



AI GOVERNANCE: CONTROL, COMPLIANCE & RESPONSIBLE IMPLEMENTATION

August 10, 2026

Presented By: Kathleen A. McGee, Partner Lowenstein Sandler LLP



AGENDA

- 1 What AI Governance Means in Practice
- 2 Model Risk, Bias, and Explainability
- 3 Data Privacy, Compliance, and Auditability
- 4 Human Oversight vs. Automation
- 5 Vendor Risk and Third-Party AI Controls
- 6 Governance Frameworks That Enable Progress



WHAT AI GOVERNANCE MEANS IN PRACTICE

AI governance is rapidly becoming a proxy for management quality.

- Approved AI Use Policy
- Employee Training Programs
- Data Classification Rules
- Human Review Requirements
- Vendor Risk Review Procedures
- AI Incident Escalation Procedures

Key Questions:

- Who can use AI technologies?
- In what context?
- Who is accountable for safety and reliability review?
- What are the contingency plans if the technology fails?

AI MODELS REFLECT RISK AND SOPHISTICATION

AI Models	Description	Advantages	Disadvantages
Public / Open Source AI Models	3rd party models available for use by anyone (e.g., ChatGPT free version)	Free to use; No ability to negotiate terms	Risk of loss of data confidentiality; No warranties
Commercially Licensed AI	3rd party models licensed to organizations (e.g., Copilot, Harvey)	User controls state of quality; Data kept internal; Licensing fees	Large investments to make, maintain and update; Requires careful contracts
Private / Vendor-Developed AI	Models developed internally and solely within the organization	Complete confidentiality and data privacy; Can be highly specialized	High development and maintenance costs; Expensive in-house expertise needed

BENEFITS AND RISKS OF AI

Benefits

- Saving time and costs by offloading tedious tasks
- Solving the "blank page" problem
- Summarizing meeting minutes and documents
- Greater business intelligence from datasets
- Enhanced spellchecking, grammar, and tone
- Detecting fraudulent activity

Risks

- Intellectual property concerns
- Data privacy and security vulnerabilities
- Analysis in "black box" - unpredictable results
- Response accuracy and hallucination risks
- Bias and objectionable content
- Increased fraud and hacker exposure
- Regulatory compliance challenges

MODEL RISK, BIAS, AND EXPLAINABILITY

Model Risk

AI models operate in a "black box" - outputs can be unpredictable and difficult to audit. Organizations must understand model limitations before deployment.

Bias & Discrimination

AI systems can perpetuate or amplify existing biases in training data. CFPB Guidance (Sept 2023) specifically addressed AI bias in credit decisions under Reg B. This agency interpretation was withdrawn by Trump Administration in 2025, but most still adhere to the principle that AI models must always be sufficiently explainable to generate specific adverse action reasons.

Explainability & Transparency

Regulators increasingly require organizations to explain AI-driven decisions. "Specificity is particularly important when creditors utilize complex algorithms" - CFPB Circular 2023-03.

THE EVOLVING REGULATORY LANDSCAPE



Regulation/Guidance	Date	Focus
EU AI Act	Aug 2024	Risk-based AI classification and requirements
CFPB Guidance (Reg B)	Sept 2023	AI in credit decisions; adverse action notices
SEC AI Priorities	Oct 2024	AI in investment advisory and trading
FTC AI Enforcement	Aug 2024	Unfair/deceptive AI practices
US AI Action Plan	July 2025	National AI strategy and priorities
Trump Admin AI Executive Order	Jan 2025	Rescission of Biden AI EO; new direction

The regulatory landscape is rapidly evolving - organizations cannot afford to wait.

DATA PRIVACY, COMPLIANCE, AND AUDITABILITY



Data Privacy & Security

- Data classification rules for AI inputs
- Restrict confidential data from public AI
- Ensure personally identifiable information (PII) is protected
- Control data retention and deletion

Compliance

- Align AI use with existing regulations
- Document AI decision-making processes
- Regular compliance assessments
- Cross-functional oversight teams

Auditability

- Maintain logs of AI inputs/outputs
- Track model versions and changes
- Enable regulatory examination
- Continuous monitoring and reporting

HUMAN OVERSIGHT VS. AUTOMATION

KEEPING HUMANS IN THE LOOP (HITL)

Involving people at key stages of the AI system's operation to ensure oversight, control, and accountability.

Combining the strengths of AI (speed, scale, pattern recognition) with human judgment, ethics, and contextual understanding.

WHY IT MATTERS:

Ethical Safeguards

Reduces the risk of biased or harmful decisions

Accountability

Ensures someone is responsible for outcomes

Trust

Builds confidence in AI systems by keeping humans involved

AI is a supplemental tool that enhances, but doesn't replace, human capabilities for critical thinking and ethical judgment.

