

OWLSCOR REPORT — PULSE #1 BASELINE

Acme Legal LLP

Assessed September 2, 2026 · Tier 1 — Self-Attested

Posture snapshot from intake as of September 2, 2026, 10:14 AM CDT. Mapped to NIST AI RMF 1.0. TRAIGA overlay: ON. Not an audit. Not a legal opinion. Evidence tier: Tier 1 — Self-Attested. This snapshot is evidence of posture at a point in time, not an ongoing guarantee.

OVERALL OWLSCOR 57.0 Watch	GRADE C	QUESTIONS ANSWERED 30 of 30 (26 core + 4 overlay)
---	-------------------	--

Category Breakdown

Category	Score	Band
A AI System Inventory & Classification	84.0	On Track
B Governance & Accountability	28.0	Critical Gap
C Data Provenance & Quality	70.0	Developing
D Vendor / Third-Party AI Dependency	40.0	Watch
E Bias, Explainability & Human Oversight	40.0	Watch
F Monitoring, Incident Response & Continuous Improvement	80.0	On Track

Top Findings

Every finding below ties to a specific question answered in the intake — not a generic checklist item.

HIGH Governance & Accountability

Leadership and the board do not receive recurring AI risk reporting, limiting executive visibility into the risk. (Assessed maturity: no documented posture)

→ Add AI risk metrics to a recurring leadership/board reporting cadence.

HIGH Governance & Accountability

No AI Risk Owner or governance committee has been formally designated. (Assessed maturity: aware but undocumented)

→ Formally designate an AI Risk Owner or governance committee with documented authority and scope.

HIGH Vendor / Third-Party AI Dependency

No documented fallback or exit plan exists if a critical AI vendor changes terms or discontinues support. (Assessed maturity: aware but undocumented)

→ Document a fallback/exit plan for critical AI vendors, including alternate providers or in-house contingencies.

HIGH Bias, Explainability & Human Oversight

No override or appeal mechanism is available when AI recommendations affect individuals. (Assessed maturity: aware but undocumented)

→ Stand up an override/appeal mechanism for individuals affected by consequential AI-driven decisions.

MED Governance & Accountability

No written AI Acceptable Use Policy exists, leaving employee AI use ungoverned by default. (Assessed maturity: partially documented)

→ Draft and distribute an AI Acceptable Use Policy covering approved tools, prohibited uses, and escalation paths.

MED Governance & Accountability

Roles and responsibilities for AI risk management are not documented or reviewed on a defined cadence. (Assessed maturity: partially documented)

→ Document AI risk roles/responsibilities and put them on an annual (at minimum) review cycle.

SWOT

STRENGTHS > AI System Inventory & Classification — On Track posture (84/100). > Monitoring, Incident Response & Continuous Improvement — On Track posture (80/100).	WEAKNESSES > Governance & Accountability — Critical Gap (28/100). > Vendor / Third-Party AI Dependency — Watch (40/100). > Bias, Explainability & Human Oversight — Watch (40/100).
OPPORTUNITIES > Governance & Accountability gap: closing this is the fastest lever to move the overall score and reduce audit/regulator exposure. > Vendor / Third-Party AI Dependency gap: closing this is the fastest lever to move the overall score and reduce audit/regulator exposure. > Bias, Explainability & Human Oversight gap: closing this is the fastest lever to move the overall score and reduce audit/regulator exposure.	THREATS > NIST AI RMF and TRAIGA enforcement expectations are still maturing — undocumented governance today becomes a harder gap to close once enforcement guidance solidifies. > Weak governance/accountability posture increases exposure if a regulator, insurer, or plaintiff's counsel asks who owns AI risk internally. > Unconfirmed vendor AI governance creates dependency risk outside direct control.

Migration / Remediation Roadmap

Phase 1 — Immediate (0–3 months)

- Add AI risk metrics to a recurring leadership/board reporting cadence.
- Formally designate an AI Risk Owner or governance committee with documented authority and scope.
- Document a fallback/exit plan for critical AI vendors, including alternate providers or in-house contingencies.
- Stand up an override/appeal mechanism for individuals affected by consequential AI-driven decisions.

Phase 2 — Near-Term (3–9 months)

- Draft and distribute an AI Acceptable Use Policy covering approved tools, prohibited uses, and escalation paths.
- Document AI risk roles/responsibilities and put them on an annual (at minimum) review cycle.
- Define an escalation path for high-risk AI use cases, including who reviews and who can approve or block deployment.
- Formally request written AI governance and risk documentation from all critical AI vendors (model providers, SaaS AI tools).
- Track AI vendor commitments, limitations, and renewal dates in a maintained vendor risk register.
- Run a disparate-impact/fairness evaluation on every high-risk AI system before and periodically after deployment.
- Document, at a level a regulator or auditor could follow, how each material AI system generates its outputs.

Phase 3 — Ongoing (9+ months)

- Run a shadow-AI discovery pass (network/SaaS logs, procurement records) and bring findings into the formal inventory.

Overlay Readiness — Legal / TRAIGA

Score: 45.0 / 100 — Watch

HIGH Assessment findings have not been mapped to the NIST AI RMF affirmative-defense / substantial-compliance pathway.

→ [Map current findings to the NIST AI RMF pathway TRAIGA recognizes for affirmative defense / substantial compliance.](#)

MED AI use cases have not been assessed against TRAIGA's prohibited-use categories.

→ [Screen all AI use cases against TRAIGA's prohibited-use categories \(intentional manipulation toward harm, unlawful discrimination, etc.\).](#)

LOW No documented process classifies AI deployments under TRAIGA's developer-vs-deployer applicability criteria.

→ [Document a classification process for each AI deployment under TRAIGA's developer/deployer framework.](#)

LOW Client- or public-facing TRAIGA disclosure language is not ready, if applicable (government contractor / healthcare entity).

→ [Draft TRAIGA-compliant disclosure language in advance if the organization is a government contractor or healthcare entity.](#)

Maps to: Texas TRAIGA, NIST AI RMF 1.0 (Govern/Map/Measure/Manage), sector disclosure duties