Posteitaliane

POSTE ITALIANE

Risk Management | Approfondimenti

Posteitaliane

Risk Governance

LA GOVERNANCE SUI RISCHI DI GRUPPO

Al fine di garantire una corretta ed efficace identificazione e gestione dei rischi di Gruppo, Poste Italiane ha definito una specifica governance in ambito rischi, come di seguito rappresentata:

Consiglio di Amministrazione (CdA)

Tra i principali compiti, con il supporto del CCR, definisce e approva le linee di indirizzo del SCIGR in coerenza con le strategie della Società, in modo che i principali rischi afferenti il Gruppo risultino correttamente identificati, nonché adeguatamente misurati, gestiti e monitorati; determina la natura e il livello di tali rischi ritenuto compatibile con gli obiettivi strategici individuati e verifica almeno annualmente l'adeguatezza del SCIGR

Amministratore Delegato

È incaricato dell'istituzione e del mantenimento del Sistema di Controllo Interno e Gestione dei Rischi (SCIGR) e fornisce pareri/supporto agli altri attori coinvolti nell'organizzazione del SCIGR

Comitato Controllo e Rischi (CCR)[1]

Comitato endoconsiliare che ha il compito di assistere, con adeguate attività istruttorie, di natura propositiva e consultiva, le valutazioni e le decisioni del Consiglio di Amministrazione relative al sistema di controllo interno e di gestione dei rischi. Il Comitato riporta al CdA almeno ogni sei mesi, fornendo aggiornamenti in merito all'attività svolta nonché sull'adeguatezza del sistema di controllo interno e di gestione dei rischi

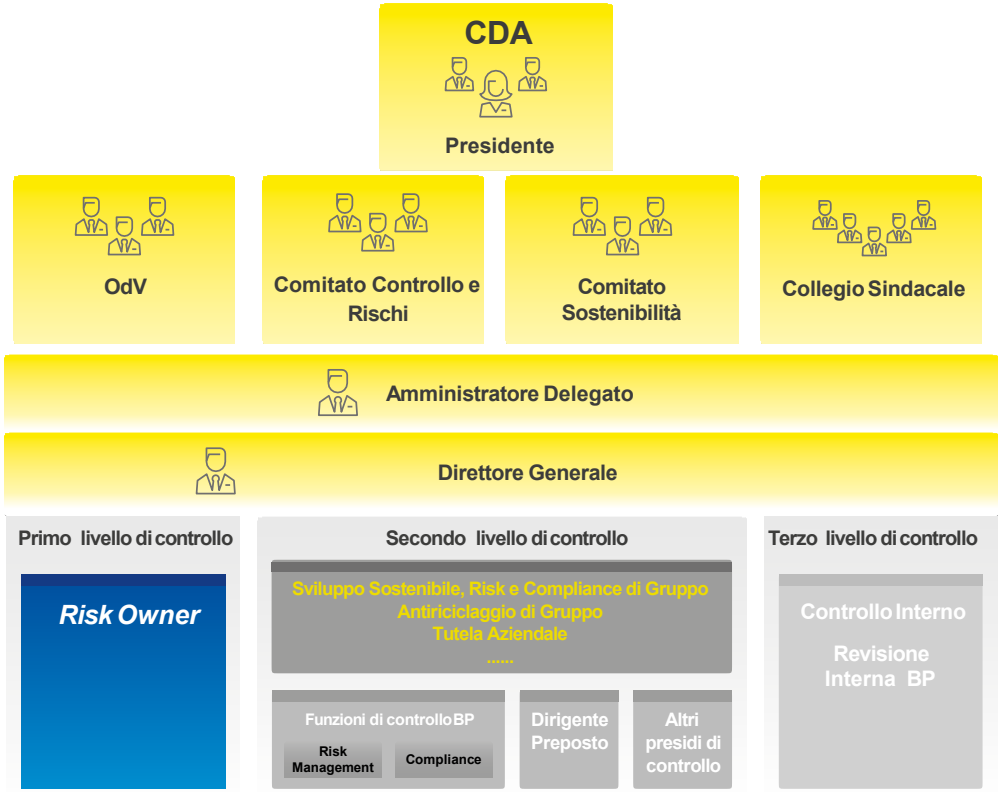
Chief Risk & Sustainability Officer[1]

