RISK MANAGEMENT

Approfondimento

Gruppo TIM

Giugno 2025

INDICE

1. Il nostro modello di Risk Management 3
2. Il processo di Risk Management 5
3. Approccio quantitative alla valutazione del rischio 7
4. Gestione integrata del rischio: il ruolo del Risk Appetite Framework 8
5. Mappatura, classificazione e prioritizzazione of risks 11
6. Analisi e gestione dei rischi più rilevanti 14
7. Riconoscimento e gestione dei rischi emergenti 16

1. Il nostro modello di Risk Management

Nel Gruppo TIM adottiamo un modello strutturato di Enterprise Risk Management (ERM), ispirato agli standard internazionali ISO 31000:2018 e al COSO Framework, con l'obiettivo di identificare, valutare, gestire e monitorare in modo sistematico i rischi aziendali.
Promuoviamo una cultura del rischio diffusa a tutti i livelli dell'organizzazione, e il nostro approccio si basa su alcuni principi fondamentali:

- **allineamento con strategia e obiettivi**: teniamo conto del contesto interno ed esterno in cui operiamo, integrando il processo ERM nella strategia aziendale per supportare il raggiungimento degli obiettivi principali, anche in termini economico-finanziari;
- **integrazione e collaborazione:** consideriamo il processo ERM parte integrante delle nostre attività quotidiane e favoriamo la cooperazione tra le diverse funzioni, mettendo insieme competenze tecniche e di business;
- **dinamicità e adattabilità** : siamo consapevoli che i rischi cambiano nel tempo. Per questo monitoriamo costantemente l'evoluzione dei fattori di rischio e interveniamo con azioni di mitigazione quando necessario.
- **approccio analitico:** dove possibile, il processo ERM utilizza metodi di valutazione quantitativa, basandoci su impatto e probabilità di accadimento.
- **visione complessiva:** non analizziamo i rischi solo singolarmente, ma anche come insieme di elementi correlati, per avere una visione più completa
- **miglioramento continuo**: aggiorniamo e rivediamo regolarmente il processo ERM, per mantenerlo efficace e allineato alle best practice.

Il processo ERM è gestito in modo continuativo, ha carattere ciclico ed è pervasivo nell'organizzazione, poiché coinvolge tutte le funzioni aziendali ed i principali stakeholder.

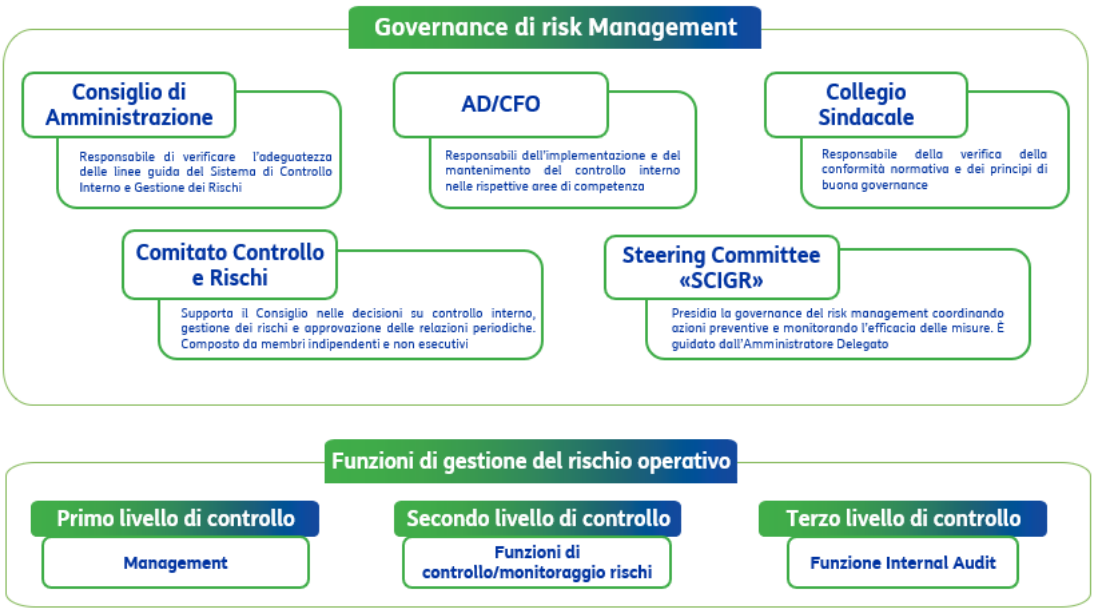
Il Sistema di Gestione dei Richi adottato in TIM si fonda su un solido **sistema di governance**, in cui il **Consiglio di Amministrazione**, il **Comitato Controllo e Rischi** e il **Collegio Sindacale,** ne assicurano l'adeguatezza, vigilano sulla conformità normativa e verificano l'allineamento con i principi di buona governance.

A supporto della governance, agisce il modello delle “**tre linee di difesa**” (ovvero tre linee di responsabilità di gestione e controllo):

- la **prima linea**, rappresentata dal **management**, identifica, valuta e gestisce i rischi nell’ambito delle attività operative;
- la **seconda linea**, costituita dalle **funzioni di controllo e monitoraggio**, supervisiona il processo di gestione, definisce metodologie e verifica l’applicazione delle misure di mitigazione;
- la **terza linea**, infine, è affidata alla **Direzione Internal Audit**, che svolge un’attività indipendente di verifica dell’efficacia dell’intero sistema, riferendo direttamente agli organi di governo.

