AI Risk Diagnostic

Fellowship Intelligence

AI governance and control-layer advisory

Client: [Redacted – Financial Services Firm]
Date: April 2026
Prepared by: Fellowship Intelligence

---

1. Executive Summary

The organization is currently utilizing AI across multiple areas of its operations, including internal analysis, reporting, and workflow support. Based on structured evaluation, the organization is operating with a **high level of AI-related risk exposure**.

AI usage is occurring in the following areas:

- Internal analysis and reporting
- Client-related documentation and communication support
- Operational workflow assistance
- AI usage appears active across internal reporting, client-facing, and operational functions, with adoption occurring at the team level without centralized coordination

At present, there is **no formal governance framework aligned to AI usage**, and existing controls do not appear to extend to AI-specific risks. This creates exposure related to:

- Handling of sensitive financial and client information within AI systems
- AI influence on outputs that may impact client-facing or regulated activities

Overall Risk Score: 68 / 100
Risk Tier: High

Recommendation:
Assurance Assessment Required

---

2. AI Usage Overview

AI is currently being used within the organization in the following functional areas:

Primary Use Cases

- Internal reporting and analysis — **Embedded**
- Client-related documentation and support — **Moderate to Embedded**
- Operational workflow assistance — **Moderate**

General Observations

- Usage appears **partially structured but not governed at a policy level**
- AI is being used for **analysis, documentation, and workflow efficiency**
- Leadership visibility is **partial**, but not systematically enforced
- Use intersects with **client-sensitive and potentially regulated information environments**

---

3. Risk Scoring Summary

Total Score: 68 / 100

Risk Tier:

- High (50+)

Category Breakdown

Category	Score (0–20)
Data Exposure Risk	17
Decision Impact Risk	14

Workflow Dependence	12
Governance & Policy Gaps	15
Visibility & Accountability Gaps	10

---

4. Key Risk Exposures

1. **Handling of Sensitive Financial and Client Data**
   AI systems may be processing client-related or financial information without defined restrictions, creating potential compliance and confidentiality exposure.
2. **AI Influence on Client-Impacting Outputs**
   AI is contributing to documentation and analysis that may influence client interactions or decisions without standardized review protocols.
3. **Absence of AI-Specific Governance Layer**
   Existing operational controls do not appear to extend to AI usage, resulting in a gap between current practices and expected control environments.
4. **Partial Visibility and Control Coverage**
   Leadership awareness exists but is not supported by structured monitoring, ownership, or enforcement mechanisms.
5. **Embedded Use Across Operational Workflows**
   AI is becoming integrated into recurring workflows, increasing reliance without corresponding governance alignment.

---

5. Immediate Priority Actions

The following actions are recommended to reduce immediate exposure:

- Establish clear visibility into AI usage across all functions
- Restrict use of sensitive financial or client data in AI systems until standards are defined

- Require review of AI-assisted outputs used in client-facing or decision-related contexts
- Define initial expectations for acceptable AI use aligned to existing control environments

Note: These actions are intended to reduce immediate exposure and do not constitute a complete governance solution.

This document reflects an assessment of governance-layer exposure and does not constitute legal advice. Organizations with regulatory, privacy, or enforcement obligations should consult qualified legal counsel.

---

6. Recommended Next Step

Assurance Assessment Required

Rationale

AI is being used within workflows that intersect with client data and potentially regulated activities. The absence of an AI-specific governance layer creates a gap between current usage and expected control standards. A structured assessment is required to align AI usage with appropriate governance expectations.

A structured Assurance Assessment will:

- Provide a formal evaluation of AI-related risk and material exposure across client-facing and regulated workflows
- Define required governance controls based on actual usage and the organization's operational environment
- Establish a clear path to implementing a controlled AI usage framework

---

7. Closing Statement

This Diagnostic provides an initial view into AI usage and associated risk exposure. It is designed to establish visibility and support decision-making regarding next steps.

Further evaluation is required to define appropriate governance structures and controls aligned to the organization’s operational and regulatory environment.

Fellowship Intelligence is an AI governance and control-layer advisory firm. The AI Risk Diagnostic is the first stage in a structured engagement pathway: it establishes an initial view of AI usage, identifies risk exposure, and determines whether a formal assessment is warranted. The Assurance Assessment evaluates that exposure in depth and produces a defined governance framework aligned to the organization's operational environment; Implementation installs it — the policy layer, workflow controls, ownership structure, and oversight mechanisms required to operate AI with accountability and consistency. Continuity provides the ongoing monitoring, auditing, and governance maintenance required to sustain that framework as AI usage evolves.