

AI Governance Readiness Checklist

CHECKLIST

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

July 2026

How to Use This Checklist

Rate each item as **Yes**, **Partial**, or **No**. Items rated No or Partial in Framework Areas 1–4 represent your highest-priority governance gaps. This checklist is typically completed during the AI Risk & Efficiency Diagnostic and reviewed quarterly thereafter.

1. Ownership & Accountability

Control Statement	Yes	Partial	No	Owner / Notes
A named executive is accountable for AI use and governance firm-wide.	■	■	■	
Each business unit has a designated AI owner responsible for approved use cases.	■	■	■	
Roles and responsibilities for AI oversight are documented.	■	■	■	
An escalation path exists for AI-related concerns or incidents.	■	■	■	

2. Approved Tools & Vendor Management

Control Statement	Yes	Partial	No	Owner / Notes
A current list of approved AI tools is published and accessible to all staff.	■	■	■	
A formal process exists to evaluate and approve new AI tools before adoption.	■	■	■	
Data processing agreements (DPAs) are in place with all AI vendors handling client or regulated data.	■	■	■	
Vendor AI training-use and data-retention terms have been reviewed and documented.	■	■	■	
A process exists to remove or restrict tools when vendor terms change.	■	■	■	

3. Data Handling Rules

Control Statement	Yes	Partial	No	Owner / Notes
Written guidance defines what data categories may and may not be entered into AI tools.	☒	☒	☒	
Staff are aware of restrictions on entering client PII, financial data, or regulated information into AI tools.	☒	☒	☒	
Data classification levels are mapped to permitted AI tool tiers (consumer vs. enterprise).	☒	☒	☒	
A process exists to handle accidental data entry into an unapproved tool.	☒	☒	☒	

4. Human Review Requirements

Control Statement	Yes	Partial	No	Owner / Notes
AI-assisted outputs used in client-facing work are subject to a documented human-review step.	☒	☒	☒	
Review requirements are defined by output type (e.g., draft communications, analysis, recommendations).	☒	☒	☒	
Reviewers understand what to check and are not simply approving AI output without evaluation.	☒	☒	☒	
AI-generated content is disclosed to clients or regulators where required.	☒	☒	☒	

5. Training & Awareness

Control Statement	Yes	Partial	No	Owner / Notes
All staff have received at least one AI governance training session in the past 12 months.	☒	☒	☒	
New-hire onboarding includes AI acceptable-use guidance.	☒	☒	☒	
Training covers both permitted uses and prohibited actions (e.g., entering client data into ChatGPT).	☒	☒	☒	
Staff know how to report an AI-related concern or potential data exposure.	☒	☒	☒	

6. Risk Register & Monitoring

Control Statement	Yes	Partial	No	Owner / Notes
An AI risk register exists and is reviewed at least quarterly.	■	■	■	
New AI use cases are added to the risk register before deployment.	■	■	■	
Risk ratings are updated when tool terms, workflows, or data types change.	■	■	■	
A process exists to track and close open risk register items.	■	■	■	

7. Incident Response

Control Statement	Yes	Partial	No	Owner / Notes
An AI-specific incident response path is defined (separate from general IT incidents if needed).	■	■	■	
Staff know how to report a suspected AI-related data exposure or misuse.	■	■	■	
Post-incident reviews include an AI governance component when applicable.	■	■	■	
Incidents are logged and used to update the risk register and training materials.	■	■	■	

8. Policy & Documentation

Control Statement	Yes	Partial	No	Owner / Notes
An AI Acceptable Use Policy (AUP) is in place, current, and acknowledged by all staff.	■	■	■	
The AUP is reviewed and updated at least annually or when significant new tools are adopted.	■	■	■	
Use-case documentation exists for each approved AI workflow (purpose, data inputs, review steps, owner).	■	■	■	
Governance documentation is stored in a location accessible to auditors and leadership.	■	■	■	

9. Continuous Improvement

Control Statement	Yes	Partial	No	Owner / Notes
A quarterly governance review is scheduled to assess new tools, risks, and policy gaps.	☐	☐	☐	
Lessons from incidents and near-misses are incorporated into training and policy.	☐	☐	☐	
AI governance maturity is tracked over time against a defined baseline.	☐	☐	☐	
Leadership receives a periodic summary of AI governance status and open items.	☐	☐	☐	

This checklist 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.