L’Amministratore Delegato, supportato dal Chief Financial Officer e dallo Steering Committee SCIGR (Sistema di Controllo Interno e di Gestione dei Rischi), coordina l’attuazione operativa del modello di gestione dei rischi a livello di Gruppo.

Questa modello di governance integrato, sintetizzato di seguito, assicura un presidio costante e trasversale dei rischi aziendali, a beneficio della solidità e della continuità operativa dell’azienda



Inoltre, per diffondere una cultura consapevole del rischio all'interno dell'Azienda, adottiamo una serie di iniziative specifiche, tra cui:

- attività regolare di allineamento e informazione del Consiglio di Amministrazione sulla gestione dei rischi e sulle iniziative avviate per la loro mitigazione e il loro monitoraggio;
- corsi di formazione specialistici sul risk management, su base annuale, pensato per rafforzare una visione integrata del rischio lungo la filiera produttiva e offrire un aggiornamento continuo sull'evoluzione dell'argomento e delle applicazioni in azienda
- incontri periodici con relatori esperti della materia con l'obiettivo di ampliare le conoscenze in materia di risk management;
- integrazione dei criteri di rischio nei processi di sviluppo di prodotti e servizi;
- allineamento delle politiche retributive agli obiettivi di gestione del rischio, attraverso metriche legate ai rischi rilevanti per il Gruppo – inclusi quelli di sostenibilità, come la soddisfazione del cliente, il coinvolgimento dei giovani dipendenti e il gender pay gap – applicate nel sistema di incentivazione variabile (MBO e LTI).

2. Il processo di Risk Management

Nel Gruppo TIM, il processo di Enterprise Risk Management (ERM) è strutturato in un ciclo continuo e integrato, pensato per garantire una gestione efficace e proattiva dei rischi aziendali. Il processo si articola in quattro fasi principali, affiancate dalla promozione trasversale di una solida cultura del rischio.

1. Analisi di contesto, identificazione e assessment: analizziamo il contesto aziendale in relazione agli obiettivi strategici, identificando i principali rischi potenziali attraverso strumenti come il Risk Register, le Heat Map e modelli quantitativi utili a valutarne impatto e probabilità. Per comprenderli e gestirli in modo efficace, applichiamo un approccio integrato che ci consente di scomporre il Piano Strategico nei suoi elementi chiave, evidenziandone la volatilità e le aree critiche. Questo collegamento diretto tra strategia e rischio ci permette di assicurare un controllo rigoroso e dinamico, grazie ad aggiornamenti periodici e a un flusso continuo di feedback da parte delle Business Unit e della funzione di Pianificazione e Controllo.

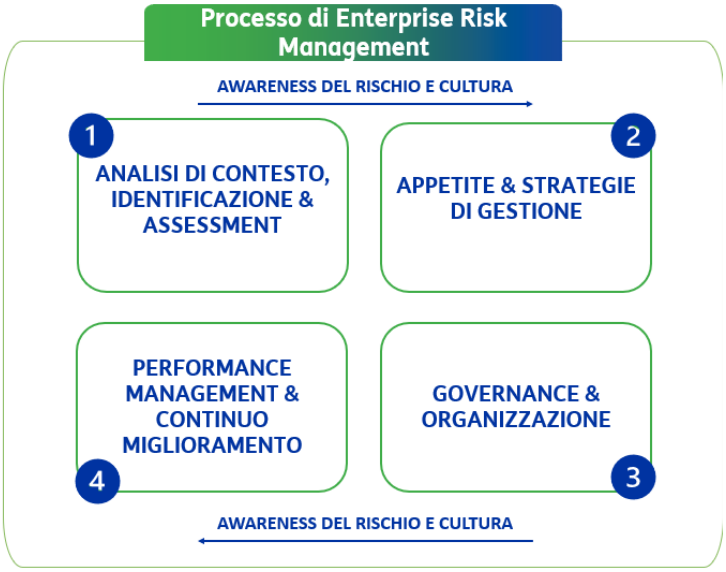
2. Risk Appetite e strategie di gestione: valutiamo il profilo complessivo dei rischi mappati insieme ai Risk Owner di competenza, definendo soglie di tolleranza (Risk Appetite e Tolerance), strategie di trattamento (ad esempio mitigazione o trasferimento), responsabilità e piani d'azione. Questa fase è fondamentale per trasformare la consapevolezza del rischio in una strategia operativa. A supporto della definizione del Risk Appetite e delle strategie di gestione, utilizziamo modelli quantitativi avanzati per analizzare scenari di rischio e correlazioni tra eventi, con l'obiettivo di stimare l'impatto potenziale sul conto economico e sul flusso di cassa.

Questi strumenti forniscono una base oggettiva per la valutazione del profilo di rischio aziendale, contribuendo a supportare decisioni più informate e a definire eventuali priorità di intervento.

3. Governance e organizzazione: il processo è supportato da un solido sistema di governance da parte del CDA che prevede il coinvolgimento del top management (tre linee di difesa) nel processo decisionale.

