



RISK MANAGEMENT

Approfondimento

Gruppo TIM

Luglio 2026



INDICE

1. Il nostro modello di Risk Management.....	3
2. Il processo di Risk Management	5
3. Approccio quantitativo alla valutazione del rischio	7
4. Gestione integrata del rischio: il ruolo del Risk Appetite Framework	8
5. Mappatura, classificazione e prioritizzazione dei rischi.....	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 Rischi 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):

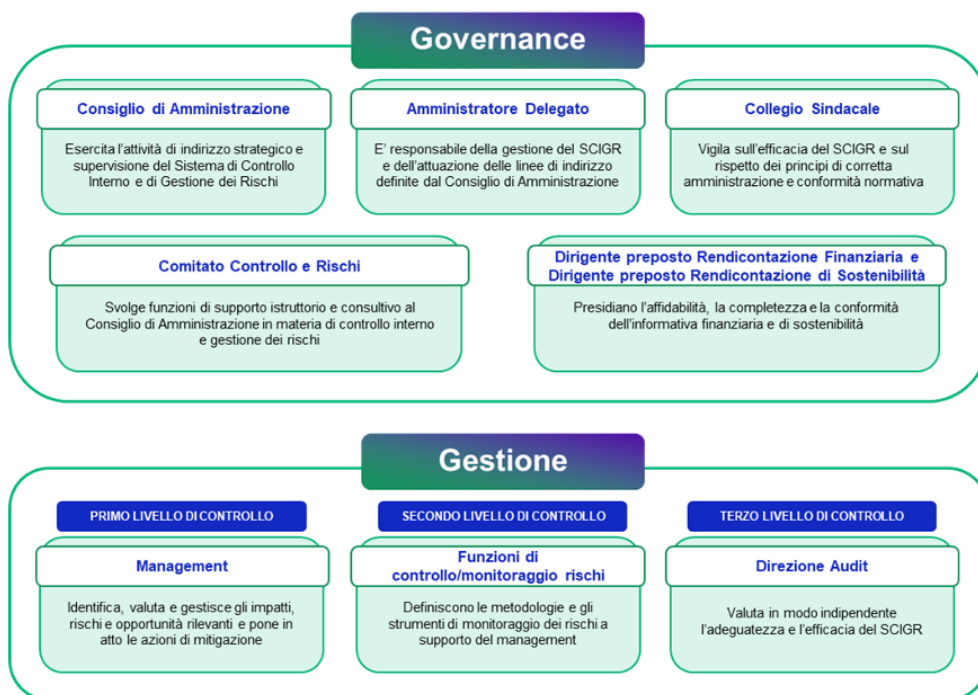
- la **prima linea**, rappresentata dal **management**, identifica, valuta e gestisce i rischi nell’ambito delle attività operative;
- la **seconda linea**, costituita dalle **funzioni di controllo e monitoraggio**, supervisiona il processo di gestione, definisce metodologie e verifica l’applicazione 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.

Questo 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.



I rischi di maggiore rilevanza strategica o con impatti cross-funzionali sono oggetto di supervisione da parte dello Steering Committee ERM, che supporta il CFO nel governo del profilo di rischio di Gruppo.



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

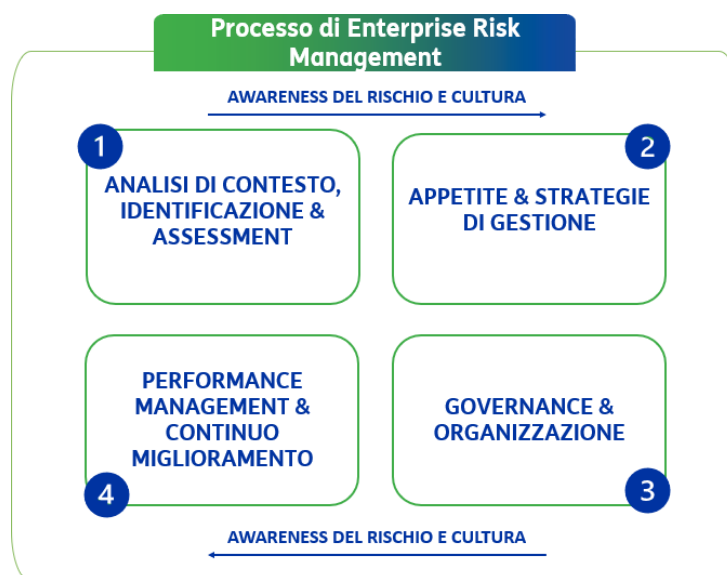
Nel Gruppo TIM, il processo di Enterprise Risk Management (ERM) è strutturato in un ciclo continuo e integrato, pensato per garantire una gestione efficace e proattiva dei rischi aziendali. Il processo si articola in quattro fasi principali, affiancate dalla promozione trasversale di una solida cultura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



