HEALTH / SCIENCE / TECHNOLOGY
Critical in a crisis, creative in court.®
/ SHB.COM /

SEPTEMBER 5, 2025

Anchoring Responsible AI Use With Good Governance Practices

Matthew Fox
Senior Corporate Counsel
JM Family Enterprises

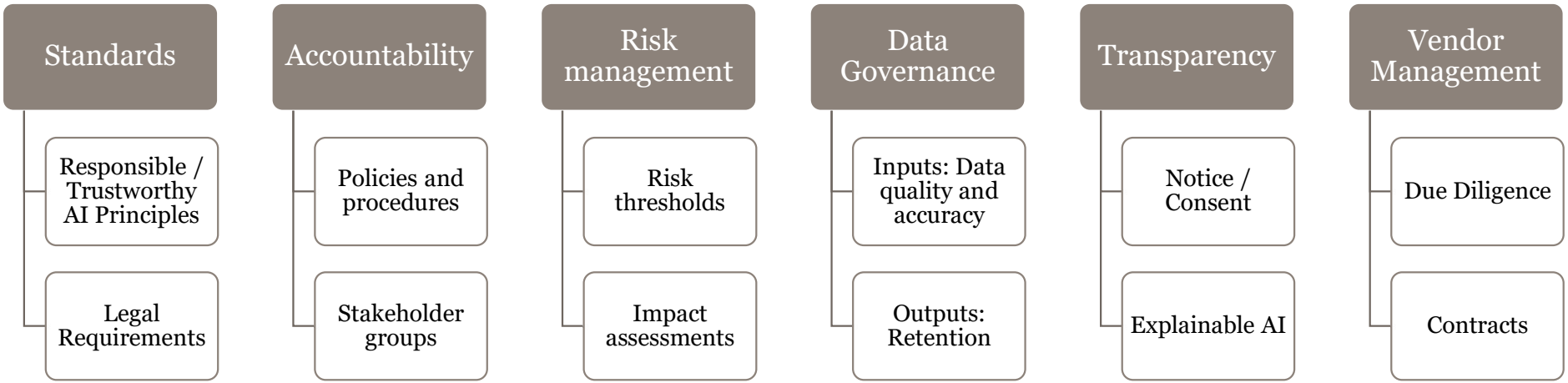
Camila Tobón
Partner
Shook, Hardy & Bacon LLP

SHOOK
HARDY & BACON

What is AI Governance?

- AI Governance starts with a framework setting out the company's vision for the responsible use of AI
- An AI Governance program includes the guardrails the company uses to ensure adherence to that vision
- For the program to work, companies need:
  - Documentation
  - Defined roles & responsibilities
  - Stakeholder awareness and buy-in