4. Performance management e miglioramento continuo: Infine, lavoriamo per integrare la cultura del rischio nella quotidianità organizzativa, sviluppando nuove competenze e promuovendo comportamenti consapevoli. Il sistema di performance management è orientato al miglioramento continuo, in coerenza con l'evoluzione del contesto e dei rischi emergenti.

Parallelamente, adottiamo un adeguato livello di comprensione dei rischi legati al business e ai processi aziendali, così da ottimizzare i risultati e rafforzare la capacità di risposta del Gruppo. Una gestione strutturata e consapevole dei rischi contribuisce inoltre a migliorare la capacità negoziale sul mercato e a tutelare la continuità operativa, mantenendo gli impatti di eventuali eventi negativi entro limiti di accettabilità definiti. A conferma della solidità del sistema, le risultanze delle analisi del processo ERM sono condivise periodicamente anche con la Funzione Internal Audit.



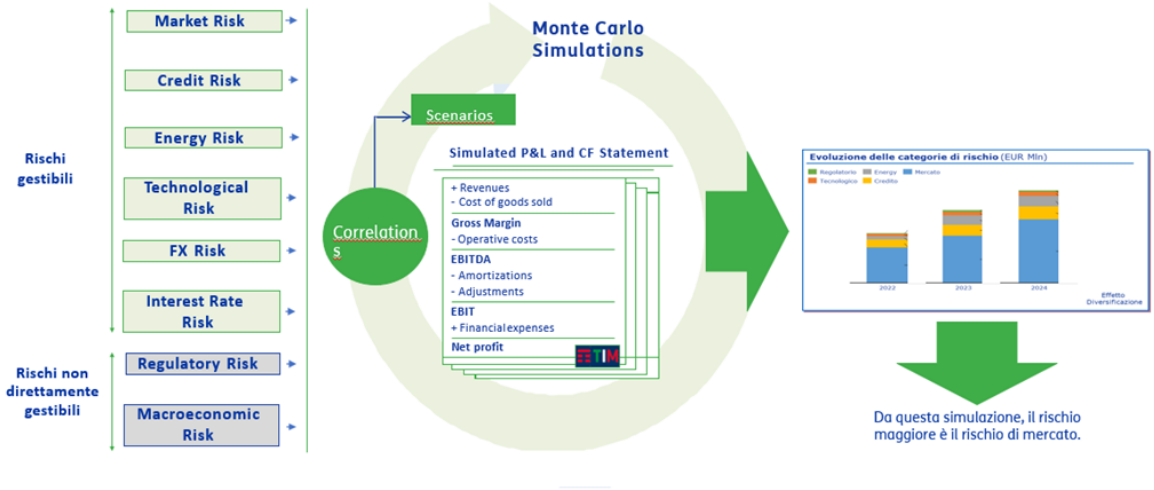
3. Approccio quantitativo alla valutazione del rischio

Nella fase di valutazione dei rischi, oltre all'analisi qualitativa, adottiamo anche strumenti quantitativi per stimare in modo oggettivo l'impatto potenziale dei diversi eventi di rischio. Tra questi, il **metodo Monte Carlo** rappresenta una tecnica centrale: si tratta di un modello di simulazione che, attraverso l'elaborazione di migliaia di scenari costruiti su basi statistiche e probabilistiche, consente di quantificare le possibili variazioni nei risultati economico-finanziari dell'azienda.

Come illustrato nello schema di seguito, il processo prende avvio dall'individuazione delle principali categorie di rischio, distinte tra quelle gestibili (come rischio di mercato, di credito, tecnologico, energetico, valutario, tassi d'interesse) e quelle non direttamente controllabili (come rischio regolatorio e macroeconomico). A partire da queste, vengono generate simulazioni che incorporano le correlazioni tra i diversi rischi, producendo così una serie di scenari plausibili. Ogni scenario consente di stimare l'effetto sul conto economico e sul flusso di cassa: ricavi, margini, EBITDA, EBIT e utile netto.

L'output della simulazione, visibile nel grafico di seguito rappresentato, mostra l'evoluzione aggregata del contributo di ciascuna categoria di rischio sull'andamento economico nei diversi anni. L'analisi evidenzia che, nel periodo considerato, il rischio di mercato rappresenta

la componente con il maggiore impatto potenziale, seguita da altre categorie con peso minore grazie anche all'effetto di diversificazione.