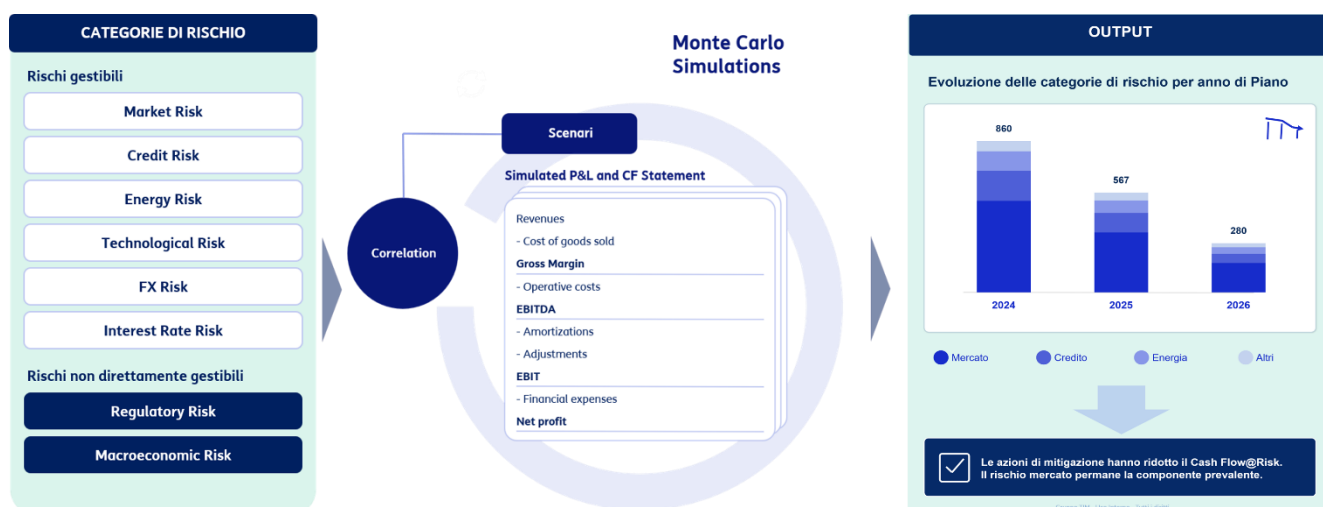


3. Approccio quantitativo alla valutazione del rischio

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.



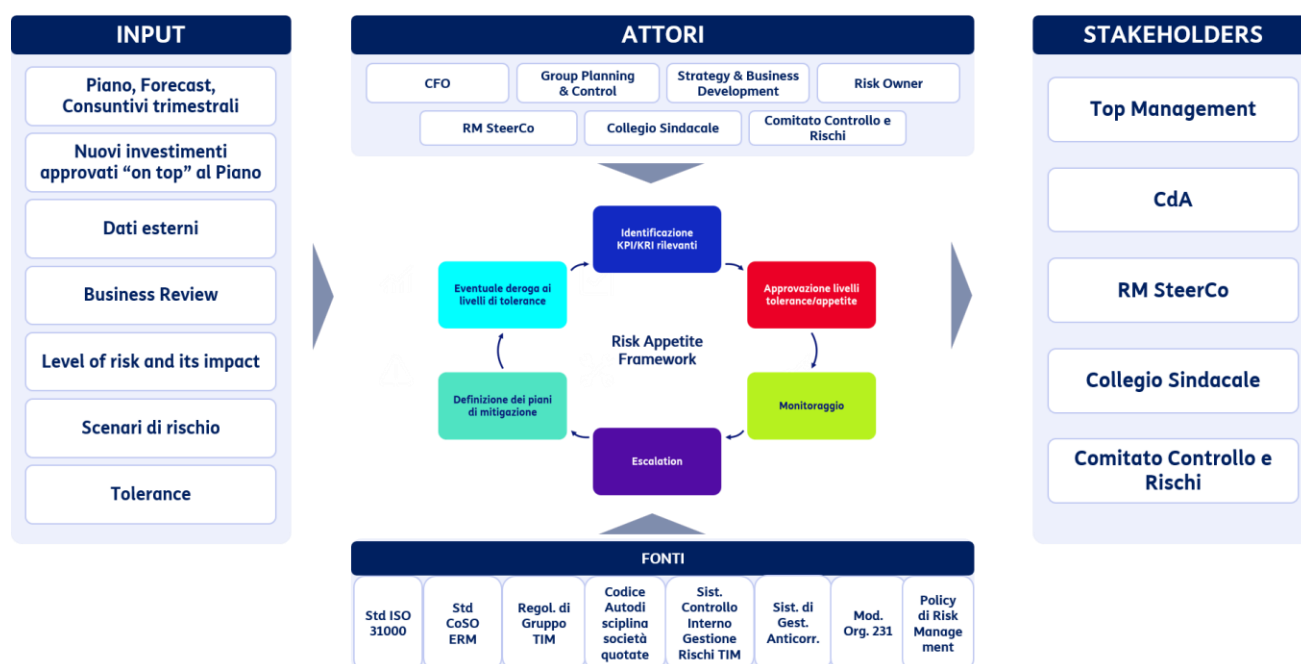
4. Gestione integrata del rischio: il ruolo del Risk Appetite Framework

