AI Risk Diagnostic

Fellowship Intelligence

AI governance and control-layer advisory

Client: [Redacted – Fleet Operations Company]
Date: April 2026
Prepared by: Fellowship Intelligence

---

1. Executive Summary

The organization is currently utilizing AI across multiple operational areas, including sales prospecting, internal operations management, and technical troubleshooting. Based on structured evaluation, the company is operating with a **high level of AI-related risk exposure**.

AI usage is occurring in the following areas:

- Sales prospecting and outbound client communication
- Internal operations and fleet management
- Technical troubleshooting and service support
- AI usage appears distributed across the sales, operations, and service teams, driven by individual adoption without centralized direction or defined ownership

At present, there is **no formal governance, policy structure, or oversight mechanism** governing AI usage. This creates exposure related to:

- Uncontrolled handling of sensitive client and pricing data
- AI influence over operational and commercial decision-making without defined review standards

Overall Risk Score: 70 / 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

- Sales prospecting and outbound communication — **Embedded**
- Operations and fleet performance management — **Embedded**
- Service troubleshooting and research — **Moderate**

General Observations

- Usage appears **decentralized and informal**, driven by individual operators
- AI is being used for **communication, operational analysis, and decision support**
- Leadership visibility into usage is **limited and non-structured**
- Adoption is expanding organically without defined boundaries

---

3. Risk Scoring Summary

Total Score: 70 / 100

Risk Tier:

- High (50+)

Category Breakdown

Category	Score (0–20)
Data Exposure Risk	17

Decision Impact Risk	15
Workflow Dependence	11
Governance & Policy Gaps	19
Visibility & Accountability Gaps	8

---

4. Key Risk Exposures

1. **Uncontrolled Sensitive Data Exposure**
   Client information, pricing details, and operational data are likely being entered into AI tools without restrictions or oversight, creating potential confidentiality and contractual risk.
2. **AI Influence on Commercial and Operational Decisions**
   AI is being used to support pricing, vendor-related decisions, and operational management without defined review standards or accountability structures.
3. **Absence of Governance Framework**
   There are no policies, approved usage boundaries, or formal controls governing AI usage, resulting in inconsistent and unmanaged behavior across the organization.
4. **Decentralized and Unmonitored Usage**
   AI adoption is occurring at the individual level without centralized visibility, limiting leadership's ability to assess exposure or enforce standards.
5. **Expanding Workflow Reliance Without Controls**
   AI is becoming embedded in sales, operations, and service workflows, increasing operational dependence without corresponding governance mechanisms.

---

5. Immediate Priority Actions

The following actions are recommended to reduce immediate exposure:

- Establish basic visibility into where and how AI is being used across all teams
- Restrict entry of sensitive, client, and pricing data into AI tools until clear standards are defined
- Require review of AI-generated outputs used in external communication or decision-making
- Define initial expectations for acceptable AI usage across the organization

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

The organization is operating with high exposure across multiple risk categories, including data handling, decision influence, and governance absence. AI is embedded in core workflows without defined controls, making it impossible to safely scale or standardize usage without a structured assessment.

A structured Assurance Assessment will:

- Provide a formal evaluation of AI-related risk and exposure across sales, operations, and service workflows
- Define required governance controls based on confirmed usage patterns and operational dependencies
- 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 operations.

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.