenze tra i riferimenti

internazionali e mostrando come tradurli in pratiche coerenti. Secondo: sistematizzare le evidenze su come i temi ESG entrino nel perimetro ERM attraverso la doppia materialità, fungendo da ponte tra impatti e rilevanza finanziaria: gli *issue* materialmente rilevanti alimentano la mappa dei rischi, informano *risk appetite* e KPI, e trovano coerenza nel *reporting*.

Coerentemente con l'impianto ricostruito, Stewart individua l'essenza dell'ERM: "Il rischio (...) è una cosa buona. Lo scopo del *risk management* non è eliminarlo, così si eliminerebbe anche il rendimento. Il punto è gestirlo: cioè scegliere dove puntare e dove evitare del tutto di scommettere. La gestione della *performance* e la gestione del rischio sono due facce della stessa medaglia"[92].

In definitiva, un ERM realmente integrato non è un costo di conformità né un esercizio di *reporting*: è architettura organizzativa che allinea strategia, rischio e performance, abilita resilienza e guida l'innovazione sostenibile del modello di *business*. La sua efficacia è funzione non soltanto della sofisticazione degli strumenti, bensì, in misura preponderante, della coerenza tra *governance*, dati, cultura aziendale e competenze. È su questa coerenza, e sulla capacità di trasformare l'informazione di rischio in decisioni migliori, che si gioca la competitività delle imprese nel medio-lungo periodo.

[92] Stewart, T. A. (2000, February 7). Managing Risk in the 21st Century. *Fortune*, 202.

Bibliografia:

A2A. (2025, Gennaio 23). *A2A, primo european Green Bond collocato sul mercato.* Tratto da A2A: https://www.gruppoa2a.it/it/media/comunicati-stampa/a2a-primo-european-green-bond-mercato

Abnett, K., & Payne, J. (2025, 02 26). *Europe plans to ease sustainability reporting rules to compete globally*. Tratto da Reuters: https://www.reuters.com/world/europe/eu-set-propose-sweeping-red-tape-cuts-boost-business-competitiveness-2025-02-26/

Accardi, F. (2024). *Governo e Controllo dei Rischi, manuale per scelte consapevoli e sostenibili.* Franco Angeli.

AccountAbility. (2015). *AA1000 Stakeholder Engagement Standard (2015).* AccountAbility.

Acebes, F., Gonzáles-Verona, J. M., Lopez-Paredes, A., & Pajares, J. (2024). Beyond probability-impact matrices in project risk management: A quantitative methodology for risk prioritisation. *Humanities and Social Sciences Communications*.

Adler, R. M. (2020). *Bending the Law of Unintended Consequences: A Test-Drive Method for Critical Decision-Making in Organizations.* Cham: Springer.

Adler, R. M. (2020, Gennaio 7). *How to Manage Portfolios of Enterprise Risks*. Tratto da Medium: https://medium.com/@rich_77042/how-to-manage-portfolios-of-enterprise-risks-5e11c864c532

Anton, S. G., & Afloarei Nucu, A. E. (2020). Enterprise Risk Management: A Literature Review and Agenda for Future Research. *Journal of Risk and Financial Management, 13*, p. 281.

Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. *Accounting, Organization and Society, 35*, 659-675.

Assicurazioni Generali S.p.A. (2025). *Relazione annuale integrata e bilancio consolidato 2024.*

Atkova, I., Galkina, T., Yang, M., Leposky, T., & Ahokangas, P. (2025). Opening the black box of transition towards a sustainable business model. *Long Range Planning*.

Auguer, M., & Teece, D. J. (2018). *The Palgrave Encyclopedia of Strategic Management.* Palgrave Macmillan.

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 1-13.

Bailey, C. (2022). The Relationship Between Chief Risk Officer Expertise, ERM Quality, and Firm Performance. *Journal of Accounting, Auditing & Finance*, 205-228.

Beasley, M. S., & Branson, B. C. (2024). *The State of Risk Oversight: An Overview of Enterprise Risk Management Practices.* Raleigh: NC State University, AICPA, CIMA.

Bellini, M. (2025, Gennaio 7). *ESG: tutto quello che c'è da sapere per orientarsi su Environmental, Social, Governance*. Tratto da ESG360: https://www.esg360.it/environmental/esg-tutto-quello-che-ce-da-sapere-per-orientarsi-su-environmental-social-governance/#

Bezis, J. N. (2014). *Integrating Portfolio Risk Management into the ERM Framework.* Social Science Research Network.

Bocken, N. M., Short, S. W., Rana, P., & Evans, S. (2014). A literature and practice review to develop sustainable business model archetypes. *Journal of Cleaner Production*, 42-56.