Il Chief Risk & Sustainability Officer, a capo della funzione Sviluppo Sostenibilie, Risk e Compliance di Gruppo (SSRCG), che riporta al Direttore Generale dell'Azienda, rappresenta la persona con la più alta responsabilità operativa per la gestione e supervisione dei rischi del Gruppo, compresi quelli ESG (es. diritti umani, discriminazioni, violenza di ogni genere incluso sexual harassment, labour rights e organizzazioni sindacali, salute e sicurezza, privacy, etica e corruzione, ambiente - incluso il cambiamento climatico, cybersecurity, inclusione finanziaria, ecc.). Tra gli altri, costituisce, a livello di Gruppo, il presidio di riferimento unico per il governo e la gestione di tutti i rischi, servendosi, a tal fine, del contributo delle unità specialistiche a suo diretto riporto e degli altri presidi di rischio presenti in Poste Italiane e nelle Società del Gruppo. In particolare, presenta trimestralmente al Top Management e al CCR un report di monitoraggio integrato dei rischi e annualmente agli Organi Sociali (CdA e CCR) la «Relazione Rischi e Compliance»

[1] Il Chief Risk & Sustainability Officer, responsabile della struttura SSRCG, insieme al Comitato Controllo e Rischi, rappresentano la figura e l'organo con le maggiori responsabilità operative in materia di gestione dei rischi di Gruppo, compresi quelli ESG (es. *climate change*, salute e sicurezza sul lavoro, *cybersecurity*, *privacy*, diritti umani, inclusione finanziaria, ecc.).

FOCUS RISK GOVERNANCE FRAMEWORK | MODELLO DELLE TRE LINEE DI DIFESA

Il Gruppo Poste Italiane, al fine di assicurare un'appropriata gestione dei rischi aziendali, ha definito un governance framework di Risk Management strutturato secondo il modello delle Tre Linee di Difesa (COSO Framework), sintetizzato di seguito. Per ulteriori dettagli, si rimanda alle Linee Guida sul Sistema di Controllo Interno e di Gestione dei Rischi (SCIGR) del Gruppo.



Governo
(Organi)

Definisce, approva e verifica il Sistema di Controllo Interno e Gestione dei Rischi

I livello di controllo
(management/funzioni di linea/ operative)

Identifica, monitora e valuta i rischi operativi, in relazione ai quali definisce e attua azioni di mitigazione specifiche, occupandosi anche di coadiuvare l'esecuzione dei controlli stabiliti dalla seconda linea.

Questo ruolo operativo è ricoperto dai cosiddetti Risk, che sono responsabili di specifici rischi e gestiscono gli stessi.

II livello di controllo
(funzioni di controllo/ monitoraggio dei rischi)

Definisce le metodologie di misurazione del rischio e propone le linee guida sui relativi sistemi di controllo; identifica, valuta e monitora i rischi aziendali, verificando l'adeguatezza degli stessi sistemi di controllo al fine di assicurare l'efficienza e l'efficacia delle operazioni, una prudente conduzione del business, l'affidabilità delle informazioni, la conformità a leggi, regolamenti e procedure interne.

Le funzioni preposte a tali controlli, che riportano al Comitato Controllo e Rischi, sono autonome, indipendenti e distinte da quelle operative.

III livello di controllo
(funzioni di Internal Audit)

Fornisce assurance indipendente sull'adeguatezza ed effettiva operatività del primo e secondo livello di controllo e, in generale, sul SCIGR.

Ha la finalità di valutare la completezza, l'adeguatezza, la funzionalità e l'affidabilità in termini di efficienza ed efficacia del sistema dei controlli interni, nonché di individuare violazioni delle procedure e delle norme applicabili a Poste Italiane.

Le funzioni preposte a tali controlli riportano direttamente al CDA.

Posteitaliane

Risk Review | Focus

LE CATEGORIE DI RISCHIO IDENTIFICATE DAL GRUPPO

Di seguito si riportano le principali categorie di rischio connesse alle attività del Gruppo Poste Italiane, come individuate nel Risk Model[1] di Gruppo.

