AI Vendor Evaluation Guide for Ethical & Legal Compliance

A Due-Diligence Framework for Law Firms & In-House Counsel

Executive Summary

This guide equips law firms and in-house counsel to evaluate AI vendors—particularly those providing research, drafting, billing, or trust-account tools—through the lens of legal ethics and risk management.

It translates ABA Model Rules 1.1 (Competence), 1.6 (Confidentiality of Information), 1.15 (Safekeeping Property), and 5.1 / 5.3 (Supervision) into practical due-diligence questions. The goal: adopt AI responsibly, protect client data, and preserve professional accountability.

1. Vet the Vendor's Data Practices (Rules 1.1, 1.6, 1.15)

Why it matters: Ethical compliance and data security are fundamental to client trust.

Key Questions

- **Data Storage & Access:** Where is client data hosted? Who can access it (vendor staff, subcontractors, or third parties)?
- **Privacy Compliance:** Does the vendor comply with GDPR, CCPA, or similar laws? Can they show evidence (e.g., SOC 2 or ISO 27701 certification)?
- **Data Use for Training:** Is client data used to train or fine-tune AI models? If so, is it anonymized and can you opt out?
- **Financial Data Handling:** If the tool records or reconciles client funds or trust-account activity, does it maintain segregation and audit trails consistent with Rule 1.15 – Safekeeping Property?

Example: "Does your platform log trust-account transactions in compliance with Rule 1.15's record-keeping requirements?"

Risk if Ignored: Potential ethical violations or disciplinary exposure from mishandling client or trust data.

2. Define Liability and Supervision Boundaries (Rules 1.1, 1.15, 5.1, 5.3)

Why it matters: Lawyers remain responsible for work done or assisted by technology.

Key Questions

- **Error Responsibility:** Who bears liability for AI-generated errors (e.g., mis-cited authority, trust-report inaccuracies)?
- **Indemnification:** Does the vendor contract protect your firm against harm caused by AI malfunctions?
- **Supervision of Vendors:** How will you meet supervisory duties under Rules 5.1 and 5.3 for nonlawyer service providers and technology systems?
- **Error Support:** Does the vendor provide timely assistance to correct compliance-related issues?

Example: A compliance manager documents how vendor supervision and error response meet Rules 5.1 and 5.3.

Risk if Ignored: Malpractice exposure and lack of defensible oversight.

3. Demand Security and Confidentiality Safeguards (Rules 1.6 and 1.15)

Why it matters: Using third-party AI can compromise client confidentiality or privilege.

Key Questions

- **Encryption Standards:** Is data encrypted in transit and at rest (AES-256 minimum)?
- **Security Certifications:** Does the vendor hold ISO 27001, SOC 2, or equivalent credentials?
- **Confidentiality Protections:** Does the tool maintain client confidentiality under Rule 1.6 and minimize discoverability risk?
- **Financial Integrity:** For systems interacting with client funds, confirm secure segregation and reconciliation per Rule 1.15.

Example: An AI billing tool encrypts client-funds data to preserve confidentiality and 1.15 compliance.

Risk if Ignored: Breach of confidentiality or waiver of privilege in discovery.

4. Spot Red Flags Before You Sign

Why it matters: Hidden contract terms can transfer ethical and financial risk back to you.

Common Red Flags

- Vague or missing terms on data ownership, storage, or reuse.
- No transparency on model training sources or retention policies.
- Lack of compliance documentation for Rule 1.6 or 1.15 obligations.
- No provision for error-resolution support or third-party audits.

Example: Decline any vendor unable to demonstrate Rule 1.15 compliance for handling client-fund data.

Risk if Ignored: Contractual gaps that void your ability to enforce confidentiality or accuracy standards.

5. Follow a Documented Due-Diligence Workflow

Why it matters: A clear paper trail demonstrates competence and reasonable precautions.

Checklist

- **Request Documentation:** Privacy policies, security audits, and service terms.
- **Consult Experts:** Involve IT security and compliance counsel to verify claims.
- **Test with Non-Sensitive Data:** Pilot the tool with anonymized or dummy inputs.
- **Verify Financial Compliance:** Confirm Rule 1.15 segregation and audit accuracy for any trust-related modules.
- **Record Your Decision:** Keep internal notes detailing evaluation factors and risk mitigations.

Example: A legal-ops lead pilots an AI trust-account tool with sample data and documents test results before adoption.

Risk if Ignored: No defensible record of due diligence during audits or disciplinary review.

Quick-Check Table

Evaluation Area	Key Question	Proof Needed	Relevant Rule	Risk if Ignored
Data Storage	Where is data hosted?	SOC 2 / ISO 27001 report	1.6	Breach / discoverability
Model Training	Is client data reused?	Written opt-out confirmation	1.6	Confidentiality violation
Financial Integrity	Are client funds segregated?	Audit logs / Rule 1.15 records	1.15	Trust-account breach
Liability & Supervision	Who is accountable for errors?	Contract clauses / supervision plan	1.1, 5.1, 5.3	Malpractice exposure
Security	What encryption standard is used?	AES-256 proof / SOC 2 attestation	1.6	Unauthorized access

Resources:

- ABA Formal Opinion 512 (2024): Guidance on lawyer use of generative AI and supervisory duties.
- Firm IT and Compliance Teams: Evaluate vendor representations and security posture.
- CLE Resource: *AI Ethics & Risk Management for Lawyers* — a 2-hour accredited course with vendor-evaluation exercises.
  Enroll Now → getaiready.com/courses/ai-ethics-lawyers

Adopt AI responsibly and ethically.

This guide translates professional-conduct rules into an actionable vendor-evaluation workflow—helping legal teams embrace innovation while maintaining the standards of competence, confidentiality, and fiduciary care.