Components of an AI Governance Framework

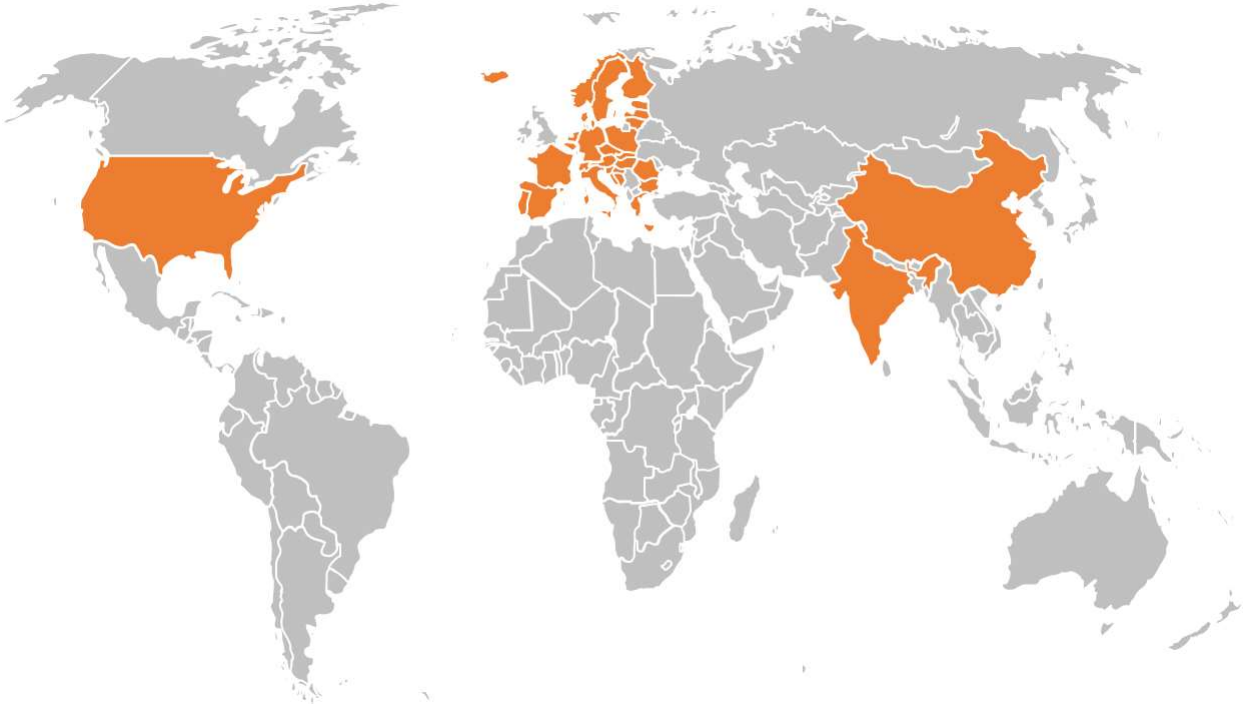


Principles

Responsible AI Principles	NIST Characteristics of Trustworthy AI	OECD Principles for Trustworthy AI
• Fairness • Reliability and safety • Privacy and security • Inclusiveness • Transparency • Accountability	• Valid and reliable • Safe • Secure and resilient • Accountable and transparent • Explainable and interpretable • Privacy-enhanced • Fair – with harmful bias managed	• Inclusive growth, sustainable development and well-being • Human rights and democratic values, including fairness and privacy • Transparency and explainability • Robustness, security and safety • Accountability

Global AI Laws

- EU – AI Act (entered into force 8/2/24)
- China – Interim Measures for the Management of Generative AI Services (eff. 8/15/23)
- US – AI Action Plan (July 23, 2025)
- South Korea – Basic Act on the Development of Artificial Intelligence and the Establishment of Trust (eff. 1/1/26)
- Japan – AI Promotion Act (eff. 6/4/25)



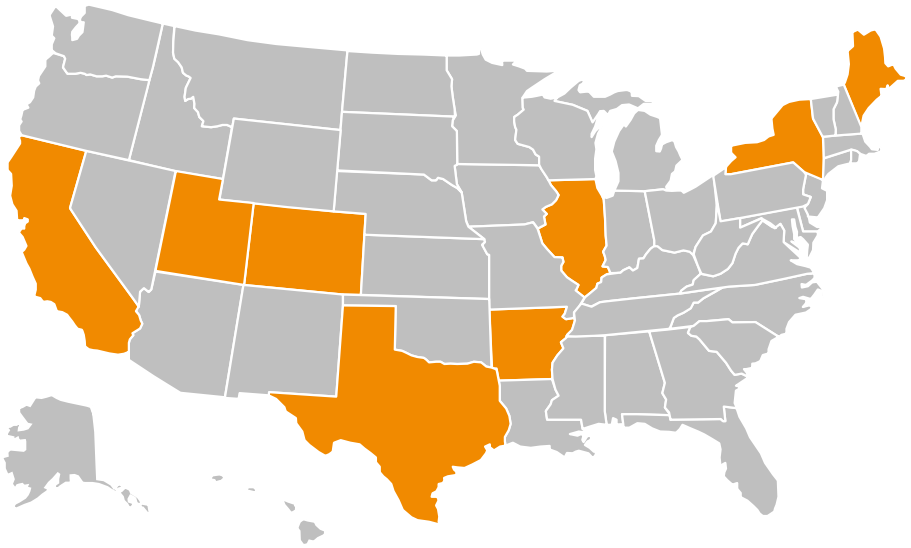
U.S. AI Regulation

Transparency

- California AI Transparency Act (eff. 1/1/26)
- California Generative AI Training Data Transparency Act (eff. 1/1/26)
- Maine Transparency in Consumer Transactions Involving AI (eff. 6/19/25)
- Utah AI Policy Act (eff. 5/1/24)

Certain AI Use Cases

- Arkansas Ownership of Model Training and Content (eff. 7/1/25)
- Colorado Act Concerning Consumer Protections in Interactions with AI Systems (eff. 2/1/26)
- Texas Responsible AI Governance Act (eff. 1/1/26)
- New York Responsible AI Safety and Education Act



AI in the Workplace

- Illinois AI Video Interview Act (eff. 1/1/20)
- New York City Local Law 144 (eff. 1/1/23)
- Illinois HB 3773 (eff. 1/1/26)
- CA regs re discrimination (eff. 10/1/25)

AI in Insurance

- CO SB 21-169 (eff. 9/6/21)
- NYDFS Circular Letter No. 7 (2024)
- NAIC Model Bulletin (adopted in several states)

AI in Healthcare

- CA AB 3030 – AI in healthcare (eff. 1/1/25)
- UT HB 452 – mental health chatbot (eff. 5/7/25)

AI in the Legal Profession

- Rules of Professional Responsibility
- ABA and state bar opinions

Accountability

AI Policies	• **Internal AI Policy:** Defines principles, roles, and responsibilities for AI governance • **Acceptable Use Policy:** Outlines permissible applications and usage boundaries for AI tools • **Development Policy:** Sets standards for ethical design, testing, and deployment of AI systems
Cross-functional working group	• Should include representatives from legal, compliance, IT, data science, and business units • Reviews and approves use cases (all / only those deemed high-risk) • Monitors compliance and advises on trustworthy AI / ethical concerns
AI Lifecycle	• Model / use case inventory • Track and document decisions, data sources, model changes, and performance metrics • Implement checkpoints for risk assessment, testing, and post-deployment monitoring • Foster a culture of accountability and continuous improvement

Types of Risks

Operational

- **Model Drift**: AI performance degrades over time due to changes in input data or environment.
- **System Failures**: AI misclassifies or makes incorrect predictions, leading to business disruption.
- **Security Vulnerabilities**: AI systems can be exploited through adversarial attacks or data poisoning.
- **Scalability Issues**: AI models may not perform consistently across different platforms or volumes of data.