CATEGORIA	STRATEGICI	OPERATIVI	NON CONFORMITÀ ALLE NORME	REPUTAZIONALI	ESG	FINANZIARI E ASSICURATIVI
DESCRIZIONE	Rischi che possono influire sul raggiungimento degli obiettivi fissati nel Piano Strategico	Rischi di subire perdite derivanti dall'inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni a livello di Gruppo, oppure da eventi esogeni	Rischi di violazione di norme o regolamenti esistenti o connessi all'introduzione di nuove norme o regolamenti che hanno rilevanza generale ovvero specifica nei settori di attività del Gruppo Poste Italiane	Rischi che possono derivare da una percezione negativa da parte degli stakeholder del Gruppo, per i quali il framework adottato prevede l'attivazione di un intervento di analisi e di gestione al fine di intercettare e valutare le fonti di rischio	Rischi derivanti da fattori riconducibili a problematiche ambientali, sociali e di governance (in particolare, collegati ai diritti umani, ai cambiamenti climatici e alla finanza sostenibile)	Rischi finanziari che sono regolamentati e vigilati dalle Autorità (Banca d'Italia e IVASS) e presidiati dalle strutture di Risk Management dei rispettivi settori, coordinati dal referente unico in ambito Sviluppo Sostenibile, Risk e Compliance di Gruppo

[1] Il Gruppo valuta la propria esposizione al rischio con cadenza trimestrale.

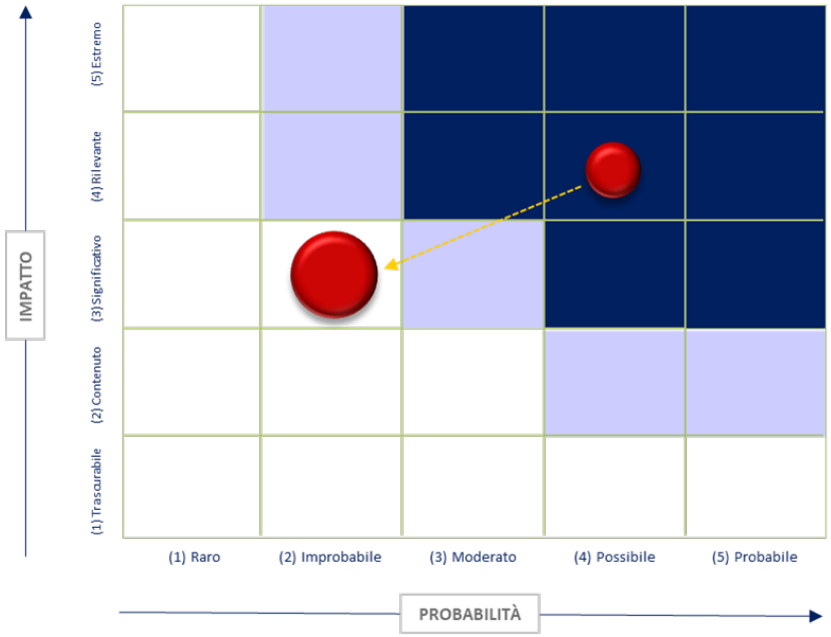
La funzione «Controllo Interno» annualmente sottopone ad audit interno il Sistema di Controllo Interno e Gestione dei Rischi (SCIGR) del Gruppo, predisponendo una Relazione di Valutazione sullo stesso Sistema che viene, successivamente, approvata dal Board. La Relazione ha la finalità di esprimere una valutazione complessiva del SCIGR in modalità di «Positive Assurance». Inoltre, la conformità del sistema di gestione del rischio di Poste Italiane è verificata annualmente anche attraverso audit esterni condotti da enti terzi nell'ambito delle attività di verifica dei processi di certificazione e ricertificazione ISO 37301, e nell'ambito delle ulteriori attività di verifica attuate per mantenere/ottenere le numerose certificazioni ISO conseguite dal Gruppo.

VALUTAZIONE DEI RISCHI

Per ogni rischio identificato, il Gruppo determina il livello di rischiosità sotto un duplice profilo:

- il profilo di **Rischio Inerente**, determinato considerando la componente di rischio intrinseca alla natura stessa della specifica Attività, non tenendo conto dell'esistenza e della effettiva operatività delle azioni di trattamento del rischio in essere;
- il profilo di **Rischio Residuo**, ottenuto considerando il livello di intensità delle azioni di trattamento[1].

La valutazione complessiva del rischio residuo permette la prioritizzazione dei rischi ed è rappresentata all'interno di una heatmap (matrice probabilità-impatto), come di seguito raffigurata a titolo esemplificativo:



LEGENDA

Probabilità:

(1) Raro; (2) Improbabile; (3) Moderato; (4) Possibile; (5) Probabile;

Impatto:

(1) Trascurabile; (2) Contenuto; (3) Significativo; (4) Rilevante; (5) Estremo.