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 traduce in un processo ciclico e continuo che parte dalla definizione dei livelli di tolleranza al rischio, prosegue con l'approvazione del Risk Appetite ossia del livello di rischio che l'azienda è disposta ad accettare e delle relative soglie operative di allerta preventiva (Early Warning), di tolleranza (Tolerance) e di criticità (Stress) -; 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.



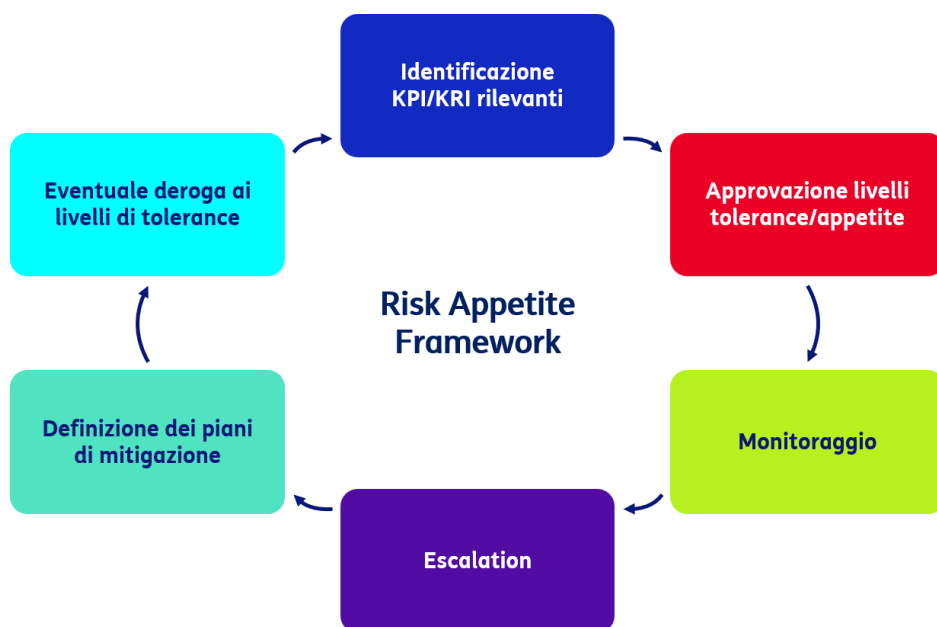
Come illustrato nell'immagine seguente, il Risk Appetite Framework si alimenta con input provenienti da più fonti: analisi del piano industriale, dati previsionali e consuntivi, approvazioni di investimenti straordinari, dati di mercato, scenari di rischio e valutazioni di impatto.



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 Risk appetite Framework **si articola in sei fasi operative:**

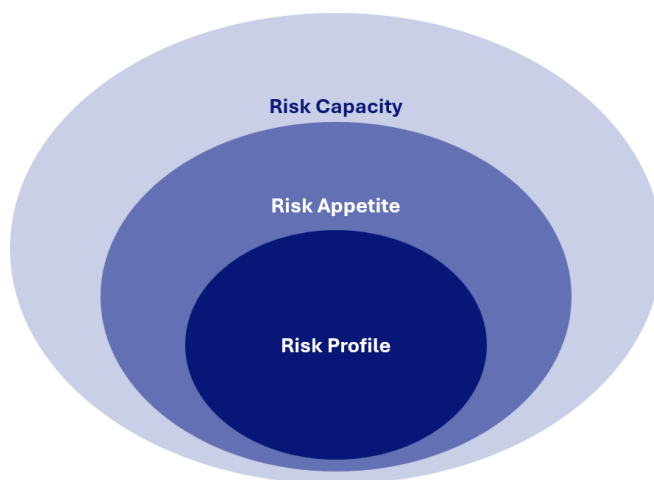


1. **Identificazione dei KPI/KRI rilevanti e livelli proposti di appetite/tolerance:** la funzione ERM analizza i dati del Piano Strategico e, sulla base dei livelli di rischio stimati (@Risk), propone gli obiettivi ritenuti rilevanti e i relativi livelli di appetite e tolerance.
2. **Approvazione:** 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 ERM, adottiamo una metodologia che prevede la mappatura e la classificazione delle principali aree di rischio, la valutazione della probabilità e dell'impatto potenziale e la successiva prioritizzazione in una matrice dinamica. Questo approccio offre una visione strutturata e aggiornata dell'esposizione complessiva al rischio, e orienta in modo efficace le attività di mitigazione e controllo.