Regulatory & Legal

- **Non-Compliance with Data Protection Laws**: AI systems may violate GDPR, CCPA, or other privacy regulations.
- **Intellectual Property Infringement**: AI-generated content may unintentionally breach copyright or trademark laws.
- **Consumer Protection Violations**: AI-driven pricing or subscription models may run afoul of auto-renewal or transparency requirements.
- **Liability and Accountability**: Unclear legal responsibility when AI causes harm or makes a faulty decision.

Ethical & Societal

- **Bias and Discrimination**: AI systems may reinforce or amplify existing biases in training data.
- **Lack of Transparency**: Black-box models make decisions that are difficult to explain or justify.
- **Job Displacement**: Automation through AI can lead to workforce disruption and unemployment.
- **Surveillance and Privacy Intrusion**: AI used in facial recognition or behavioral tracking can infringe on personal freedoms.

Assessing Risk

Low Risk

E.g., Internal productivity tools, basic automation, or non-sensitive data processing

Light touch review - Streamlined checklists focusing on data privacy, basic functionality, and alignment with internal policies

Moderate Risk

E.g., Customer-facing applications, decision-support systems, or tools using personal data

Enhanced review - Includes stakeholder consultation, bias testing, and documentation of intended use and safeguards

High Risk

E.g., AI systems involved in hiring, lending, healthcare, law enforcement, or any use with significant legal, ethical, or societal implications

In-depth review - Comprehensive evaluation covering fairness, accountability, transparency, and compliance with applicable laws and standards. May involve external audits or expert review

Data Governance

Data Sourcing & Quality

- **Provenance**: Ensure data sources are documented and legally acquired.
- **Accuracy & Reliability**: Use high-quality, representative datasets to reduce model errors and bias.
- **Diversity & Balance**: Avoid overrepresentation of specific viewpoints or demographics to mitigate bias.
- **De-duplication**: Remove redundant or repeated data to prevent overfitting.

Privacy & Compliance

- **Personal Data Handling**: Identify and remove or anonymize personal data to comply with privacy laws (e.g., GDPR, CCPA).
- **Consent Management**: Confirm that data subjects have provided valid consent where required.
- **Sensitive Data Controls**: Avoid using data that includes health, financial, or other sensitive information unless explicitly permitted.
- **Cross-border Data Transfers**: Ensure compliance with international data transfer regulations.

Usage & Lifecycle Management

- **Purpose Limitation**: Clearly define and document the intended use of the LLM and its training data.
- **Access Controls**: Restrict access to training data and model outputs to authorized personnel.
- **Auditability**: Maintain logs and documentation for data usage, model updates, and decision-making processes.
- **Retention & Deletion**: Establish policies for data retention and secure deletion when no longer needed.

Transparency

Required notices	• **Data Use Disclosures**: Explaining how personal data is collected, processed, and used by AI systems • **Automated Decision-Making Notices**: Disclosing when decisions are made or significantly influenced by AI (e.g., in hiring, lending, or customer service)
Consent	• Where required, obtain informed consent before deploying AI tools
Explainability	• **Summaries**: Describe the purpose, inputs, and outputs of the system in plain language • **Model Explainability**: Where feasible, provide insight into how the model reaches its conclusions, especially for high-impact decisions • **Limitations and Risks**: Clearly communicate known limitations, potential biases, and appropriate use contexts

Vendor Management

Due diligence

- **Model Transparency**: Request documentation on model architecture, training data sources, and performance metrics
- **Testing and Validation**: Review how the vendor tests for accuracy, bias, robustness, and fairness
- **Security Practices**: Assess data protection measures, including encryption, access controls, and incident response protocols
- **Legal and Regulatory Compliance:** Confirm the vendor complies with applicable law
- **Responsible AI Practices:** Evaluate how the vendor enables interpretability of AI outputs; Confirm whether the vendor supports human review
- **Performance Monitoring**: Ensure the vendor provides updates, maintenance, and retraining as needed; Confirm mechanisms for tracking model drift, performance degradation, and compliance over time.

Contractual language

- **Transparency Requirements**: Mandate disclosure of model architecture, training data provenance, and explainability features
- **Audit Rights**: Allow periodic reviews of AI systems and processes
- **Compliance Obligations**: Require adherence to relevant AI regulations and organizational policies
- **Liability and Risk Allocation**: Clearly define accountability for harm caused by AI outputs or failures

Contacts

Matthew Fox

Senior Corporate Counsel
JM Family Enterprises
Matthew.Fox@jmfamily.com

Camila Tobón

Partner
Shook, Hardy & Bacon LLP
ctobon@shb.com

HEALTH / SCIENCE / TECHNOLOGY / SHB.COM /

SHOOK
HARDY & BACON

SHOOK
HARDY & BACON