In base al posizionamento su tale matrice, è possibile classificare i rischi secondo le seguenti aree di rilevanza:

- Tier 1 (area blu scuro);
- Tier 2 (area blu chiaro);
- Tier 3 (area bianca).

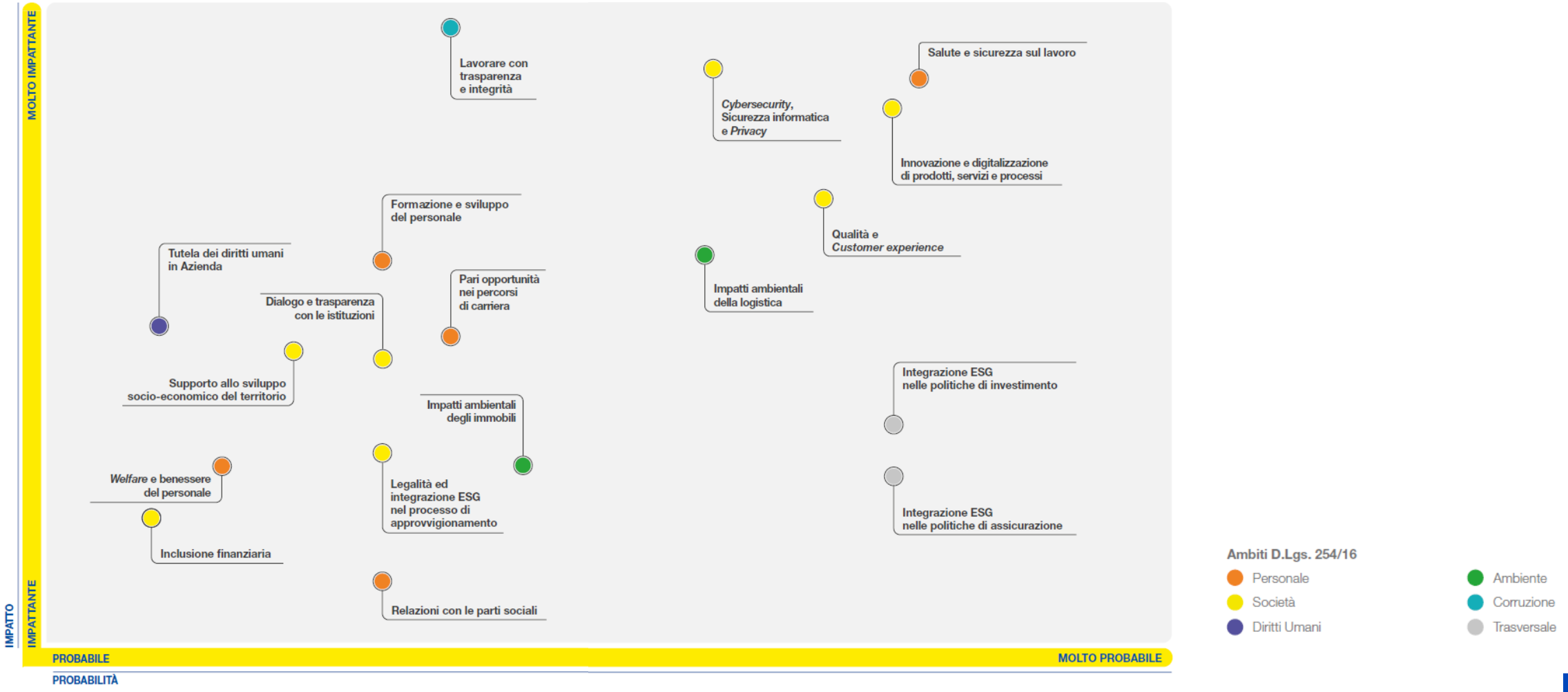
I rischi che rientrano nel "Tier 1" e "Tier 2" vengono definiti "Top risk".

[1] Il livello di intensità delle azioni di trattamento da mettere in campo viene valutato anche prendendo in considerazione la conduzione di analisi di scenario (stress test), sia su alcune tipologie di rischi finanziari che di rischi non finanziari (ad esempio, rischi legati al climate change, alle tematiche di anti-corruzione, rischi legati alla sicurezza informatica, ecc.).