In coerenza con l'evoluzione del contesto normativo, tecnologico e di business, il framework ERM monitora costantemente i rischi emergenti e i fattori di cambiamento che possono modificare il profilo di rischio aziendale.

Di seguito le principali aree di rischio identificate dal Gruppo TIM:

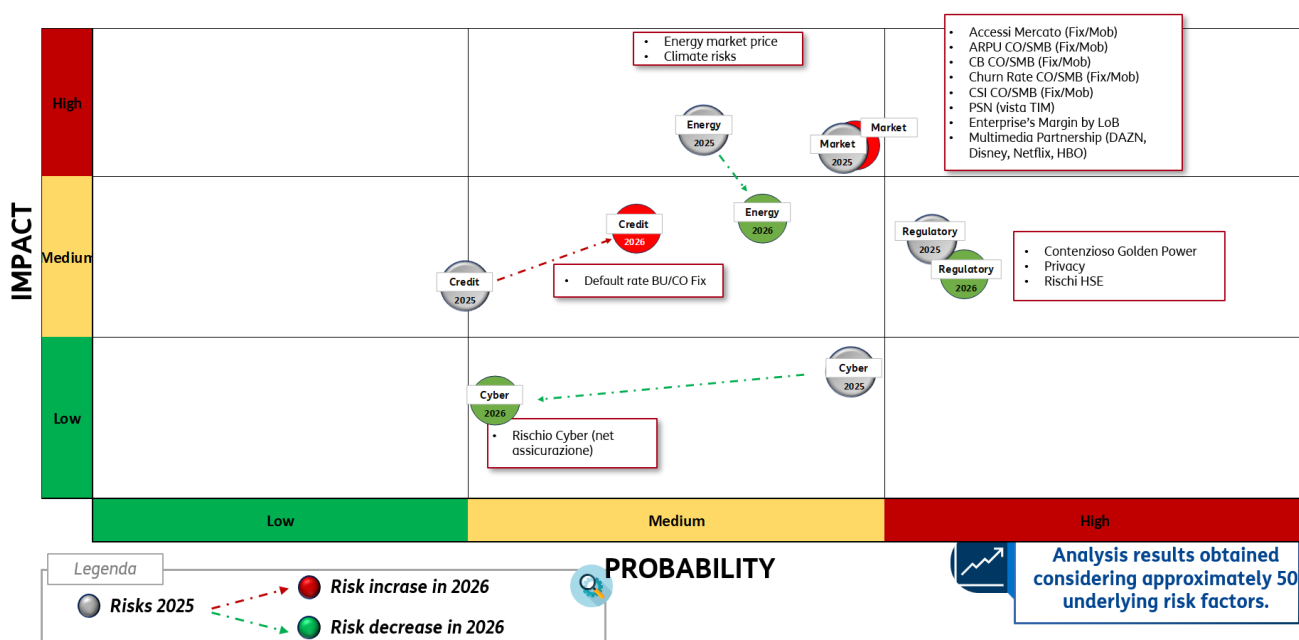
Rischi di mercato	Rischi derivanti da cambiamenti nell'ambiente competitivo e nella domanda, in relazione al pubblico di riferimento specifico, a seconda della qualità percepita dai clienti, dell'andamento dei prezzi e degli accordi commerciali.
Rischi tecnologici	Rischi legati al funzionamento quotidiano della rete TLC, alla sua trasformazione tecnologica, alla protezione degli asset da attacchi informatici, nonché agli effetti di accordi strategici/commerciali.
Rischi informatici e di sicurezza	Rischio di incorrere in perdite economiche/finanziarie e/o reputazionali a seguito di verificarsi di eventi accidentali o azioni dolose inerenti alle informazioni gestite dai sistemi informatici (hardware, software, database, ecc.) che comportano violazioni dei dati, furti e distruzione.
Rischi energetici	Rischio di superamento dei costi energetici a causa della volatilità del mercato energetico e dell'ambiente macroeconomico e geo-politico nazionale e internazionale.
Rischi legali e regolatori	Volatilità dei prezzi regolamentati all'ingrosso per l'accesso al mercato fisso e incertezza sull'esito delle controversie significative in corso derivanti dalle indicazioni dell'Autorità.
Rischi di compliance	Non conformità dei processi alle normative pertinenti e alle regolamentazioni delle autorità competenti, che espongono l'azienda a una certa quantità di sanzioni e costi aumentati.
Rischi climatici	Scenario meteorologico in evoluzione con generazione di condizioni climatiche estreme che impattano sul valore degli asset fisici distribuiti sul territorio, sui costi aziendali (Assicurazione, Energia) sostenuti per garantire la continuità e gli obiettivi di risparmio e sulla produttività del lavoro.
Rischi di credito commerciale	Perdite derivanti dal mancato pagamento del fatturato attivo da parte di clienti o partner commerciali/tecnologici.
Rischi finanziari	Incertezza sulle performance finanziarie attese a causa di condizioni di finanziamento volatili o di cambiamenti nelle condizioni macroeconomiche.
Rischi legati al tasso di cambio	Fluttuazioni nei tassi di cambio delle diverse valute, rispetto alla valuta di consolidamento (Euro), che possono comportare variazioni nel patrimonio netto consolidato; e fluttuazioni nei tassi di cambio di valute derivanti dalla valutazione e conversione di crediti (debiti) commerciali.
Rischi legati all'Intelligenza Artificiale	Rischi derivanti dall'adozione e dall'utilizzo di sistemi di Intelligenza Artificiale, con particolare riferimento a trasparenza, affidabilità, sicurezza, bias algoritmici, tutela dei dati, conformità normativa (AI Act) e rispetto dei principi etici e di equità.
Rischi legati alla catena di fornitura	Rischi derivanti dalla gestione della supply chain, con particolare riferimento alla resilienza dei fornitori, al rispetto dei principi ESG, dei diritti umani, delle normative ambientali e sociali e alla continuità delle forniture.