Borgia, M. (2024). *L'Enterprise Risk Management nell'Opinione dei Professionisti della Gestione dei Rischi Aziendali.* Caucci Editore – Bari.

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise Risk Management: Review, Critique, and Research Directions. *Long Range Planning, 48*, 265-276.

Buendia Giribaldi, A. R., Rojas Quispe, M. A., Tosso Pineda, L. H., Silva Sánchez, O., Bravo Rojas, L. M., & Espinoza Santos, M. G. (2021). Methodology of the Deming cycle as a management process for business competitiveness. *Journal of Scientific and Technological Research Industrial, 2*, p. 8-10.

Cardenas, V. (2024). *Financial climate risk: A review of recent advances and key challenges.* Institute for Resources, Environment and Sustainability, University of British Columbia (UBC).

Clarckson, M. B. (1995). A Stakeholder Framework for Analyzing and Evaluating Corporate Social Performance. *Academy of Management Review, 20*, 92–117.

Comitato per la Corporate Governance. (2020). Codice di Corporate Governance.

COSO. (2004). *Enterprise risk management: Integrated Framework.* COSO.

COSO. (2017). *Enterprise Risk Management: Integrating with Strategy and Performance.* COSO.

COSO. (2017). *Enterprise Risk Management: Integrating with Strategy and Performance - Executuve Summary.* COSO.

COSO. (2017). *Enterprise Risk Management: Integrating with Strategy and Performance – Appendices.* COSO.

COSO, WBCSD. (2018). *Enterprise Risk Management: Applying enterprise risk management to environmental, social and governance-related risks.* COSO, WBCSD.

CSR Manager Network. (2019). *Sostenibilità ed Enterprise Risk Management (ERM).* CSR Manager Network Italia.

Damayanti, E. S. (2023). Risk Management: In an Overview of Literature Review. *Formosa Journal of Science and Technology (FJST), 2*, 1115–1122.

De Nicola, A. (2018). *Il Diritto dei Controlli Societari.* Giappichelli.

Di Carlo, E. (2017). *Interesse primario dell'azienda come principio guida e bene comune.* Giappichelli.

Dittmeier, C. A. (2007). *Internal Auditing. Chiave per la Corporate Governance.* Egea.

Draghi, M. (2024). *The future of European competitiveness.* European Commission.

Driessen, M. (2024, 09 26). *The Draghi Report: a reality check for ESG regulation in the EU*. Tratto da Stibbe: https://www.stibbe.com/publications-and-insights/the-draghi-report-a-reality-check-for-esg-regulation-in-the-eu

Elkington, J. (1994). Towards the Sustainable Corporation: Win-Win-Win Business Strategies for Sustainable Development. *California Management Review, 36*, p. 90-100.

Enel S.p.A. (2025). *Relazione finanziaria annuale consolidata 2024.*

ESG Post. (2024, 9 9). *EU's ESG rules face criticism from European businesses*. Tratto da ESG Post: https://esgpost.com/eus-esg-rules-face-criticism-from-european-businesses/