FOCUS | LA MATRICE DI RISCHIO DEL GRUPPO POSTE ITALIANE

Company-specific risk exposure

Di seguito è rappresentata la matrice del Gruppo Poste Italiane che descrive la *company-specific risk exposure*, in considerazione della probabilità e la magnitudo associata ad ogni rischio.



ESEMPI DI AZIONI DI MITIGAZIONE E CULTURA DEL RISCHIO AZIENDALE

ESEMPI DI AZIONI DI MITIGAZIONE

CYBERSECURITY, IT SECURITY E PRIVACY	Il Gruppo Poste Italiane, al fine di mitigare i rischi collegati alla cybersecurity e alla privacy, si è dotata di opportuni processi di valutazione del rischio e di misure precauzionali. Di seguito, si riportano le principali azioni di mitigazione messe in atto: • verifiche tecniche di sicurezza preventive svolte su tre applicativi: Vulnerability Assessment, Code Review statica e dinamica e Penetretion Test • ottenimento/mantenimento delle certificazioni ISO 27001 e 20001 • definizione e implementazione di un piano di continuità operativa aziendale che identifica i sistemi informativi maggiormente critici, delle potenziali minacce e delle contromisure da adottare • adozione del Framework Privacy che garantisce il rispetto degli obblighi di monitoraggio dei principali processi di business • introduzione di una Policy sulla Privacy a cui seguono degli audit che garantiscono la conformità alla stessa
IMPATTI AMBIENTALI DEGLI IMMOBILI	Il Gruppo Poste Italiane, al fine di mitigare i rischi collegati agli impatti ambientali dei propri immobili, si è dotata di opportuni processi di valutazione del rischio e di misure precauzionali. Di seguito, si riportano le principali azioni di mitigazione messe in atto: • utilizzo di energia elettrica proveniente da fonte rinnovabile (99% dell'energia elettrica acquistata dal Gruppo proviene da fonti 100% rinnovabili, certificate Garanzie di Origine) • adozione di un Sistema di Gestione Ambientale certificato ISO 14001 • realizzazione di 1.400 impianti fotovoltaici entro il 2026 al fine di coprire il 15% del fabbisogno energetico dell'Azienda • prosecuzione del Progetto *Smart Building* al fine di realizzare un sistema di gestione in termini di *Building and Energy Management System* (*BEMS*) • avvio del progetto di decarbonizzazione al fine di sostituire su circa 100 siti le caldaie a gas con le pompe di calore • utilizzo delle *smart technologies*, installando impianti di illuminazione a tecnologia LED

CULTURA DEL RISCHIO AZIENDALE

Al fine di assicurare un'adeguata diffusione dei principi di gestione del rischio adottati all'interno della Società, il Gruppo Poste Italiane ha avviato una serie di iniziative specifiche, quali:

- iniziative di formazione verticale sui principi di gestione del rischio per la popolazione aziendale, come quelli relativi ai principi di gestione dei rischi ESG identificati come rilevanti per il Gruppo Poste Italiane. L'impegno della funzione SSRCG comprende la realizzazione di corsi di formazione specifici sulla gestione del rischio e sulla conformità normativa. Nel 2023, infatti, il Gruppo ha erogato circa 6,5 milioni di ore di formazione, comprendendo corsi utili a promuovere un'efficace cultura del rischio. Ad titolo esemplificativo e non esaustivo, al fine di promuovere consapevolezza sui temi della corruzione e della salute e sicurezza, l'Azienda prevede formazione obbligatoria continua attraverso corsi sia e-learning che in aula su questi temi;
- formazione periodica del Consiglio di Amministrazione sui rischi aziendali, sulle iniziative avviate a riguardo per la loro mitigazione e rispetto alle attività di monitoraggio;
- le funzioni competenti si confrontano con la funzione di risk management per la valutazione preliminare dei rischi derivanti dalla definizione del nuovo prodotto, per la valutazione della sostenibilità finanziaria associata all'iniziativa in corso di sviluppo e per la definizione di un business case al fine di garantire che i rischi derivanti dallo sviluppo del nuovo prodotto/servizio siano coerenti con la propensione al rischio dell'Azienda;
- integrazione nell'ambito dei sistemi di incentivazione finanziaria (MBO e ILT) di metriche legate alla gestione dei rischi di Gruppo, come quelle relative agli aspetti di sostenibilità considerati come rilevanti (es. transizione green, progetti strategici ESG, qualità PCL, valorizzazione delle persone, ecc.). Questi ultimi sono integrati con l'obiettivo di potenziare ulteriormente la gestione dei rischi legati a queste tematiche. Inoltre, il Gruppo Poste Italiane tiene in considerazione anche il parametro di redditività corretta per il rischio utilizzato da BancoPosta.