Come rappresentato precedentemente, 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, dalle condizioni ambientali e dai cambiamenti climatici;
- **Rischi legali e regolatori**, connessi a incertezze normative e contenziosi;
- **Rischi finanziari, di credito e di cambio** riconducibili a condizioni macroeconomiche, solvibilità e fluttuazioni monetarie;
- **Rischi connessi all'Intelligenza Artificiale**, relativi a trasparenza, affidabilità, bias algoritmici, sicurezza, protezione dei dati, conformità normativa e rispetto dei principi etici e di equità;
- **Rischi della catena di fornitura**, connessi alla continuità operativa, all'affidabilità dei fornitori, alla volatilità dei costi, alla conformità normativa e agli impatti ambientali e sociali, inclusi la tutela dei diritti umani e il rispetto degli standard ESG.

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.



*The representation is based on EBITDA-Capex@Risk, evaluated at a 5% confidence level.



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. 2025 o 2026), 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 di rischio del paragrafo precedente, approfondiamo di seguito alcuni dei rischi più rilevanti per il Gruppo, selezionati in funzione del loro posizionamento e della significatività delle potenziali conseguenze per il business. Per ciascun rischio sono descritti i principali fattori di esposizione, le metodologie adottate per la valutazione e le relative modalità di gestione e mitigazione.



Rischi 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.

Rischi energetici e climatici

Il **rischio energetico** deriva principalmente dalla volatilità dei prezzi dell'energia, influenzata dall'evoluzione del contesto macroeconomico e geopolitico, e può determinare effetti significativi sui costi operativi del Gruppo e sulla loro prevedibilità.

Per valutare l'esposizione a tale rischio, TIM utilizza un **modello probabilistico** che simula l'andamento dei prezzi dell'energia, integrando elementi di trend e volatilità. La metodologia di quantificazione dell'esposizione misura la distanza tra il 5° percentile del prezzo simulato e



il valore previsto nel Piano, consentendo di stimare in termini prudenziali le potenziali conseguenze economiche derivanti da variazioni sfavorevoli dei prezzi dell'energia.

I **rischi climatici** comprendono sia i **rischi fisici**, derivanti dagli effetti del cambiamento climatico sulle infrastrutture e sulle attività del Gruppo, sia i **rischi di transizione**, associati all'evoluzione del contesto normativo, tecnologico e di mercato connessa al percorso verso un'economia a basse emissioni.

Con riferimento ai **rischi fisici**, la presenza di un'infrastruttura di rete estesa e capillare espone il Gruppo agli effetti del cambiamento climatico e agli eventi naturali estremi, che possono incidere sull'integrità degli asset, sulla continuità operativa e sulla qualità dei servizi erogati. I rischi considerati comprendono sia eventi acuti, quali alluvioni, tempeste, incendi e frane, sia fenomeni cronici, come l'aumento delle temperature e lo stress termico, che possono influenzare nel tempo le prestazioni delle infrastrutture, i consumi energetici e i relativi costi operativi.

