Politica di gestione dei rischi

Obiettivo

Minimizzare gli eventi di rischio che possono causare impatti avversi sull'organizzazione e i suoi Stakeholder.

Responsabili

Ruolo	Responsabilità specifica nell'ambito della politica
Comitato Etico	Approva la politica di gestione dei rischi, il risk appetite dell'Agenzia e ne verifica l'efficacia complessiva nell'ambito del Rapporto Etico annuale.
Risk Owner / Responsabile Gestione Rischi	Coordina il processo di identificazione, valutazione e trattamento dei rischi; mantiene il Registro dei Rischi (Risk Register) aggiornato.
Funzione di Sorveglianza	Effettua una verifica indipendente sull'adeguatezza del sistema di gestione dei rischi e sulla sua effettiva applicazione operativa.
Compliance Officer (CO)	Garantisce l'integrazione dei rischi normativi e di compliance (inclusi quelli da conflitto di interesse e da esternalizzazione) nel framework complessivo.
Responsabili di Funzione / Process Owner	Identificano e segnalano i rischi specifici del proprio ambito operativo e attuano le misure di trattamento assegnate.

Elementi

- Definire e implementare un approccio integrato per la gestione del rischio secondo i principi e il processo descritti dalla norma ISO 31000:2018, adattato alle attività della Società
- Definire il contesto interno ed esterno, degli obiettivi aziendali e del risk appetite/risk tolerance approvati dal Comitato Etico, come riferimento per la valutazione dei rischi.
- Definire e aggiornare un Risk Register per l'identificazione dei rischi rilevanti per la Società: strategico, governance, indipendenza, conflitto di interessi, sociale, ambientale, di salute e sicurezza dei lavoratori, etica aziendale, metodologico (accuratezza e coerenza dei rating), reputazionale, normativo/regolamentare, operativo e tecnologico (inclusa la sicurezza dei dati), e esternalizzazione/fornitori terzi.
- Valutare i rischi in termini di probabilità e impatto, con conseguente prioritizzazione e mappatura su una matrice di rischio (heat map), mantenuta nel Registro dei Rischi nella società e lungo la catena del valore,
- Trattare i rischi attraverso misure di mitigazione, trasferimento o accettazione consapevole, con assegnazione di un Risk Owner responsabile per ciascun rischio rilevante e con piani d'azione tracciati.
- Monitoraggio e riesame continuo dell'efficacia delle misure di trattamento, con aggiornamento del Registro dei Rischi almeno semestrale e immediato in presenza di eventi rilevanti (incidenti, modifiche normative).
- Comunicazione e consultazione tra le funzioni aziendali, il Comitato Etico e la Funzione di Sorveglianza, inclusa l'integrazione con il processo di due diligence RBC e il registro dei conflitti di interesse (cfr. Politica 1).
- Integrazione della gestione dei rischi nei processi decisionali strategici e operativi, incluse le decisioni relative a nuove attività, nuovi clienti, nuovi fornitori terzi e modifiche metodologiche sostanziali.

Indicatori Chiave di Prestazione (KPI)

Indicatore (KPI)	Modalità di calcolo / fonte
% rischi del Registro con piano di trattamento attivo	Rischi con piano e owner / Totale rischi mappati
N° rischi critici non mitigati entro i termini previsti	Verifica su Registro dei Rischi e piani d'azione
N° eventi di rischio materializzati non identificati prima	Analisi post-evento (lessons learned)
Adeguatezza delle risorse finanziarie allocate per mitigare il livello di esposizione ai rischi	Registro rischi e budget

Riferimenti

Regolamento (UE) 2024/3005: *Art. 15 (requisiti organizzativi); Art. 25 (solidi meccanismi di governance); Art. 21 (rischi da esternalizzazione)*

Linee Guida OCSE per la Condotta d'Impresa Responsabile (RBC): *Cap. II (Principi generali — diligenza dovuta basata sul rischio); approccio risk-based trasversale a tutte le Linee Guida OCSE*