

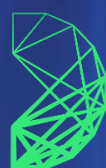
ARTICOLO

Model Governance e Internal Audit: l'assessment del rischio modello

Settembre 2026

Stefano Romano

Senior Partner



prometeia

ABSTRACT

Modelli statistici, algoritmi e sistemi di intelligenza artificiale sono sempre più integrati nei processi decisionali aziendali, dal pricing al forecasting, dalla fraud detection alla pianificazione e all'allocazione delle risorse.

*La crescente dipendenza delle decisioni dai modelli determina tuttavia un'esposizione al **model risk**, inteso come rischio di conseguenze negative derivanti da errori metodologici, dati inadeguati, deterioramento delle performance o utilizzi non coerenti con le finalità originarie.*

Tali effetti possono tradursi in perdite economiche, inefficienze operative, violazioni normative e danni reputazionali.

*La **Model Governance** assume pertanto rilevanza crescente nell'ambito del sistema di governance, risk management e controllo, richiedendo all'Internal Audit di integrare il model risk nel proprio perimetro di assurance.*

1. Modelli e rischio modello

La crescente disponibilità di dati, l'evoluzione delle capacità computazionali e la diffusione di machine learning e intelligenza artificiale hanno reso i modelli una componente strutturale di numerosi processi aziendali.

Un **modello** può essere definito come una rappresentazione semplificata di un fenomeno reale che, attraverso dati di input, assunzioni, metodologie e relazioni quantitative o algoritmiche, produce output finalizzati alla misurazione, previsione, classificazione o supporto di decisioni.

Rientrano pertanto in tale perimetro strumenti eterogenei: modelli di forecasting e pricing, sistemi di scoring, modelli di rischio, algoritmi antifrode, recommendation engine, modelli di manutenzione predittiva, machine learning e applicazioni di intelligenza artificiale.

La natura stessa del modello implica necessariamente un certo grado di approssimazione. L'affidabilità dei relativi output dipende dalla qualità e rappresentatività dei dati, dalla robustezza metodologica, dalla validità delle assunzioni e dalla stabilità delle relazioni sottostanti nel tempo.

Il **model risk** deriva dalla possibilità che output non corretti o non sufficientemente robusti, oppure l'utilizzo improprio di output corretti, determinino conseguenze negative per l'organizzazione.

Le principali fonti di rischio possono essere ricondotte a errori di specificazione o implementazione, dati incompleti o non rappresentativi, assunzioni non più valide, deterioramento delle performance, modifiche non adeguatamente governate e utilizzi del modello al di fuori del relativo perimetro di applicabilità.

Con l'introduzione di sistemi di machine learning e AI assumono inoltre crescente rilevanza rischi legati a bias, explainability, model drift, robustezza, data governance, dipendenza da terze parti e tracciabilità degli output.

Il model risk non costituisce pertanto un rischio esclusivamente metodologico: attraverso le decisioni supportate dai modelli si trasferisce direttamente al profilo di rischio dell'organizzazione.

Errori sistematici possono determinare riduzione dei margini, errata allocazione delle risorse, inefficienze operative, perdite finanziarie, decisioni commerciali inappropriate, contenziosi o violazioni normative.

A tali effetti si aggiunge il **rischio reputazionale**, particolarmente rilevante quando gli output incidono direttamente su clienti, dipendenti o altri stakeholder.

L'automazione amplifica ulteriormente tale esposizione: un errore incorporato in un modello può essere applicato sistematicamente a un elevato numero di decisioni prima di essere identificato. **Scalabilità e capacità di propagazione dell'errore rappresentano quindi caratteristiche distintive del model risk.**

2. Model Governance e gestione del rischio

La risposta organizzativa al model risk è rappresentata dalla **Model Governance**, intesa come l'insieme di ruoli, responsabilità, processi, metodologie e controlli attraverso cui l'organizzazione governa i modelli **lungo l'intero ciclo di vita**.

Un framework strutturato dovrebbe innanzitutto assicurare la completa identificazione del perimetro attraverso un **model inventory** che includa, secondo criteri definiti, modelli tradizionali, algoritmi, soluzioni sviluppate internamente o da terze parti e sistemi AI.

