

AI Risk Register

RISK REGISTER

Meridian Advisory Partners (fictional) · Sample Deliverable — Prado AI Solutions

July 2026

About This Register

This register documents identified AI-related risks across Meridian Advisory Partners. Each risk is rated by **Likelihood** (1–5) and **Impact** (1–5); the **Risk Score** is their product. Risks scoring 15 or above are High priority; 8–14 are Medium; below 8 are Low. This register is reviewed quarterly and updated when new tools, workflows, or incidents occur.

ID	Category	Risk Description	Like-li hood	Impact	Score	Rating	Recommend ed Actions	Owner
R-001	Data Privacy	Client PII and financial data entered into consumer-grade AI tools (e.g., ChatGPT free tier) with no data processing agreement in place.	4	5	20	HIGH	Restrict client/regulated data entry to enterprise-tier tools with signed DPAs; publish approved-tools list immediately.	COO
R-002	Data Privacy	Applicant SSN fragments and financial data processed in underwriting AI notes outside approved, controlled systems.	4	5	20	HIGH	Move underwriting AI workflow to an enterprise tool with a signed DPA; implement mandatory human review before saving.	Head of Underwriting
R-003	Output Quality	AI-assisted client communications and analysis delivered without a documented human-review step, risking accuracy or compliance errors.	3	4	12	MEDIUM	Define and document human-review requirements by output type; train all client-facing staff.	Practice Leads

ID	Category	Risk Description	Like-li hood	Impact	Score	Rating	Recommend ed Actions	Owner
R-00 4	Vendor Risk	New AI tools adopted without evaluating data retention, training-use, or security terms, creating undisclosed vendor risk.	4	3	12	MEDIUM	Implement a lightweight AI vendor evaluation checklist; require approval before any new tool is used for business purposes.	IT / Compliance
R-00 5	Incident Response	No defined incident-reporting path specific to AI use; a data exposure through an AI tool could go unreported or be handled inconsistently.	3	4	12	MEDIUM	Add AI-specific scenarios to incident response playbook; communicate reporting path to all staff.	Compliance
R-00 6	Governance	No single executive accountable for AI use firm-wide; governance gaps persist because ownership is unclear.	3	3	9	MEDIUM	Assign a named AI governance owner; define business-unit AI owner roles.	CEO
R-00 7	Operational	Employees using AI tools not on any approved list, creating unknown exposure across tool types and use cases.	5	3	15	HIGH	Publish approved-tools list; require staff to submit requests for any tool not on the list before use.	COO / IT
R-00 8	Compliance	No AI Acceptable Use Policy in place; staff have no formal guidance on permitted or prohibited AI use.	5	3	15	HIGH	Draft, approve, and distribute AI AUP; require written acknowledgment from all staff within 30 days.	Compliance

ID	Category	Risk Description	Like-li hood	Impact	Score	Rating	Recommend ed Actions	Owner
R-009	Training	Staff have not received AI governance training; risk of inadvertent misuse is elevated.	4	2	8	MEDIUM	Deliver firm-wide AI governance training session; include AI use guidance in new-hire onboarding.	HR / Compliance
R-010	Operational	No use-case documentation for active AI workflows; inability to audit, replicate, or assess impact of AI-assisted work.	3	2	6	LOW	Document each active AI use case (purpose, data inputs, review steps, owner) in a use-case inventory.	Business Unit Owners

Risk Rating Key

Rating	Score Range	Definition
HIGH	15–25	Requires immediate action; escalate to leadership.
MEDIUM	8–14	Address within 30–60 days; assign owner and target date.
LOW	1–7	Monitor; address in next quarterly review cycle.

This risk register is a sample deliverable prepared by Prado AI Solutions. "Meridian Advisory Partners" and all data above are fictional and for illustration only. This document does not constitute legal, regulatory, or cybersecurity advice.