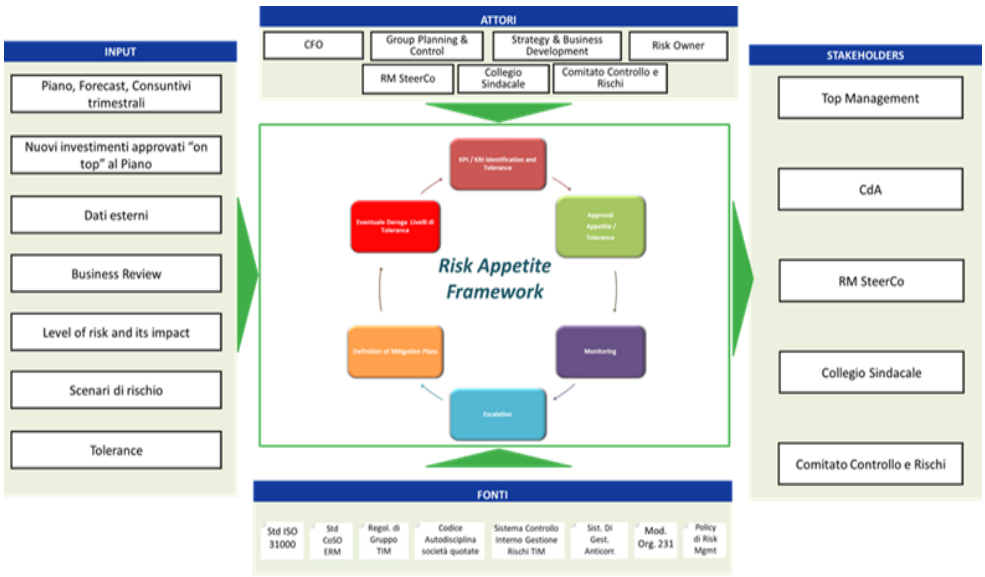


4. Gestione integrata del rischio: il ruolo del Risk Appetite Framework

Nel nostro approccio all'Enterprise Risk Management, utilizziamo il Risk Appetite Framework (RAF) per definire e rappresentare in modo strutturato la propensione al rischio dell'azienda, in coerenza con gli obiettivi strategici di medio-lungo termine espressi nel Piano Industriale. Nello specifico, questo strumento ci consente di identificare, valutare e monitorare i rischi chiave attraverso una metodologia basata su Key Risk Indicators (KRIs) e modelli che stimano la probabilità di raggiungimento delle performance attese, nonché l'impatto di eventuali scostamenti rispetto ai target prefissati.

Il framework si sviluppa attorno a un processo ciclico e continuo che parte dalla definizione dei livelli di tolleranza al rischio, prosegue con l'approvazione del Risk Appetite, -ovvero del livello di rischio che l'azienda è disposto ad accettare-, il monitoraggio dei risultati e l'eventuale escalation o deroga nei casi di superamento delle soglie, e si chiude con la definizione e l'attuazione di piani di mitigazione.

Come illustrato nell'immagine seguente, il RAF si alimenta con input provenienti da più fonti: analisi del piano industriale, dati previsionali e consuntivi, approvazioni di investimenti straordinari, dati di mercato, scenari di rischio e valutazioni di impatto.



Il RAF coinvolge attivamente diverse funzioni aziendali (CFO, Group Planning & Control, Strategy & Business Development, Risk Owner) e organi di controllo (Comitato Controllo e Rischi, Collegio Sindacale), garantendo un presidio trasversale e condiviso dei rischi. Gli output del processo sono condivisi con i principali stakeholder, tra cui il Top Management, il Consiglio di Amministrazione e lo Steering Committee ERM .

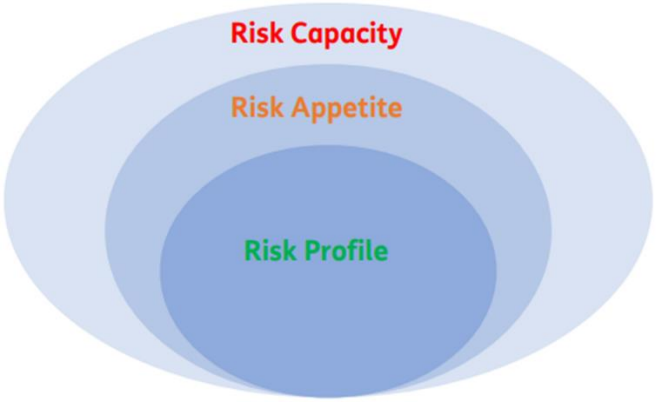
Il RAF si basa su un insieme articolato di riferimenti normativi e regolamentari, tra cui gli standard ISO 31000 e COSO ERM, il Modello Organizzativo 231, le policy aziendali di risk management e il Codice di Autodisciplina delle società quotate. Gli output del processo alimentano le nostre decisioni strategiche e operative, guidando lo sviluppo di azioni di mitigazione mirate e contribuendo a garantire un equilibrio efficace tra rischio e rendimento.

Andando nel dettaglio il nostro **ciclo RAF si articola in sei fasi operative**:

1. **Identificazione dei KPI/KRI rilevanti e livelli proposti di appetite/tolerance :** la funzione ERM analizza i dati del Piano Strategico e, sulla base dei livelli di rischio stimati (@Risk), propone gli obiettivi ritenuti rilevanti e i relativi livelli di appetite e tolerance.
2. **Approvazione:** i livelli di appetite/tolerance vengono condivisi con il CFO e sottoposti al Comitato Controllo e Rischi, per poi essere approvati dal Consiglio di Amministrazione.
3. **Monitoraggio:** trimestralmente, o su richiesta, monitoriamo i livelli approvati tramite l'analisi dei dati previsionali, consuntivi e di business aggiornati. Nei Business Plan includiamo anche i nuovi progetti strategici, che simuliamo tramite modelli quantitativi e Monte Carlo analysis per valutarne l'impatto sulla probabilità di raggiungimento degli obiettivi.
4. **Escalation**: in caso di superamento dei livelli definiti, la funzione ERM attiva un processo di escalation, coinvolgendo il Risk Owner per valutare l'esposizione al rischio e definire azioni correttive.
5. **Piani di mitigazione:** definiamo e attuiamo piani mirati a riportare i livelli di rischio entro i limiti di accettabilità.
6. **Deroga**: in casi selezionati e formalmente autorizzati, possiamo prevedere una deroga ai livelli di tolerance, mantenendo comunque il presidio attraverso il monitoraggio

