Legaltech Hub

AI Governance Checklist

This checklist can be used by firms to consider the AI governance issues they should be taking into account as they develop internal policies and security protocols around AI use.

**This list is not exhaustive as every organization will have different requirements. The below should help as a guide as to the types of questions you will want to consider as you procure and deploy AI solutions.*

1. Data Governance and Confidentiality

- Client confidentiality: Ensure AI tools do not retain or learn from privileged or sensitive information.
- Data residency and sovereignty: Verify where client data is stored and processed, especially in cross-border matters.
- Access controls: Limit who can input, view, and retrieve sensitive content from AI systems.
- Data leakage risks: Understand how models (especially third-party tools) handle input data, caching, and outputs.
- Data terms: Review terms of model providers and other relevant parties (e.g. Microsoft if deploying in Azure environment) to ensure compliance with data standards.

2. Model Selection and Customization

- Open vs. closed models: Evaluate trade-offs between transparency, control, and vendor risk.
- Fine-tuning vs. RAG: Consider whether the model is trained on firm-specific data or retrieves from it (retrieval-augmented generation).
- Model Agnosticism: Does the solution allow for swapping out of models when one becomes obsolete, another model is released, or to ensure the best model is used for the relevant purpose?
- Bias and accuracy: Assess for hallucinations and ensure outputs are reliable and verifiable in legal contexts. How is the vendor mitigating risk of hallucination?

3. Ethics and Professional Responsibility

- Compliance with legal ethics: Align with rules of professional conduct around competence, diligence, supervision, and candor.
- Transparency with clients: Decide whether (and how) to disclose use of AI in client matters.
- Unauthorized practice of law (UPL): Ensure AI use doesn't cross into activities requiring licensed human lawyers.

4. Human Oversight and Validation

- Review and supervision: Maintain a clear policy that all AI-generated outputs must be reviewed by qualified attorneys.
- Audit trails: Keep records of prompts and outputs for accountability and audit purposes.
- Feedback loops: Build mechanisms for human correction and iterative improvement.

5. Vendor and Technology Risk

- Due diligence on vendors: Assess security posture, indemnity, data handling practices, and ongoing model updates.
- Contractual safeguards: Include clauses around data ownership, IP rights, liability (including reliability on wrong answers), and uptime.
- Dependency risk: Avoid over-reliance on a single AI vendor or platform.
- Appropriate use: Consider your internal stance on appropriate use. Which platforms does your firm permit for legal research? What is the firm's position on access to public, browser-based models like ChatGPT?
- Agentic AI: If true agents (with some degree of autonomy) are deployed, ensure vendor offers transparency over reasoning so that users can see and agree to course of action before a workflow is commenced.

6. Security and Compliance

- SOC 2 / ISO 27001 compliance: Ensure tools meet basic security certification standards.
- Integration with existing systems: Prevent vulnerabilities by ensuring AI tools work securely within the firm's tech stack.
- Incident response planning: Prepare for security breaches or output-related liabilities.

7. Training and Change Management

- Lawyer education: Equip attorneys with skills to use and question AI effectively. Ensure this education is ongoing to accommodate evolution in technology.
- Training: Offer tool-specific training as you deploy solutions. Consider requiring training and education (including on topics of ethics and responsible use) prior to allowing access.
- Support functions: Include knowledge managers, librarians, and IT staff in rollout plans.
- Culture of responsible experimentation: Encourage use while establishing red lines.

8. Use Case Strategy and ROI

- Prioritize low-risk, high-impact use cases first: e.g., normalizing financial data, generating marketing content, producing internal summaries, KM retrieval.
- Avoid black-box automation of legal reasoning: Start with assistive and augmentative use, not replacement.
- Iterate based on feedback: Use data and lawyer experience to guide expansion.

9. Client Expectations and Market Signaling

- Client policies: Many clients are drafting AI use clauses—ensure alignment.
- Competitive positioning: Communicate firm capabilities without overpromising or misrepresenting AI sophistication.
- Fee structures: Consider how AI use affects pricing, billing, and efficiency claims.

10. Long-term Governance and Innovation

- AI governance committees: Establish cross-functional groups to guide responsible AI deployment.
- Policies and guidelines: Maintain a living document governing acceptable AI use.
- Monitoring developments: Stay ahead of regulatory, technical, and market changes (e.g., EU AI Act, U.S. state bar rulings).