La valutazione dei rischi fisici si basa su un approccio strutturato che considera l'identificazione degli hazard rilevanti, l'esposizione degli asset e la loro vulnerabilità rispetto ai singoli eventi climatici. Per i rischi fisici acuti, TIM utilizza inoltre metodologie quantitative a supporto della stima delle potenziali conseguenze economiche.

In tale ambito, il modello CLIMADA consente di valutare i potenziali effetti degli eventi climatici sugli asset e di supportare le decisioni relative alle misure di resilienza e alle coperture assicurative. Le valutazioni possono essere integrate da analisi desk e on-site e da simulazioni probabilistiche delle potenziali perdite dirette, al fine di individuare gli asset maggiormente esposti e definire le opportune misure di prevenzione e adattamento.

TIM sta inoltre sviluppando strumenti di analisi climatica orientati alla valutazione degli scenari futuri e delle conseguenze di medio-lungo periodo, con l'obiettivo di rafforzare progressivamente l'integrazione dei rischi climatici nei processi di pianificazione e gestione del rischio.

Con riferimento ai **rischi di transizione**, questi derivano dai cambiamenti connessi alla transizione verso un'economia a basse emissioni e possono incidere sul percorso di



decarbonizzazione del Gruppo e sul raggiungimento degli obiettivi climatici definiti nel Piano di Transizione.

I principali fattori di rischio considerati riguardano:

- l'evoluzione del quadro normativo e regolatorio e dei requisiti di rendicontazione in materia climatica e di sostenibilità, incluso il possibile rafforzamento dei meccanismi di carbon pricing;
- la crescita della domanda di traffico dati, servizi digitali, cloud e intelligenza artificiale, con il conseguente aumento dei consumi energetici e delle esigenze di efficientamento delle infrastrutture;
- l'evoluzione e la disponibilità di tecnologie e soluzioni a supporto dell'efficienza energetica delle reti e dei Data Center, nonché la capacità della catena del valore di contribuire agli obiettivi di riduzione delle emissioni Scope 3;
- l'evoluzione delle dinamiche competitive e delle aspettative di investitori, clienti e altri stakeholder rispetto agli impegni e alle performance climatiche del Gruppo.

Tali fattori possono determinare conseguenze economiche, finanziarie e operative, tra cui:

- maggiori costi e investimenti connessi all'adeguamento normativo e ambientale, ai meccanismi di carbon pricing, all'efficientamento delle infrastrutture e al raggiungimento degli obiettivi di decarbonizzazione;
- possibili scostamenti rispetto ai target climatici e alla traiettoria Net Zero, con potenziali effetti sull'accesso ai capitali e agli strumenti di finanza sostenibile e sulla reputazione del Gruppo;
- necessità di adeguare progressivamente processi, infrastrutture e modelli operativi per rispondere all'evoluzione tecnologica e di mercato e preservare la competitività nel lungo periodo.

La gestione dei rischi energetici e climatici è integrata nei processi di Enterprise Risk Management e si articola in misure di mitigazione, adattamento e trasferimento del rischio, definite in funzione delle diverse tipologie di esposizione.



Con riferimento al rischio energetico, il Gruppo adotta una policy per la gestione delle coperture energetiche, che prevede l'utilizzo di contratti forward e strumenti derivati finalizzati a contenere gli effetti della volatilità dei prezzi e a stabilizzare i costi. L'esposizione è inoltre oggetto di monitoraggio continuo, attraverso analisi condivise periodicamente tra le funzioni coinvolte, in particolare Pianificazione, Controllo e Finanza e Procurement, con frequenza almeno trimestrale.

Per i rischi climatici fisici, le analisi sull'esposizione e sulla vulnerabilità degli asset supportano l'individuazione delle misure di prevenzione, adattamento e resilienza e, per i rischi trasferibili, la definizione delle strategie di trasferimento del rischio, anche attraverso il ricorso a coperture assicurative.

Per i rischi climatici di transizione, le principali misure sono integrate nel Piano di Transizione e comprendono:

- il mantenimento dell'approvvigionamento di energia elettrica da fonti rinnovabili attraverso Garanzie d'Origine, PPA e iniziative di autoproduzione energetica;
- l'efficientamento energetico e la modernizzazione delle reti, dei Data Center, degli uffici e dei punti vendita;
- l'utilizzo di tecnologie innovative e soluzioni di monitoraggio energetico per l'ottimizzazione dei consumi;
- la progressiva elettrificazione della flotta aziendale e la riduzione dell'utilizzo di combustibili fossili;
- la riduzione delle emissioni lungo la catena del valore attraverso l'integrazione di criteri ESG nei processi di qualifica, selezione e monitoraggio dei fornitori;
- la promozione di iniziative di economia circolare, riutilizzo e ricondizionamento degli apparati e dei dispositivi.