Il RAF adottato in azienda si basa su un insieme di concetti ben distinti che guidano la gestione del rischio:

- **Risk Capacity** : è il livello massimo di rischio che siamo tecnicamente in grado di sopportare senza compromettere la continuità aziendale.
- **Risk Appetite**: rappresenta il livello complessivo di rischio che siamo disposti ad accettare per perseguire i nostri obiettivi strategici.
- **Risk Tolerance**: indica lo scostamento massimo dagli obiettivi che riteniamo tollerabile senza compromettere il raggiungimento degli stessi, né esporci a perdite, problemi operativi o danni reputazionali.
- **Risk Profile**: è il livello di rischio effettivamente assunto dall'Azienda in un determinato momento.



La rappresentazione grafica evidenzia come il risk profile debba restare all'interno del perimetro definito dal risk appetite, il quale, a sua volta, non deve mai avvicinarsi alla soglia della risk capacity. La tolerance funge da cuscinetto di sicurezza, oltre il quale si attivano meccanismi di controllo o di mitigazione.

5. Mappatura, classificazione e prioritizzazione dei rischi

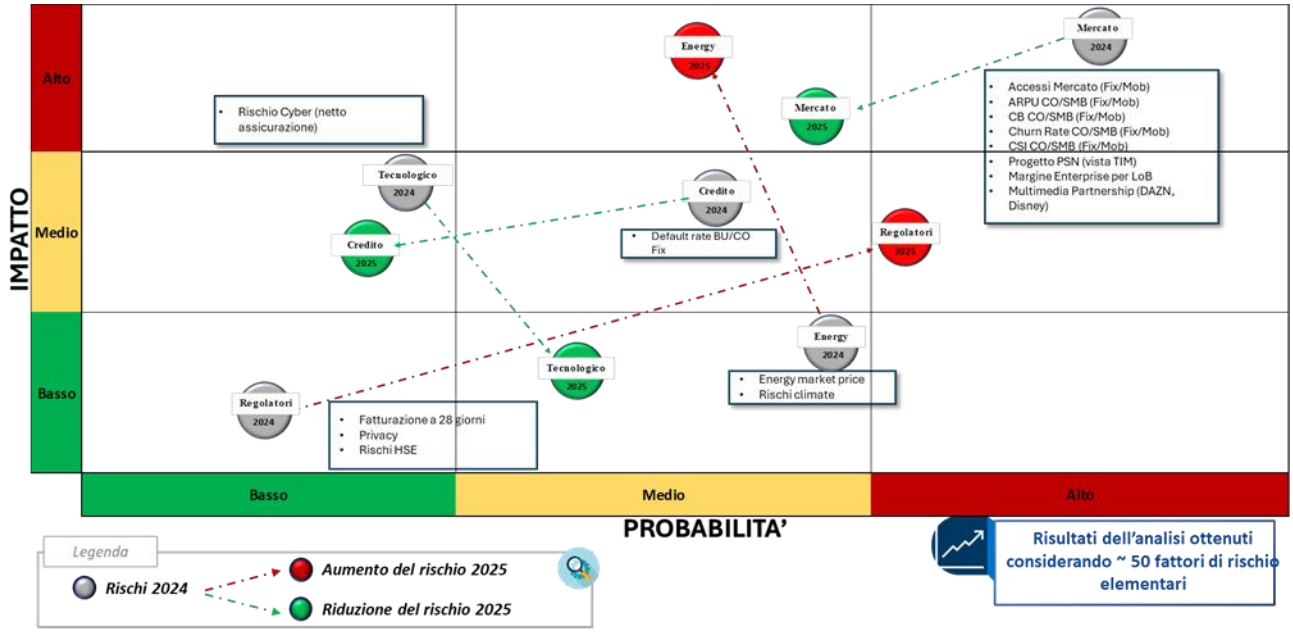
Nel nostro sistema di gestione integrata del rischio, adottiamo una metodologia che parte dalla mappatura e classificazione delle principali aree di rischio per arrivare alla valutazione della loro probabilità e impatto potenziale, e quindi alla prioritizzazione all'interno di una

matrice dinamica. Questo approccio offre una visione strutturata e aggiornata della nostra esposizione complessiva al rischio, con l'obiettivo di orientare in modo efficace le attività di mitigazione e controllo.

Come rappresentato nella figura sopra, i rischi che consideriamo sono organizzati nelle seguenti categorie principali:

- **Rischi di mercato,** legati all'andamento della domanda e ai cambiamenti competitivi;
- **Rischi tecnologici,** relativi al funzionamento e all'evoluzione della rete TLC;
- **Rischi informatici e di sicurezza**, legati a minacce cyber, furto di dati o distruzione;
- **Rischi energetici e climatici,** che derivano dalla volatilità dei mercati e dalle condizioni ambientali;
- **Rischi legali e regolatori,** connessi a incertezze normative e contenziosi;
- **Rischi finanziari**, di **credito** e di **tasso di cambio**, riconducibili a condizioni macroeconomiche, solvibilità e fluttuazioni monetarie.

