Shumaker

NOVEMBER 13, 2025 | PUBLICATION

"From Disclosure to Defense: A Strategic AI Governance Blueprint"

Artificial intelligence (AI) is no longer a speculative frontier. It is embedded in the operational core of modern enterprises, ranging from customer service bots to predictive analytics. However, as AI systems scale, so do the risks. The challenge is no longer whether AI poses legal exposure but rather how to govern AI effectively before it becomes a liability. A strategic AI governance blueprint can assist leaders in building defensible and scalable governance programs that mitigate risk while enabling responsible innovation.

INDUSTRY SECTOR

Technology

SERVICE LINE

Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

Lloyd J. Wilson

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

I. Understanding the Legal Risk Landscape

AI introduces a multidimensional risk profile that spans several areas. Recent analysis shows that 72 percent of S&P 500 companies now disclose AI-related risks in their U.S. Securities and Exchange Commission (SEC) filings, which is up from just 12 percent in 2023, and these disclosures increasingly focus on reputational harm, cybersecurity vulnerabilities, and regulatory scrutiny, underscoring the need for legal teams to proactively govern AI systems.[1] As a result, boards are now expected to integrate AI into enterprise risk frameworks, treating it with the same rigor as financial, operational, and compliance risks.

II. Building a Defensible AI Governance Program

a. Establish a Policy Stack – A defensible AI governance program begins with a clear and enforceable policy architecture. Legal leaders should collaborate with technical and operational stakeholders to define the boundaries of acceptable AI use and embed oversight mechanisms into enterprise workflows. Together, these processes in the policy stack form the backbone of a scalable governance program. A well-structured policy stack typically includes:

i. An AI Acceptable Use Policy

1. This foundational document sets the guardrails for how AI may be used across the organization. It should define (a) permissible and prohibited use cases, (b) requirements for human oversight in high-impact applications, and (c) restrictions on generative AI tools for sensitive or regulated content.

ii. A Model Risk Classification Standard

1. Not all AI systems carry equal risk. This classification standard should (a) categorize models by risk level, (b) define validation, monitoring, and decommissioning protocols based on risk tier, and (c) align with external frameworks such as the NIST AI Risk Management Framework or ISO/IEC 42001.

iii. Disclosure and Transparency Protocols

1. Legal teams should ensure that AI use is communicated clearly to internal and external stakeholders. This includes (a) notices to employees and customers when AI is used in decision making, (b) guidelines for substantiating AI-related claims in marketing and investor communications, and (c) coordination with privacy teams to align disclosures with data protection obligations.

b. Inventory and Classify AI Systems – A defensible AI governance program requires visibility. Legal teams should work with IT, procurement, and business units to create a centralized inventory registry of all AI systems in use, including those embedded in third-party tools. This registry serves as the foundation for risk assessments, policy enforcement, and regulatory readiness.

i. Key Steps for Classifying AI Systems

1. Catalog all AI systems by identifying and documenting every AI-enabled tool, model, or service, both internally developed and vendor-provided solutions, used across the enterprise.

2. Tag the AI systems by risk drivers (e.g., use of personal or sensitive data, involvement in consequential decisions, and safety-critical functions or autonomous behavior).

3. Link each AI system to supporting documentation indicating intended use, bias audits and validation results, and vendor due diligence with associated contractual protections.

c. Implement Evaluation and Monitoring Protocols – Once AI systems are inventoried and classified, legal and compliance teams must ensure that robust evaluation and monitoring protocols are in place. These controls are essential for mitigating risk and demonstrating proactive oversight to regulators, auditors, and stakeholders. Important evaluation and monitoring protocols include:

i. Pre-Deployment Testing

1. Before any AI system goes live, it should undergo rigorous testing for accuracy and reliability in intended use cases, bias and fairness, privacy vulnerabilities, and explainability through understandable outputs.

ii. Simulation of Adversarial Scenarios

1. Legal teams should coordinate with technical experts to simulate misuse scenarios,

adversarial attacks, and edge cases to identify failure modes and inform escalation protocols.

iii. Ongoing Monitoring and Drift Detection

1. AI systems must be continually monitored for model drift, bias regression, and abuse or unintended use.

iv. Governance Dashboards and Reporting

1. Dashboards can be established to track key risk indicators, provide audit logs, and display compliance status across AI systems to support internal accountability and external reporting obligations.

d. Human Oversight and Escalation Mechanisms – Even the most advanced AI systems require human judgment to ensure fairness, accountability, and legal defensibility. Embedding structured human oversight into AI workflows is essential for systems that affect rights, safety, or access to services.

i. Thresholds for Human Review

1. Define clear criteria for when human intervention is required.

ii. Override and Kill-Switch Capabilities

1. Ensure that authorized personnel can override or disable AI systems in real time. This includes manual override functions for automated decisions and emergency shutdown protocols for systems that pose safety or reputational risks.

iii. Feedback Loops

1. Establish mechanisms for individuals to challenge AI-driven outcomes using internal review procedures with defined response timelines and integration of user feedback into model retraining.