FOCUS | RISK APPETITE FRAMEWORK

Obiettivi

Il Consiglio di Amministrazione, in base al Codice di Corporate Governance, previo parere del Comitato Controllo e Rischi, definisce la natura e il livello di rischio compatibile con gli obiettivi strategici, tenendo conto dei diversi fattori di rischio tra cui quelli esogeni (es. l'evoluzione del contesto macro-economico)

Risk Appetite Framework - Obiettivi

Assicurare che il **business del Gruppo**, nella sua articolazione in entità, **si sviluppi entro i livelli di rischio accettabile e tollerabile** stabiliti dal Consiglio di Amministrazione

Garantire la sostenibilità degli obiettivi strategici rispetto al profilo di rischio assunto, a fronte delle diverse tipologie di rischio

Declinare il profilo di rischio di Gruppo sostenibile con riferimento all'anno successivo rispettando le aspettative degli stakeholder e/o i requisiti regolamentari applicabili

Coordinare e integrare i presidi delle entità sottoposte a Vigilanza che definiscono i propri **RAF individuali** approvati dai rispettivi CdA

A livello di Gruppo, a valle del processo di *risk assessment* strategico, accanto agli indicatori relativi ai top risk individuati viene incluso un set di indicatori, con rispettive soglie, relativi ai rischi il cui andamento è influenzato principalmente dall'**evoluzione del contesto macro-economico**. Tali indicatori sintetizzano peraltro anche i rischi finanziari e assicurativi più rilevanti per il Gruppo Poste Italiane.

Gli **Indicatori di Gruppo** sono oggetto di **approvazione da parte del CdA** e di monitoraggio trimestrale, gli esiti del quale sono rappresentati al CCR. Relativamente agli indicatori di **Dividendo**, **Liquidità** e **Struttura Finanziaria**, **Performance Economica** sono sottoposti all'approvazione del CDA anche le relative soglie.

Nella determinazione di tali soglie vengono recepite le previsioni di budget e vengono individuati dei limiti di protezione, al superamento dei quali è prevista un'informativa agli Organi Aziendali preposti e, a livello delle singole entità del Gruppo, un processo di escalation finalizzato all'individuazione e valutazione di eventuali azioni manageriali correttive atte a ripristinare la traiettoria originaria.

FOCUS | RISK APPETITE FRAMEWORK

Processo di Risk Appetite Framework

Al fine di rafforzare ulteriormente il grado di integrazione con i RAF individuali, sia per quanto riguarda gli indicatori che i criteri di definizione delle rispettive soglie, il continuativo percorso di integrazione nella gestione dei rischi vede il coordinamento tra tutte le strutture di Risk Management operanti nell'ambito del Gruppo Poste Italiane. In particolare, il RAF di Gruppo è oggetto di condivisione anche con i Risk Manager delle singole entità vigilate:

Processo di Risk Appetite Framework

I — ANALISI OBIETTIVI E RISCHI - processo Risk Assessment

Nell'ambito del **processo di *Risk Assessment***, analisi dei principali obiettivi aziendali, a partire da quelli di piano, e **individuazione dei rischi rilevanti** per il Gruppo

II — DEFINIZIONE DEL RISCHIO RESIDUO ACCETTABILE

Definizione di **livelli di accettabilità e tolleranza** per i principali rischi e individuazione di **indicatori quali-quantitativi di monitoraggio** e **azioni di trattamento**

III — APPROVAZIONE IN CDA

Approvazione del *framework* RAF che esprime il **grado di compatibilità** dei rischi con una gestione dell'impresa coerente con gli obiettivi strategici individuati

IV — MONITORAGGIO e REPORTING

Monitoraggio periodico del profilo di rischio nel tempo attraverso l'analisi dell'andamento degli indicatori e delle azioni di trattamento

Owner

Si specifica che i **Risk Owner** sono i soggetti **responsabili** dei **rischi specifici** e sono chiamati a **gestire** gli stessi.

SSRCG	**SSRCG con il supporto dei *Risk Owner* e dei *Risk Specialist***	**CdA, previo parere CCR**	**SSRCG**