Per ciascuna categoria, definiamo il livello di tolleranza e stimiamo la probabilità e l'entità dell'impatto potenziale, attraverso modelli valutativi supportati da circa 50 fattori elementari di rischio.



I risultati della nostra analisi vengono quindi rappresentati all'interno di una matrice dei rischi, come illustrato nella seconda immagine. Ogni rischio è posizionato in base al suo livello di probabilità (asse orizzontale) e di impatto (asse verticale), e contrassegnato da un'etichetta che indica la categoria di appartenenza e l'orizzonte temporale (es. 2024 o 2025), per supportare una pianificazione efficace nel tempo i rischi sono distribuiti lungo tre livelli di severità:

- Basso (verde): tollerabili senza azioni urgenti;
- Medio (giallo): soggetti a monitoraggio e azioni preventive;
- Alto (rosso): richiedono interventi prioritari.

Alcuni esempi evidenziano le nostre priorità attuali:

Il rischio Cyber, mitigato attraverso il trasferimento al mercato assicurativo, è posizionato in area "gialla" per il potenziale impatto sulla continuità operativa.

I rischi di mercato risultano distribuiti su più livelli, in funzione delle dinamiche di accesso, churn rate e ricavi medi.

Rischi energetici, regolatori e di credito commerciale assumono importanza variabile in base all'evoluzione del contesto esterno e normativo.

Aggiorniamo la matrice periodicamente, sulla base di dati previsionali, consuntivi e analisi di scenario, al fine di garantire un presidio continuo e reattivo. Questo ci consente di anticipare

criticità, rafforzare le misure di mitigazione e ottimizzare le risorse impiegate nei meccanismi di controllo, in coerenza con la nostra propensione al rischio e con gli obiettivi di sostenibilità, resilienza e creazione di valore nel lungo periodo.

6. Analisi e gestione dei rischi più rilevanti

A partire dalla matrice dei rischi presentata nel paragrafo precedente, nella quale rappresentiamo visivamente il posizionamento dei rischi secondo una valutazione combinata di probabilità di accadimento e potenziale impatto, approfondiamo di seguito l'analisi di due rischi significativi per il nostro Gruppo: il rischio di mercato e il rischio energetico. Per ciascuno descriviamo le metodologie utilizzate per la valutazione dell'impatto e le principali azioni di mitigazione adottate.

Rischio di mercato

L'evoluzione del contesto competitivo e della domanda, influenzata da fattori come i prezzi dei servizi, la qualità percepita dai clienti e le dinamiche degli accordi commerciali, rappresenta un elemento critico nella nostra analisi dei rischi di mercato. Per valutarne l'impatto, utilizziamo una combinazione di modelli quantitativi deterministici e probabilistici, tra cui:

- Metodo di ottimizzazione vincolata;
- Simulazioni Monte Carlo per analisi probabilistica;
- Modello basato sulla Teoria dei Giochi (Equilibrio di Nash);
- Modello CashFlow@Risk, focalizzato sull'impatto sui target del Piano Industriale;
- Modello NPV@Risk per la valutazione dei rischi associati a progetti industriali di investimento.

Per mitigare l'impatto dei rischi identificati, abbiamo messo in atto diverse iniziative, tra cui:

- offerte convergenti con partner come DAZN, Netflix e Disney+, che aumentano il valore percepito e fidelizzano la clientela;
- miglioramento continuo della qualità di rete, con investimenti nelle infrastrutture, inclusa la rete 5G;

- campagne di acquisizione mirate, rivolte a clienti provenienti da altri operatori;
- monitoraggio del posizionamento prezzo/qualità, per garantire competitività in linea con le dinamiche di mercato.

Rischio Energy

L'impatto del rischio energetico, dovuto alla volatilità del prezzo dell'energia e all'evoluzione del contesto macroeconomico e geopolitico, è anch'esso monitorato con estrema attenzione. Per valutare questo rischio, utilizziamo:

- **il modello probabilistico** che simula l'andamento dei prezzi dell'energia integrando elementi di trend e volatilità;
- La quantificazione avviene misurando la distanza tra il 5° percentile del prezzo simulato e il valore previsto nel Piano, in modo da ottenere una stima robusta e prudenziale.

Le azioni di mitigazione adottate comprendono:

- **la definizione di una policy per la gestione delle coperture energetiche**, che prevede l'uso di contratti forward e strumenti derivati per stabilizzare i costi;
- **Il monitoraggio continuo del rischio,** con analisi condivise periodicamente tra le funzioni coinvolte, in particolare Pianificazione Controllo e Finanza e Procurement, con una frequenza almeno trimestrale.

Attraverso queste attività, manteniamo un controllo attivo e integrato sul profilo di rischio, assicurando coerenza con i nostri obiettivi di sostenibilità economica e stabilità operativa.

7. Riconoscimento e gestione dei rischi emergenti

In continuità con la valutazione dei rischi prioritari, ampliamo la nostra prospettiva includendo quei fenomeni che, pur non essendo ancora pienamente manifesti, possono avere impatti rilevanti nel medio-lungo termine (3–5 anni). Questi rischi emergenti rappresentano, in linea con il modello del World Economic Forum, nuove tipologie di rischio "disruptive" difficili da quantificare e di lunga durata

Nei sottoparagrafi seguenti approfondiamo tre rischi emergenti di particolare significato per il Gruppo TIM, cedendo attenzione anche agli impatti e alle azioni di mitigazione adottate.