III. Legal Leadership in Vendor Governance

a. Contracts as Governance Tools – As AI capabilities are increasingly embedded in third-party platforms and enterprise tools, legal teams must take a proactive role in managing vendor risk. Contracts act as governance tools that allocate responsibility, define oversight, and mitigate exposure.

i. AI-Specific Contract Riders

1. Legal counsel should require tailored provisions in vendor agreements that address the unique risks of AI systems. These provisions may include:

a. Representations and warranties regarding training data provenance, intellectual property (IP) ownership, and compliance with applicable laws.

b. Bias testing and performance obligations, including thresholds for accuracy, fairness, and explainability.

c. Audit rights to inspect model documentation, testing results, and governance practices.

d. Indemnification clauses for AI-related harms, such as discriminatory outcomes, IP infringement, or data misuse.

ii. Technical Documentation Supporting Advertised Features

1. To avoid regulatory enforcement or litigation, companies should maintain internal files that indicate any public claims about AI capabilities. These files should include (a) technical documentation supporting the advertised features, (b) records of bias audits, validation tests, and model limitations, and (c) legal review of marketing materials and investor disclosures.

iii. Flow-Down Obligations for Third-Party Tools

1. When vendors rely on external AI models or services, contracts should include flow-down obligations requiring transparency, compliance, and risk mitigation throughout the supply chain.

IV. Incident Response and Disclosure Readiness

a. Tailored Incident Response – A defensible governance program must include tailored incident response protocols that anticipate the unique risks posed by AI systems and ensure readiness to disclose material events.

i. Notification Playbooks

1. Notification playbooks should (a) define thresholds for mandatory reporting under laws like General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), or state consumer protection statutes, (b) include pre-approved messaging templates and escalation paths, and (c) align with cybersecurity and privacy incident protocols to ensure consistency.

ii. Audit Trails

1. Legal teams should (a) record all incident investigations, decisions, and remediation steps and (b) maintain version histories of affected models and datasets.

V. Implementation Blueprint

a. Getting Started – Legal leadership is essential to operationalizing AI governance.

i. Step 1 – Appoint a senior leader to champion the initiative and ensure cross-functional alignment within the enterprise.

ii. Step 2 – Form a cross-functional working group that includes representatives from legal, compliance, IT, data science, and other product teams to ensure diverse perspectives and shared ownership.

iii. Step 3 – Approve core governance policies (e.g., an AI acceptable use policy, model risk classification standard, and disclosure protocols).

iv. Step 4 – Launch a centralized registry of AI systems, including vendor tools, internal models, and experimental pilots.

b. Evaluate and Engage

i. Step 5 – Focus on high-impact systems involving personal data, consequential decisions, or customer-facing outputs.

ii. Step 6 – Review contracts for AI-specific clauses (e.g., indemnification, audit rights, bias testing) and evaluate whether updates are needed.

iii. Step 7 – Educate business units on AI governance policies, legal risks, and escalation procedures.

c. Operationalize and Test

i. Step 8 – Deploy tools for model drift detection, bias regression, and performance tracking.

ii. Step 9 – Simulate AI-related incidents to test response readiness.

iii. Step 10 – Provide governance updates to leadership indicating risk findings, policy adoption status, and next-phase priorities.

VI. Conclusion

AI governance is a strategic imperative as companies continue to embed it within their operational framework. As AI becomes embedded in core business functions, the legal risks multiply across contracts, compliance, privacy, and reputation. Legal counsel is uniquely positioned to lead the charge, not only by identifying exposure but by architecting the policies, controls, and contractual protections that define responsible AI use. A defensible governance program requires more than reactive compliance. It demands proactive structure: clear policies, system inventories, risk assessments, vendor oversight, and incident response protocols. By embedding legal oversight into the AI lifecycle, legal counsel can protect the enterprise, enable innovation, and build trust with regulators, customers, and investors.

The blueprint is clear. The time to act is now.

---

[1] Matteo Tonello, *AI Risk Disclosures in the S&P 500: Reputation, Cybersecurity, and Regulation*, Harv. L. Sch. F. on Corp. Governance (Oct. 15, 2025), https://corpgov.law.harvard.edu/2025/10/15/ai-risk-disclosures-in-the-sp-500-reputation-cybersecurity-and-regulation.