JUPITER
CAPITAL MANAGEMENT

EXPERT ADVISORY & CONSULTING SERVICES

Legal Services - AI Risk

AI

AI risk management is critical in legal services because the stakes (client confidentiality, attorney client privilege, case outcomes, and professional liability) are exceptionally high; unchecked or poorly governed AI can produce inaccurate legal analysis, leak privileged information to third parties, introduce bias that harms clients, and create regulatory or ethical violations. Robust AI risk controls (data governance, human in the loop review, vendor due diligence, explainability, and incident response) preserve client trust, ensure compliance with professional duties and privacy laws, reduce malpractice exposure, and enable firms to harness AI's efficiency gains responsibly protecting both clients and the integrity of the legal system.

CONFIDENTIALITY & PRIVILEGE

Data classification: label privileged/ sensitive matter files and restrict AI access accordingly.
Data flows: map where client data goes (on prem, cloud, vendor models) and block high risk paths.
Technical controls: encryption (at rest/in transit), tokenization, DLP, and least privilege access.
Contractual safeguards: NDAs, confidentiality, and data-use limits with vendors.
Privilege protection policy: explicit prohibition or permitted use criteria for privileged content.
Logging & forensics: detailed access logs to demonstrate preservation of privilege.

UNAUTHORIZED PRACTICE OF LAW (UPL)

Role separation: enforce lawyer-only approval for legal advice outputs; restrict paralegal/non-lawyer use.
Output labeling: require disclaimers on AI-generated advice and that outputs are draft-only.
Supervision rules: mandatory lawyer review/attestation before client delivery or filings.
Workflow controls: gating mechanisms in tools to prevent unsupervised client-facing actions.
Training: staff education on UPL risks and when to escalate to licensed counsel.

ACCURACY & RELIABILITY

Source controls: mandate citation of authorities; preserve links to original sources.
Validation checks: verification steps (automated and human) for statutes, citations, facts, and dates.
Confidence indicators: require model confidence scores and thresholds for human review.
Testing: pre-deployment benchmarking against gold standard legal work and continuous validation.
Error handling: procedures to flag, correct, and document hallucinations or factual errors.

BIAS & FAIRNESS

Data review: analyze training and internal datasets for demographic or socioeconomic skew.
Impact testing: measure model outcomes across populations, case types, jurisdictions.
Mitigation techniques: reweighting, synthetic augmentation, or rule-based overrides for sensitive decisions.
Monitoring: continuous checks for differential performance or disparate impacts.
Governance: include fairness criteria in model acceptance and procurement decisions.

EXPLAINABILITY & AUDITABILITY

Model documentation: architecture, training data provenance, intended use, limitations, and performance.
Decision trails: retain inputs, prompts, intermediate outputs, and final decisions for each matter.
Explainability tools: human-readable rationales, citation mapping, and feature-importance summaries.
Audit access: establish who can review logs and models and under what circumstances (internal/external).
Retention policy: preserve records long enough to support audits, discovery, or regulatory inquiries.

www.jupiter-cap.com Email: rod.boothe@jupiter-cap.com

JUPITER
CAPITAL MANAGEMENT

EXPERT ADVISORY & CONSULTING SERVICES

Legal Services - AI Risk

AI

AI risk management is critical in legal services because the stakes (client confidentiality, attorney client privilege, case outcomes, and professional liability) are exceptionally high; unchecked or poorly governed AI can produce inaccurate legal analysis, leak privileged information to third parties, introduce bias that harms clients, and create regulatory or ethical violations. Robust AI risk controls (data governance, human in the loop review, vendor due diligence, explainability, and incident response) preserve client trust, ensure compliance with professional duties and privacy laws, reduce malpractice exposure, and enable firms to harness AI's efficiency gains responsibly protecting both clients and the integrity of the legal system.

DATA QUALITY & INTEGRITY

Source vetting: verify authoritative sources (court dockets, statutes, regulated databases).
Ingestion controls: validation rules, format normalization, and de-duplication during data intake.
Versioning: track document and dataset versions, timestamps, and change histories.
Provenance metadata: capture origin, custodianship, and processing steps for each data item.
Quality metrics: define and monitor completeness, accuracy, and freshness thresholds.

DATA PRIVACY & SECURITY

Privacy impact assessment: DPIAs for systems processing personal or sensitive client data.
Access controls: RBAC, MFA, and session management for AI tools and datasets.
Secure configurations: hardened infrastructure, network segmentation, and secure APIs.
Breach response: notification procedures tailored to client/ethical obligations and legal requirements.
Regulatory mapping: ensure GDPR/CCPA/sectoral rules applied to cross-border data flows and retention.

VENDOR & THIRD PARTY RISK

Due diligence: security posture, certifications, model provenance, data use practices, and legal compliance.
Contract terms: SLAs, audit rights, breach notification, IP ownership, data deletion, and indemnities.
Model transparency: require disclosure of training data sources, fine-tuning practices, and limitations.
Exit & continuity: data return/destruction clauses and migration/rollback plans.
Periodic reviews: security and performance reassessments, plus penetration testing where feasible.

MALPRACTICE & LIABILITY

Engagement terms: clear clauses about AI use, limitations, and client consent in engagement letters.
Supervision & sign-off: documented supervisory checkpoints and lawyer attestations for AI-assisted work.
Insurance review: ensure professional liability covers AI-related errors or expand coverage.
Escalation paths: rapid client remediation processes when AI errors cause client harm.
Documentation: retain decision rationale, reviews, and corrective actions to defend against claims.

GOVERNANCE, TRAINING & INCIDENT RESPONSE

Governance structure: assign AI risk owner, steering committee, and clear accountability lines.
Policies & standards: AI acceptable-use, data handling, procurement, model validation, and change control.
Training & certification: role-based training for lawyers, paralegals, and IT on risks and controls.
KPIs & monitoring: performance, accuracy, fairness, and security metrics with regular reporting cycles.
Incident playbooks: cross-functional response plans including legal, compliance, IT, client notification, and post-mortem reviews.
Continuous improvement: post-incident learning loops and policy updates based on incidents and audits.

www.jupiter-cap.com Email: rod.boothe@jupiter-cap.com