Trasversalmente ai diversi ambiti di rischio, il Gruppo monitora l'evoluzione delle esposizioni e dei target climatici attraverso specifici KPI e ne integra progressivamente le risultanze nei processi decisionali, industriali e finanziari.



7. Riconoscimento e gestione dei rischi emergenti

In continuità con l'analisi dei rischi più rilevanti, il processo di Enterprise Risk Management considera anche i rischi emergenti, con l'obiettivo di intercettare fenomeni nuovi o in evoluzione che possono determinare conseguenze significative per il Gruppo nel medio-lungo termine (3–5 anni).

In linea con il modello del World Economic Forum, tali rischi sono caratterizzati da un elevato grado di incertezza, da una difficile quantificazione e dalla capacità di produrre cambiamenti significativi nel contesto in cui il Gruppo opera.

Rischi connessi all'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. TIM utilizza l'AI nei propri processi e sviluppa e commercializza soluzioni basate su queste tecnologie, con l'obiettivo di generare efficienze operative, innovare l'offerta e rispondere all'evoluzione delle esigenze dei clienti.

Alla crescita delle opportunità connesse all'AI si accompagna tuttavia l'emergere di nuovi rischi, legati sia alla capacità di sviluppare e integrare efficacemente queste tecnologie sia al loro utilizzo responsabile, sicuro e conforme alla normativa.

I principali fattori di rischio riguardano:

- la conformità al quadro normativo, con particolare riferimento all'AI Act, nonché alla normativa in materia di protezione dei dati personali, proprietà intellettuale e copyright;
- la sicurezza, la qualità e l'integrità dei dati e dei sistemi, inclusi i rischi di cybersecurity, le possibili violazioni della privacy e la necessità di assicurare affidabilità dei risultati e prevenzione di bias e discriminazioni algoritmiche;
- la capacità tecnologica e organizzativa di sviluppare e integrare le soluzioni AI, in termini di disponibilità di competenze specialistiche, interoperabilità con i sistemi esistenti, adeguatezza delle infrastrutture e disponibilità degli approvvigionamenti tecnologici;



- la sostenibilità economica degli investimenti, anche in relazione alla disponibilità delle risorse necessarie, alla capacità di conseguire i benefici attesi e ai costi di sviluppo, gestione e adeguamento delle soluzioni;
- la trasparenza e l'affidabilità nell'utilizzo dell'AI, necessarie a preservare la fiducia di clienti, dipendenti, fornitori e altri stakeholder.

Il verificarsi di tali rischi può determinare impatti economici, legali e reputazionali per il Gruppo. Particolare rilevanza assume il rischio di non conformità normativa: la violazione di specifiche disposizioni dell'AI Act può comportare sanzioni fino al 7% del fatturato mondiale annuo per l'uso di sistemi AI vietati e fino al 3% per il mancato rispetto di determinati requisiti applicabili ai sistemi ad alto rischio.

A ciò si aggiunge il rischio economico di non conseguire i benefici attesi dagli investimenti in AI, a causa di ricavi o risparmi inferiori alle previsioni o di costi di sviluppo, gestione e adeguamento delle soluzioni superiori a quelli attesi.

Per gestire e mitigare tali rischi, TIM adotta un presidio centralizzato dell'AI, supportato da un team multifunzionale che coinvolge competenze di Strategia, Finanza, Compliance, Legale, Sicurezza e altre funzioni aziendali, con l'obiettivo di assicurare una gestione integrata lungo l'intero ciclo di vita dei sistemi AI.

Il modello di gestione prevede in particolare:

- un quadro di governance, policy e responsabilità definite, volto a disciplinare l'utilizzo responsabile dell'AI e a promuovere una cultura diffusa di consapevolezza sui relativi rischi;
- la mappatura e classificazione dei sistemi AI, attraverso un inventario aggiornato dei modelli e delle soluzioni in uso e strumenti di classificazione del rischio coerenti con le categorie e i requisiti previsti dall'AI Act;
- un processo strutturato di gestione del rischio lungo l'intero ciclo di vita delle soluzioni, dalla progettazione allo sviluppo, test e rilascio, secondo i principi di ethics by design, privacy by design e security by design;



- attività di monitoraggio e controllo successive al rilascio, che prevedono supervisione umana, verifica periodica delle prestazioni e individuazione e correzione tempestiva di eventuali anomalie o bias.

Tale approccio è finalizzato a garantire uno sviluppo e un utilizzo dell'AI sicuri, affidabili e conformi alla normativa, tutelando al contempo le persone, i dati e i processi aziendali.

Rischi informatici e di sicurezza

Il rischio informatico è connesso alla crescente dipendenza del Gruppo da tecnologie digitali, infrastrutture IT e servizi cloud, che determina una maggiore esposizione a minacce cyber sempre più complesse. Tale esposizione può essere ulteriormente accentuata dall'evoluzione del contesto geopolitico e normativo, con potenziali conseguenze sulla continuità dei servizi, sulla sicurezza dei dati e sul profilo economico e reputazionale del Gruppo.