Euronext Milano. (s.d.). *Euronext Milan*. Tratto da Borsa Italiana: https://www.borsaitaliana.it/azioni/mercati/euronext-milan/home/caratteristiche.htm
European Commission. (2019). The European Green Deal.
European Commission. (s.d.). *The Draghi Report on EU Competitiveness*. Tratto da European Commission: https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en
Evrin, V. (2021). Risk Assessment and Analysis Methods: Qualitative and Quantitative. *ISACA Journal*.
Ewertowski, T., Berlik, M., & Sławinska, M. (2024). The Effectiveness of Operational Residual Risk Assessment: The Case of General Aviation Organizations in Enhancing Flight Safety in Alignment with Sustainability. *Sustainability*.
Ferrari N.V. (2025). *2024 Annual Report and Form 20-F.*
Fink, L. (2018). *Larry Fink's 2018 Letter to CEOs: A sense of Purpose.* Tratto da BlackRock: https://www.blackrock.com/corporate/investor-relations/2018-larry-fink-ceo-letter
Floreani, A. (2004). *La valutazione dei rischi e le decisioni di risk management.* Milano: EDUCatt – ISU Università Cattolica.
Floreani, A. (2005). *Introduzione al risk management. Un approccio integrato alla gestione dei rischi aziendali.* Milano: Etas.
Fraser, J., Schoening-Thiessen, K., & Simkins, B. (2010). Who reads what most often?: A survey of enterprise risk management literature. In J. Fraser, & B. Simkins, *Enterprise risk management: Today's leading research and best practices for tomorrow's executives* (p. 399-401). John Wiley & Sons.
Freeman, E. R. (1984). *Strategic Management: A Stakeholder Approach.* Boston: Pitman.
Frigo, M. L. (2008). When Strategy and ERM Meet. *Strategic Finance*, 45-49.
Frigo, M. L., & Anderson, R. J. (2011). Strategic Risk Management: A Foundation for Improving Enterprise Risk Management and Governance. *The Hournal of Corporate Accounting & Finance*, 81-88.
Goldenberg, O., & Wiley, J. (2011). Quality, conformity, and conflict: Questioning the assumptions of Osborn's brainstorming technique. *The Journal of Problem Solving, 3*(2), 96-108.
GRI. (2024). *Serie Consolidata di Standard GRI.* GRI.
Haier. (s.d.). *Washpass by Haier*. Tratto da Haier: https://subscriptions.haier-europe.com/it_IT/washpass/
Hill, T., & Westbrook, R. (1997). SWOT analysis: It's time for a product recall. *Long Range Planning, 30*, 46-52.
Hillson, D. (1999). Developing Effective Risk Responses. *Proceedings of the 30th Annual Project Management Institute Seminars & Symposium.* Philadelphia: Project Management Institute.
Hillson, D. (2016). *The Risk management Handbook.* Kogan Page.
IIRC. (2021). *Il Framework <IR> Internazionale.* International Integrated Reporting Council.
IMA. (2019). *Enterprise Risk Management: Frameworks, Elements, and Integration.* Institute of Management Accountants.
Intesa Sanpaolo S.p.A. (2025). *Relazione e bilancio consolidato del Gruppo Intesa Sanpaolo dell'esercizio 2024.*

IRM. (2012). *Risk Culture: Resources for practitioners.* London: Institute of Risk Management.
ISO. (2018). ISO 31000:2018 Risk Management - Guidelines.
ISO. (2022). *ISO 31073:2022 Risk management - Vocabulary.* ISO.
ISO. (s.d.). *Standards catalogue*. Tratto da ISO: https://www.iso.org/standards-catalogue/browse-by-tc.html
ISO, IEC. (2019). ISO/IEC 31010:2019 Risk Management - Risk Assessment Techniques.
Kantar. (s.d.). *Who Cares? Who Does? Sustainability*. Tratto da Kantar: https://www.kantar.com/campaigns/who-cares-who-does-in-the-fmcg-industry
KPMG. (2022). *Me, my life, my wallet.* KPMG.
KPMG. (2023). *ERM's role in ESG: How Enterprise Risk Management can help companies craft and execute ESG strategies.* KPMG.
Liebenberg, A. P., & Hoyt, R. E. (2003). The Determinants of Enterprise Risk Management: Evidence From the Appointment of Chief Risk Officers. *Risk Management and Insurance Review*, 37-52.
List of ISO standards. (s.d.). Tratto da Wikipedia: https://en.wikipedia.org/wiki/List_of_ISO_standards
Martens, F., & Rittenberg, L. (2020). *Risk Appetite Critical to Success: Using Risk Appetite to Thrive in a Changing World.* COSO.
Mazzola, P. (2013). *Il Piano Industriale: Progettare e Comunicare le Strategie di Impresa.* Egea.
Micán, C., Fernandes, G., & Araújo, M. T. (2020). Project portfolio risk management: A structured literature review with future directions for research. *International Journal of Information Systems and Project Management, 8*(3), 67-84.
Mishra, B. K., Rolland, E., Satpathy, A., & Moore, M. (2019). A framework for enterprise risk identification and management: the resource-based view. *Managerial Auditing Journal*.
Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts. *Academy of Management Review, 22*(4), 853-886.
MSCI. (2024). *ESG Ratings Methodology.* MSCI ESG Research LLC.
Naik, S., & Prasad, C. (2021). Benefits of Enterprise Risk Management: A Systematic Review of Literature. *Journal of Finance and Banking Review, 5*, p. 28-35.
ONU. (2015). *Trasformare il Nostro Mondo: L'Agenda 2030 per lo Sviluppo Sostenibile.* Assemblea Generale - Organizzazione delle Nazioni Unite.
ONU. (s.d.). *Agenda 2030*. Tratto da Nazioni Unite: https://unric.org/it/agenda-2030/
Parsaei Motamed, M., & Bamdad, S. (2022). A multi-objective optimization approach for selecting risk response actions: considering environmental and secondary risks. *Operational Research Society of India, 59*, 266-303.
Pfeffer, J. (1981). *Power in Organizations.* Pitman Publishing.
Pierce, E. M., & Goldstein, J. (2018). ERM and strategic planning: a change in paradigm. *Springer Nature*, 51-59.
Pierce, E., & Goldstein, J. (2016). Moving from enterprise risk management to strategic risk management: Examining the revised COSO ERM framework. Research Gate.