Il secondo elemento è rappresentato dalla classificazione dei modelli secondo un approccio **risk-based**. Il **tiering** (ossia l'indice sintetico di rischio/materialità del modello) dovrebbe considerare almeno materialità economica, rilevanza delle decisioni supportate, complessità metodologica, livello di automazione, rilevanza dei dati trattati e potenziale impatto su clienti e stakeholder. A livelli differenti di rischio devono corrispondere requisiti di governance e controllo proporzionati.

Il framework deve quindi presidiare l'intero **model lifecycle**, dalla fase di sviluppo fino all'eventuale dismissione. Tra gli elementi essenziali rientrano ownership e accountability formalizzate, standard di sviluppo e documentazione, validazione indipendente, change management, performance monitoring, definizione di soglie e limiti, gestione delle anomalie, escalation e reporting.

Particolare rilevanza assume la **validazione indipendente**, che dovrebbe fornire una challenge rispetto alla *conceptual soundness* del modello, alla qualità dei dati, alla correttezza dell'implementazione e alle performance osservate, mantenendo un livello di profondità proporzionato alla materialità del modello.

La Model Governance rappresenta pertanto non soltanto un presidio tecnico, ma una componente del più ampio sistema di **governance delle decisioni "model-driven"**.

3. Il ruolo dell'Internal Audit

La crescente materialità del model risk rende la Model Governance un ambito di interesse diretto per l'Internal Audit.

I **Global Internal Audit Standards** dell'IIA richiedono alle funzioni di Internal Audit di valutare l'efficacia dei processi di governance, risk management e controllo e di assicurare che la pianificazione sia coerente con il profilo di rischio e con la sua evoluzione.

In tale contesto, il model risk dovrebbe essere integrato nel **risk assessment dell'Internal Audit** quando i modelli assumono rilevanza rispetto ai processi e agli obiettivi aziendali.

L'assurance non dovrebbe limitarsi alla verifica metodologica del singolo modello, ma considerare l'adeguatezza complessiva del framework: completezza dell'inventario, criteri di tiering, segregazione dei ruoli, indipendenza della validazione, qualità del monitoring, gestione delle modifiche, reporting e capacità di intercettare tempestivamente il deterioramento delle performance.

Per i sistemi di intelligenza artificiale tale prospettiva trova un ulteriore riferimento nell'**AI Act – Regolamento (UE) 2024/1689**, che introduce, in particolare per i sistemi AI classificati ad alto rischio, requisiti relativi a risk management, data governance, documentazione e tracciabilità, human oversight, accuratezza, robustezza e cybersecurity.

La progressiva estensione dell'utilizzo dei modelli richiede quindi anche un'evoluzione delle competenze dell'Internal Audit, attraverso una maggiore integrazione tra conoscenza dei processi, risk management, data analytics e competenze quantitative. Come già avvenuto per ICT, cybersecurity e data governance, il model risk è destinato a evolvere da ambito specialistico a **dimensione trasversale del sistema di assurance**.

Conclusioni

La crescente dipendenza dei processi aziendali da modelli quantitativi, algoritmi e sistemi AI modifica strutturalmente il profilo di rischio delle organizzazioni.

Il **model risk è un rischio rilevante**: errori metodologici, dati inadeguati, performance non monitorate o utilizzi impropri possono propagarsi attraverso i processi decisionali producendo conseguenze economiche, operative, normative e reputazionali. L'automazione aumenta ulteriormente tale esposizione, amplificando velocità e scala di propagazione degli errori.

La Model Governance deve quindi essere considerata una componente del sistema complessivo di governance, risk management e controllo. Per l'Internal Audit ciò implica l'integrazione del model risk nel risk assessment e, nei contesti caratterizzati da elevata dipendenza dai modelli, la capacità di fornire assurance sull'adeguatezza dell'intero framework di governance e del model lifecycle.



Linkedin: **prometeia**

YouTube: **prometeia**

Instagram: **prometeiagroup**

www.prometeia.com