AI Risk Diagnostic

Fellowship Intelligence

AI governance and control-layer advisory

Client: [Redacted – Homeowners Association]
Date: April 2026
Prepared by: Fellowship Intelligence

---

1. Executive Summary

The organization is currently utilizing AI within its private security operations to monitor vehicle speed, review gate-related incidents, and analyze overall security activity. 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:

- Speed monitoring and enforcement within the community
- Gate access monitoring and incident review
- Security operations analysis and reporting
- Usage appears concentrated within the security operations function, with AI integrated into daily monitoring and enforcement workflows

At present, there is **no formal governance structure or policy framework** governing AI usage in these functions. This creates exposure related to:

- Use of AI in environments involving resident data and potential surveillance
- AI influence on enforcement actions and incident interpretation without defined oversight

Overall Risk Score: 76 / 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

- Speed monitoring and violation detection — **Embedded**
- Gate monitoring and incident analysis — **Embedded**
- Security operations reporting and pattern analysis — **Moderate to Embedded**

General Observations

- Usage appears **operationally embedded within security workflows**
- AI is being used for **monitoring, analysis, and enforcement support**
- Leadership visibility into how AI outputs are generated and used is **limited**
- Use involves **resident-facing environments with potential sensitivity and liability exposure**

---

3. Risk Scoring Summary

Total Score: 76 / 100

Risk Tier:

- High (50+)

Category Breakdown

Category	Score (0–20)
Data Exposure Risk	18

Decision Impact Risk	17
Workflow Dependence	14
Governance & Policy Gaps	19
Visibility & Accountability Gaps	8

---

4. Key Risk Exposures

1. **Sensitive Resident and Surveillance Data Exposure**
   AI systems are likely processing video, access logs, and resident-related data without defined restrictions or handling standards, creating privacy and liability exposure.
2. **AI Influence on Enforcement and Incident Interpretation**
   AI outputs may influence decisions related to speed violations, access incidents, or security responses without formal review standards or accountability structures.
3. **Absence of Governance in a Liability-Sensitive Environment**
   There are no policies, usage boundaries, or governance controls in place despite AI being used in areas with potential legal, reputational, and resident impact.
4. **Embedded Use in Security-Critical Workflows**
   AI is integrated into core security operations, increasing reliance on outputs that are not governed or validated through structured controls.
5. **Limited Oversight and Accountability Structure**
   Leadership does not have consistent visibility into how AI is used or how outputs are validated, and there is no clearly defined ownership of AI oversight.

---

5. Immediate Priority Actions

The following actions are recommended to reduce immediate exposure:

- Establish clear visibility into all AI systems used within security operations
- Restrict processing of resident-identifiable or sensitive data until handling standards are defined
- Require human review for any AI-supported enforcement or incident-related decisions
- Define initial expectations for acceptable AI use within security workflows

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 security and enforcement-related workflows that directly affect residents and carry potential legal and reputational implications. The absence of governance, combined with embedded operational use, creates material exposure that cannot be addressed without a structured evaluation.

A structured Assurance Assessment will:

- Provide a formal evaluation of AI-related risk and exposure within the organization's security and enforcement workflows
- Define required governance controls based on actual usage and the sensitivity of the operating 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 within the organization’s security operations. 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.