AI Risk & Readiness Assessment

Use this **AI Risk & Readiness Assessment** template to evaluate the suitability and risk profile of an AI tool or vendor. It's structured as a checklist with Yes/No/Unknown options and can be used during procurement, security review, or internal compliance evaluation. This assessment is meant to guide your evaluation of AI tools, and **you should not rely solely on this assessment** in making decisions about the use of AI tools. Instead, consider your circumstances and apply your independent judgment to determining when and how to use a particular AI tool in your practice.

(Simple) AI Assessment for Law Firm Use

Date: _____
Reviewed by: _____
AI Tool or Vendor Name: _____

Section 1: Use Context

1.1. Will this AI system be used for legal research, drafting, or analysis?
☐ Yes ☐ No ☐ Unknown

1.2. Will this tool process or have access to client or case-specific data?
☐ Yes ☐ No ☐ Unknown

1.3. Will the output be used in court filings, regulatory submissions, or client deliverables?
☐ Yes ☐ No ☐ Unknown

Section 2: Confidentiality & Data Handling

2.1. Can the vendor confirm that firm or client data will not be used for training or model improvement?
☐ Yes ☐ No ☐ Unknown

2.2. Does the system allow local/private deployment or otherwise guarantee data isolation?
☐ Yes ☐ No ☐ Unknown

2.3. Are data encryption (in transit and at rest) and access controls in place?
☐ Yes ☐ No ☐ Unknown

2.4. Does the vendor agree to return or securely delete data upon request or contract termination?
☐ Yes ☐ No ☐ Unknown

Section 3: Security & Risk Controls

3.1. Has the vendor completed a security audit or penetration test in the last 12 months?
☐ Yes ☐ No ☐ Unknown

3.2. Are controls in place to prevent prompt injection, jailbreaks, or adversarial misuse?
☐ Yes ☐ No ☐ Unknown

3.3. Does the vendor notify customers of any data breach or incident within 24–72 hours?
☐ Yes ☐ No ☐ Unknown

Section 4: Accuracy & Responsible Use

4.1. Has the AI system been tested for legal accuracy, bias, and reliability?
☐ Yes ☐ No ☐ Unknown

4.2. Are disclaimers or safeguards provided when outputs may be incomplete, fabricated, or misleading?
☐ Yes ☐ No ☐ Unknown

4.3. Is there documentation or a white paper available on how the model works and its limitations?
☐ Yes ☐ No ☐ Unknown

Section 5: Compliance & Alignment with Legal Ethics

5.1. Is the vendor aware of and willing to support the firm's obligations to protect attorney-client privilege and confidentiality?
☐ Yes ☐ No ☐ Unknown

5.2. Can the vendor contractually commit to legal-sector-specific standards (e.g., ABA guidance, HIPAA, GDPR)?
☐ Yes ☐ No ☐ Unknown

5.3. Does the tool avoid impersonating a human (e.g., no AI legal avatars without disclosure)?
☐ Yes ☐ No ☐ Unknown

Preliminary Risk Rating

Total "Yes" Responses	**Suggested Risk Tier**
12–15	**Low Risk** – Proceed to legal/procurement review
8–11	**Moderate Risk** – Review needed; consider contract controls
0–7	**High Risk** – Likely unsuitable for confidential or regulated matters

---

Notes or Follow-Ups