Rischi e sfide derivanti dall'adozione dell'Intelligenza Artificiale

Nel nostro contesto aziendale, l'adozione di soluzioni e sistemi di Intelligenza Artificiale (AI) è in costante crescita, in linea con l'evoluzione tecnologica che sta trasformando il settore delle telecomunicazioni. L'AI rappresenta per noi una leva strategica in grado di generare efficienze operative e innovazione, ma al tempo stesso introduce rischi nuovi e complessi, che richiedono una gestione attenta, responsabile e lungimirante.

Le minacce: l'integrazione dell'AI nei nostri processi aziendali pone diverse sfide operative e di sistema, tra cui:

- disponibilità di budget adeguati;
- rispetto della conformità normativa nazionale ed europea;
- gestione della sicurezza dei dati e delle infrastrutture;
- mancanza di competenze specialistiche per progettare, implementare e governare le soluzioni AI;
- qualità e integrità dei dati;
- analisi dei big data e capacità decisionali in tempo reale;
- interoperabilità e adeguatezza dell'infrastruttura tecnologica;
- difficoltà di integrazione con sistemi esistenti;
- limitazioni negli approvvigionamenti tecnologici;
- necessità di assicurare trasparenza, affidabilità e fiducia nei confronti degli stakeholder.

  A fronte di queste sfide, riconosciamo che l''adozione delle tecnologie AI espone l'azienda a minacce specifiche, tra cui:

  - violazioni della privacy e della sicurezza dei dati personali;
  - mancato rispetto di norme su proprietà intellettuale e copyright;
  - discriminazioni algoritmiche e bias nei risultati dei sistemi AI;
  - esposizione a rischi di cybersecurity connessi al funzionamento dei sistemi intelligenti.

I possibili impatti: le conseguenze potenziali associate a questi rischi possono essere di tipo economico, legale e reputazionale. In particolare, l'impatto normativo è uno degli aspetti più rilevanti. La non conformità con il nuovo regolamento europeo sull'AI (AI Act) può

comportare sanzioni finanziarie elevate, che vanno fino al 7% del fatturato mondiale annuo per l'uso di sistemi AI vietati, e fino al 3% per il mancato rispetto dei requisiti relativi ai sistemi classificati ad alto rischio.

Accanto al rischio sanzionatorio, esiste anche il potenziale rischio di mancato raggiungimento dei benefici attesi dagli investimenti in AI, dovuto a minori ricavi rispetto alle previsioni, o a costi superiori sostenuti per sviluppare, mantenere o correggere le soluzioni implementate.

Le azioni di mitigazione: per affrontare in modo sistemico queste sfide, abbiamo scelto di adottare una governance centralizzata dell'AI, coerente con gli obiettivi del nostro Piano Strategico. "Abbiamo istituito un team multifunzionale, composto da esperti provenienti da diverse funzioni aziendali (es. Strategia, Finanza, Compliance, Legale, Sicurezza, ecc.), per garantire una gestione integrata e coerente dell'AI, tenendo conto della sua complessità tecnica e organizzativa.

Le nostre principali azioni di mitigazione includono:

- definizione di politiche e procedure per regolare l'uso responsabile dell'AI, promuovendo al contempo una cultura etica e una maggiore consapevolezza tra Client, Fornitori e Dipendenti.
- adozione di una struttura di governance centralizzata, con ruoli e responsabilità ben definiti, a garanzia di un presidio efficace lungo l'intero ciclo di vita dei sistemi AI.
- creazione e mantenimento di un inventario aggiornato di tutti i modelli e sistemi AI in uso all'interno del Gruppo, comprensivo dei dati utilizzati e della logica implementata.
- implementazione di uno strumento di classificazione del rischio per ciascun sistema AI, in conformità con le categorie e i requisiti previsti dall'AI Act.
- integrazione di un processo strutturato di gestione del rischio lungo tutto il ciclo di vita delle soluzioni AI: dalla progettazione allo sviluppo, fino alla fase di test e rilascio. Il modello prevede interventi:
  - preventivi, secondo il principio dell'"etica by design";

- ex-post, con attività di monitoraggio continuo, supervisione umana e revisione periodica delle prestazioni dei sistemi AI, per individuare eventuali bias e correggere le anomalie in modo tempestivo.

L'obiettivo finale è quello di garantire che ogni sistema AI sia progettato e gestito nel rispetto dei diritti fondamentali delle persone, assicurando la massima sicurezza, sia per gli individui, sia per i beni e i processi aziendali associati.

Rischio di transizione: Introduzione di una Carbon Tax

Nel nostro processo di Enterprise Risk Management abbiamo incluso il rischio ambientale emergente legato all'introduzione di una Carbon Tax sulle emissioni di CO_2. Questo rischio, di natura regolatoria e finanziaria, è strettamente connesso al percorso globale di transizione verso un'economia a basse emissioni e potrebbe generare costi aggiuntivi significativi per le nostre attività operative, in particolare in relazione alle iniziative di decarbonizzazione.