Anche l'evoluzione della regolamentazione europea, tra cui la Direttiva NIS2 e le ulteriori iniziative in materia di cybersecurity, rafforza i requisiti di sicurezza e resilienza applicabili al settore delle telecomunicazioni e i conseguenti obblighi di compliance.

Le principali conseguenze associate al rischio riguardano:

- l'indisponibilità o il degrado di asset, infrastrutture e servizi ICT, anche per effetto di interruzioni delle infrastrutture regionali o di instabilità delle regioni cloud, con particolare riferimento alle aree maggiormente esposte a tensioni geopolitiche, come l'area MENA; (Middle East and North Africa);
- la compromissione della sicurezza e della riservatezza dei dati, con conseguente esposizione a sanzioni in caso di Data Breach o di mancata conformità alla normativa applicabile, inclusa la NIS2;
- conseguenze economiche e reputazionali e perdita di fiducia da parte dei clienti, in particolare istituzionali e strategici, anche in caso di attacchi informatici connessi a tensioni geopolitiche.



Nel 2025 non si sono verificati incidenti di sicurezza ICT con impatto livello di gravità medio o alto; si sono registrati, invece, cinque incidenti rilevanti, il cui impatto le cui conseguenze sono state contenute dalle contromisure in essere, senza effetti finanziari significativi nel periodo.

La gestione del rischio informatico si basa su un sistema integrato di prevenzione, monitoraggio, risposta e continuità operativa, che comprende:

- la valutazione e quantificazione del rischio, attraverso penetration testing, vulnerability assessment e utilizzo della metodologia FAIR (Factor Analysis of Information Risk) per la stima delle potenziali conseguenze economiche dei rischi cyber;
- il monitoraggio e la risposta alle minacce, attraverso un Security Operations Center (SOC) attivo 24/7 e sistemi di protezione e crittografia dei dati sensibili;
- la resilienza e la continuità operativa, supportate dalle certificazioni ISO 22301 e ISO 27001, dalle policy di Data Recovery e dalla protezione di backup non esposti a reti pubbliche, nonché dall'integrazione dei processi della supply chain nelle politiche di business continuity;
- il presidio della compliance normativa, assicurato dalla funzione Compliance in coordinamento con le funzioni coinvolte nei processi digitali.

Tali presidi consentono al Gruppo di monitorare l'evoluzione delle minacce, rafforzare la capacità di prevenzione e risposta e contenere le potenziali conseguenze operative, economiche e reputazionali associate agli eventi di sicurezza informatica.

Rischi legati alla catena della fornitura

L'instabilità geopolitica e le tensioni tra i principali sistemi economici possono determinare criticità lungo la catena di fornitura, aumentando la pressione sui costi dell'energia, dei materiali e della manodopera e sulla disponibilità delle risorse necessarie alle attività del Gruppo.

Sebbene allo stato attuale non si registrino conseguenze dirette sul business del Gruppo TIM, anche in considerazione della limitata presenza operativa nelle aree interessate dai conflitti, un ulteriore deterioramento dello scenario geopolitico potrebbe produrre effetti indiretti sulla catena di fornitura e determinare un incremento dei costi sostenuti dal Gruppo.



Le principali conseguenze considerate riguardano:

- l'aumento dei costi energetici: con riferimento all'esposizione economica complessiva del Gruppo, a marzo 2026 il potenziale incremento dei costi per il 2026 riconducibile al conflitto tra Stati Uniti e Iran è stato stimato tra 3 e 5 milioni di euro, considerando la posizione aperta e la colocation e al netto dei consumi di Noovle indicizzati al PUN;
- possibili interruzioni o criticità della catena di approvvigionamento, con conseguenti pressioni sulla disponibilità e sui costi dei fattori produttivi;
- incremento dei costi dei materiali e della manodopera.

Per monitorare e contenere l'esposizione a tali rischi, il Gruppo adotta un insieme di misure che comprendono:

- la valutazione periodica della strategia di approvvigionamento energetico, con il coinvolgimento delle funzioni Finanza e Procurement;
- il monitoraggio trimestrale dell'EBITDA@Risk rispetto al Piano Industriale, al fine di valutare le potenziali conseguenze economiche derivanti dall'evoluzione dello scenario;
- l'utilizzo di modelli di ottimizzazione vincolata e di regressione statistica per stimare la possibile evoluzione dei costi dei materiali e della manodopera e supportare la definizione delle strategie di approvvigionamento, anche attraverso acquisti anticipati o contratti di maggiore durata.