Polchar, J., & Santamaria, N. A. (2024). Mapping Emerging Critical Risks. *Working Papers on Public Governance No. 78.* OECD (Organization for Economic Co-operation and Development).
Porter, M. E. (1980). *Competitive strategy: Techniques for analyzing industries and competitors.* New York: Free Press.
Porter, M. E. (2008). The five competitive forces that shape strategy. *Harvard Business Review, 86*, 78-95.
Power, M. (2007). *Organized uncertainty: designig a world of risk management.* Oxford University Press.
Projects, P. (2025, April 5). *The Deming Cycle For Risk Management: Applying ISO Standards to Improve Project Risk Control*. Tratto da PL Projects: https://plprojects.co.uk/deming-cycle-risk-management-iso-standards
Rowe, G., & Wright, G. (2011). The Delphi technique: Past, present, and future prospects. *Technological Forecasting and Social Change, 78*(9), 1487-1490.
Ruggerio, C. A. (2021). Sustainability and Sustainable Development: A Review of Principles and Definitions. *Science of the Total Environment*.
Sackmann, S. A. (2022). *Culture in Organizations: Development, Impact and Culture-Mindful Leadership.* Springer International Publishing.
Shrivastava, V. K., Balasubramanian, J., Katyal, A., Yadav, A., & Yogananthan, S. (2024). Understanding the significance of risk management in enterprise management dynamics. *Multidisciplinary Reviews*.
Silvestri, R., & Kamerling, J. (2024). *CFA Institute Survey Report on the ESG Regulatory Framework in the EU.* CFA Institute.
Slaper, T. F., & Hall, T. J. (2011). The Triple Bottom Line: What is it and how does it work? *Indiana Business Review*, p. 4-8.
Society for Corporate Governance, BrownFlynn. (2018). *ESG Roadmap: Observations and Practical Advice for Boards, Corporate Secretaries and Governance Professionals.*
Stewart, T. A. (2000, February 7). Managing Risk in the 21st Century. *Fortune*, 202.
Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review, 20*(3), 571–610.
Taleb, N. N. (2007). *The Black Swan: The Impact of the Highly Improbable.* New York: Random House.
Taleb, N. N. (2012). *Antifragile: Things That Gain from Disorder.* New York: Random House.
The Institute of Directors in Southern Africa. (2016). *King IV Report of Corporate Governance for South Africa 2016.* The Institute of Directors in Southern Africa.
Treccani. (s.d.). *Rischio*. Tratto da Enciclopedia on-line Treccani: https://www.treccani.it/enciclopedia/rischio/
UniCredit S.p.A. (2025). *Bilanci e Relazioni 2024.*
Vicente, V. (2024, February 15). *Risk Assessment Matrix: Overview and Guide*. Tratto da AuditBoard: https://auditboard.com/blog/what-is-a-risk-assessment-matrix
von Känel, J., Cope, E. W., Deleris, L. A., Nayak, N., & Torok, R. G. (2010). Three Key Enablers to Successful Enterprise Risk Management. *IBM Journal of Research and Development, 54*(3), p. 1-15.
WBCSD, IIA. (2022). *Embedding ESG and sustainability considerations into the Three Lines Model.* WBCSD.
WEF. (2015). *Global Risk Report 2015.* World Economic Forum.

WEF. (2022). *Risk Proof: A Framework for Building Organizational Resilience in an Uncertain Future.* World Economic Forum.
WEF. (2025). *Chief Economists Outlook – May 2025.* World Economic Forum.
WEF. (2025). *Global Risks Report 2025.* World Economic Forum.
WEF, McKinsey. (2022). *Resilience for Sustainable, Inclusive Growth - White Paper.* World Economic Forum.
What are risk categories? (Types and Ways to determine them). (s.d.). Tratto da Metricstream: https://www.metricstream.com/learn/what-are-risk-categories.html#section-1
Wilde, O. (2003). *Aforismi e Massime.* Milano: Mondadori.
Wolters Kluwer. (2022, February 22). *Apply PDCA approach to forumulize ORM or EHS management*. Tratto da Wolters Kluwer: https://www.wolterskluwer.com/en/expert-insights/apply-pdca-approach-to-formulize-orm-or-ehs-management
YouGov. (2024). *Who Cares? Who Does? Sustainability Report - 6th Edition.* YouGov.