Le minacce: abbiamo condotto un'analisi approfondita delle attività e degli asset potenzialmente incompatibili con una strategia Net Zero, valutandone la coerenza con il Regolamento Delegato (UE) 2021/2139 e con i criteri della Tassonomia UE. Gli elementi critici emersi includono:

- gestione dei data center e delle infrastrutture di rete;
- consumo energetico diretto e indiretto;
- dipendenza da fonti fossili nella supply chain.

I possibili impatti : l'impatto potenziale è stato quantificato tramite analisi di scenario – sia qualitative sia quantitative – ispirate al framework NGFS (Network for Greening the Financial System), con l'obiettivo di allineare la nostra strategia climatica al contenimento del riscaldamento globale entro 1,5 °C. In particolare:

- abbiamo stimato un prezzo medio di riferimento per la carbon tax pari a 83,5 € per tCO_2 (anno 2024);
- è stata effettuata una stima lineare della riduzione delle emissioni fino al 2040, con proiezioni a intervalli decennali;

- abbiamo valutato gli impatti economici in caso di mancato raggiungimento degli obiettivi con scostamenti del 10%, 20% e 30%;
- abbiamo considerato anche gli effetti di eventi climatici estremi che potrebbero compromettere la continuità operativa dei servizi.

Le azioni di mitigazione: per limitare l'esposizione al rischio e anticipare i potenziali impatti negativi, abbiamo adottato una serie di iniziative mirate, tra cui:

- certificazione del Sistema di Gestione Ambientale conforme allo standard ISO 14001 e adesione a target scientifici definiti con metodologia SBTi.
- anticipo al 2025 dell'obiettivo di utilizzare energia elettrica 100% rinnovabile per tutte le attività italiane. In Brasile, tale obiettivo è già stato raggiunto.
- piano nazionale di interventi per l'ammodernamento delle infrastrutture e dei sistemi di condizionamento, con l'obiettivo di ridurre le emissioni e migliorare l'efficienza energetica.
- modernizzazione dei beni tecnologici negli immobili industriali, con priorità ai siti strategici, per garantire resilienza e sostenibilità a lungo termine.
- adozione di un sistema di gestione energetica (BEMS) con dispositivi IoT per il monitoraggio e la manutenzione predittiva dei sistemi tecnologici.
- coinvolgimento attivo dei fornitori, tramite l'introduzione di criteri ESG più stringenti nei processi produttivi, al fine di ridurre le emissioni indirette lungo la supply chain.

Con queste azioni rafforziamo il nostro impegno per una transizione equa e sostenibile, riducendo la nostra esposizione a futuri costi ambientali e aumentando la resilienza delle nostre operazioni.

Rischi di minacce informatiche e impatti legati al contesto geopolitico

In un mondo sempre più interconnesso, il rischio informatico – amplificato dalle tensioni geopolitiche e dall'evoluzione normativa europea – rappresenta una delle sfide più critiche per la sicurezza del nostro business. La crescente dipendenza da tecnologie digitali e infrastrutture IT aumenta la nostra esposizione a minacce cyber complesse e sofisticate, con potenziali impatti su asset, dati e reputazione.

Le minacce: il World Economic Forum ha identificato gli attacchi informatici transfrontalieri tra le aree più critiche di rischio emergente. In questo contesto, l'adozione di misure legislative da parte dell'UE – come la Direttiva NIS2 e la proposta di Legge sulla Cybersecurity – mira a rafforzare la resilienza dei settori critici, telecomunicazioni incluse.

I possibili impatti :

- interruzione della disponibilità di asset a supporto dei servizi ICT;
- sanzioni regolatorie per Data Breach e mancata conformità alla normativa (es. NIS2);
- perdita di fiducia da parte dei clienti, soprattutto istituzionali e strategici;
- danni reputazionali ed economici in caso di attacchi geopoliticamente motivati.

Nel 2024 abbiamo registrato un solo incidente informatico di medio impatto (un attacco DDoS), prontamente contenuto senza perdite di dati né interruzioni della rete pubblica. Altri due episodi minori non hanno avuto conseguenze economiche o operative rilevanti.

Azioni di mitigazione: per garantire un presidio efficace e continuo della sicurezza informatica, abbiamo adottato un approccio proattivo e strutturato, che include:

- Valutazioni regolari del rischio, con attività di penetration testing, vulnerability assessment e utilizzo della metodologia FAIR (Factor Analysis of Information Risk) per la quantificazione economica dei rischi cyber.
- Security Operations Center (SOC) attivo 24/7, in grado di rilevare, prevenire e rispondere tempestivamente a ogni minaccia.
- Certificazione ISO 22301 per la gestione della continuità operativa, a garanzia della resilienza dei servizi erogati.
- Certificazione ISO 27001 per la sicurezza delle informazioni, insieme a sistemi crittografici avanzati per la protezione dei dati sensibili.
- Policy aziendali di Data Recovery, che prevedono il salvataggio e la protezione di backup non esposti a reti pubbliche.
- Monitoraggio continuo della compliance normativa, assicurato dalla funzione Compliance in sinergia con tutte le funzioni coinvolte nei processi digitali.

Attraverso questi strumenti, presidiamo attivamente le minacce cyber emergenti, proteggiamo la fiducia dei nostri stakeholder e assicuriamo la continuità e l'affidabilità dei nostri servizi.