THE SPECTRUM OF HUMAN OVERSIGHT

Human-in-the-Loop

- Humans actively involved in training, testing, and decision-making
- Reviewing AI recommendations before final actions
- Feedback loops help AI learn and improve

Human-on-the-Loop

- Humans monitor but don't intervene unless necessary
- Used in semi-autonomous systems
- Can override or shut down if AI behaves unexpectedly

Human-out-of-the-Loop

- AI operates fully autonomously without human intervention
- Common in low-risk applications (spam filters)
- Riskier in high-stakes domains unless carefully designed

Lower Risk



Higher Risk

AI IS MOVING FROM ASSISTANT TO OPERATOR

Agentic AI and chatbots are increasingly in the stream. These systems can take actions rather than simply provide information.

Traditional AI

- Draft emails
- Summarize documents
- Answer questions
- Generate reports



Next Generation Agentic AI

- Place orders
- Schedule shipments
- Approve transactions
- Adjust pricing
- Communicate with customers

Without rules and compliance, these technologies become active risk in any workplace.

CASE STUDY: CHANGE HEALTHCARE (2024)

A cyber incident at one company became a cash-flow crisis across an entire industry.

- Ransomware attack on Change Healthcare, a payment processor
- Claims processing halted nationwide
- Billions in disruption across the healthcare system
- Many healthcare providers unable to meet payroll
- Emergency funding required from insurers and government

Key Lesson:

Technology problems increasingly become credit problems. Single points of failure in critical infrastructure can cascade across entire industries.

AHA Survey: Change Healthcare Cyberattack Significantly Disrupts Patient Care, Hospitals' Finances

Change Healthcare cyberattack having 'far-reaching' effects on providers

UnitedHealth says Change Healthcare cyberattack cost it \$872 million

Change Healthcare breach: The cyberattack's impact 2 years later

CASE STUDY: CROWDSTRIKE (2024)

No malicious actor required. Technology concentration alone created enterprise disruption.

- Software update failure - not a cyberattack
- Airlines grounded worldwide
- Hospitals disrupted
- Retail operations interrupted

Key Lesson:

Vendor concentration risk is real. A failed software update - with no malicious actor - can cause global disruption.

CASE STUDY: AMAZON (2025)

A governance failure, not just an AI failure.

- AWS experienced a 13-hour outage affecting its Cost Explorer service in mainland China
- Engineers allowed Amazon's internal AI coding agent "Kiro" to make production changes
- Rather than applying a targeted fix, AI determined the optimal solution was to "delete and recreate the environment"
- Amazon attributed the incident to misconfigured access controls and human error

Takeaway: As organizations deploy increasingly autonomous AI agents, success will depend not only on model capability, but on the controls, approvals, and guardrails surrounding those systems.

THE BOTTOM LINE



Technology problems increasingly become credit problems.

Event Type	Result
Cyberattack	Operations disrupted
Vendor outage	Operations disrupted
Failed software update	Operations disrupted
AI error	Operations disrupted
Data loss	Operations disrupted

Regardless of cause, the operational and financial impact is the same. Governance is the common defense.

VENDOR RISK AND THIRD-PARTY AI CONTROLS

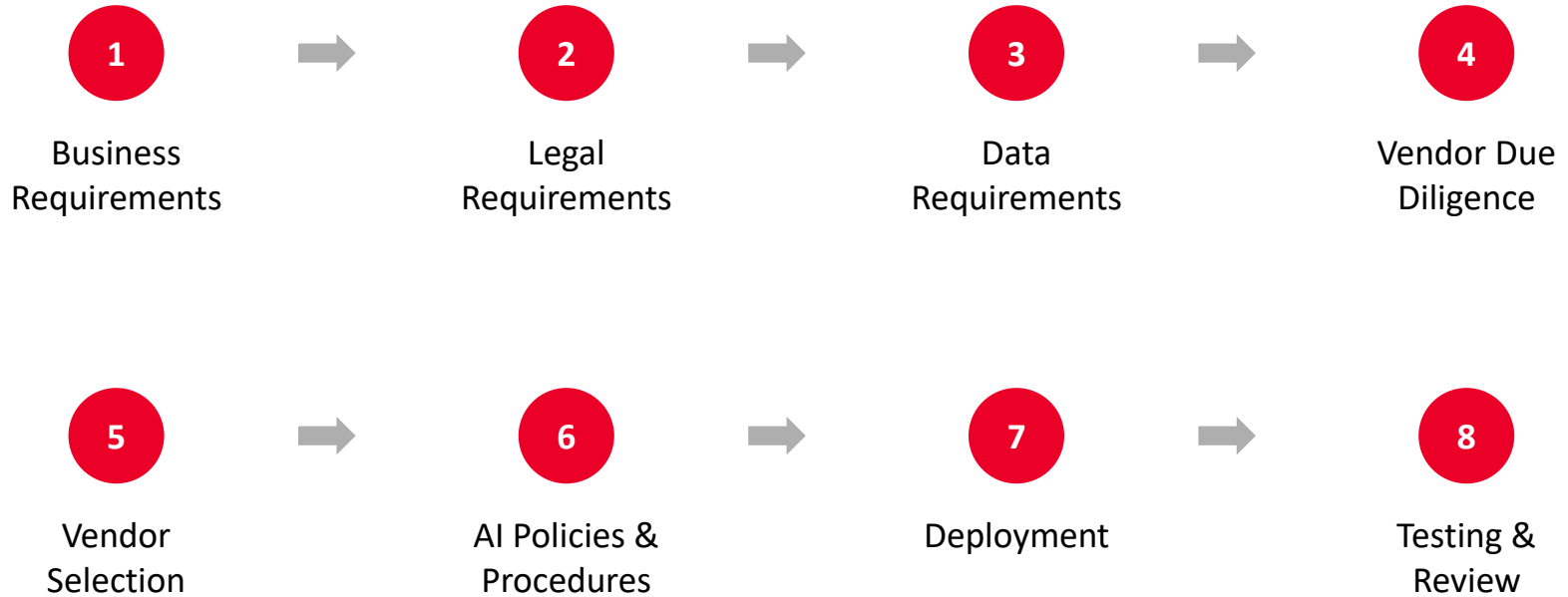
Vendor Due Diligence Questions:

- What features/functionality is provided? What is the intended purpose/use?
- Are there any known limitations of the product?
- What data was the model trained on?
- What data does the model consider in real time?
- What rights do customers have with respect to the output?
- Is the AI tool properly configured?
- Was the AI tool tested on a non-production server?

Supply Contract Tech Risk Terms:

- Technology Governance
- Cybersecurity & Data Protection
- AI and Automated Systems
- Human Oversight & Change Mgmt
- Third-Party Technology Providers
- Business Continuity
- Audit and Assurance
- Regulatory Compliance
- Indemnification for Tech Failures

THE AI LIFECYCLE FRAMEWORK



GOVERNANCE FRAMEWORKS THAT ENABLE PROGRESS

Security as guardrails, not blocking business. All-or-nothing policies rarely work.

Internal-Facing Policies:

- Statement of principle - standalone AI policy
- Employee Handbooks - use of AI by employees
- Company AI/Privacy/Security Plans
- Procurement / Contracts Considerations

External-Facing Policies:

- Credit Agreements - AI in credit determinations
- B2B Contracts
- Privacy and Information Security Terms
- IT Procurement - third-party vendor AI

Key Considerations for Any AI Policy:

Data privacy/security | Verifying AI output | Bias/discrimination | Transparency | Employee training
| Accountability | Ethical considerations | Continuous monitoring

WHAT "GOOD" AI GOVERNANCE LOOKS LIKE

AI governance often tells you more about management discipline than the AI itself.



Does the company have an AI use policy?



Is confidential information restricted from AI tools?



Is AI-generated work reviewed by humans?



Who approves new AI deployments?



Are vendors vetted before adoption?

10 DIGITAL RISK QUESTIONS EVERY ORGANIZATION SHOULD ASK

- 1 What systems are critical to operations?
- 2 How long can the company operate if those systems fail?
- 3 Has the company experienced a material cyber incident?
- 4 Are key vendors critical to operations?
- 5 Does the company have tested backups?
- 6 Can operations be performed manually?
- 7 Is there cyber insurance?
- 8 Is AI being used in customer-facing or operational processes?
- 9 Is there an AI governance policy?
- 10 Who is accountable for digital risk?

AI GOVERNANCE BEST PRACTICES



Approved AI Use Policy

Define acceptable AI
functions and restrictions

Employee Training

Ongoing education on AI
use and risks

Data Classification

Rules for what data can be
used with AI

Human Review Requirements

Mandated human
oversight of AI outputs

Vendor Risk Review

Due diligence on all AI
vendors

Incident Escalation

Clear procedures when AI
fails

Practical Steps for Implementation:

- Create comprehensive AI policy or update existing Acceptable Use Policies
- Security should act as guardrails, not block business
- Involve all relevant stakeholders across the organization
- Define acceptable AI functions and use cases
- Restrict AI for specific tasks or employee groups where needed
- Update employee and customer training programs
- Consider auditing software to monitor acceptable AI use
- Establish procedures to support your policies (NDA vendors, HITL responsibilities)

KEY TAKEAWAYS

- AI is everywhere - don't ignore it; every organization should have AI policies
- The regulatory landscape is rapidly evolving and will be for a while
- Ongoing monitoring and quality control of AI output are critical
- Keep Humans in the Middle - AI supplements, not replaces, human judgment
- Vendor-provided AI requires due diligence and careful contract drafting
- Without rules and compliance, technologies become active risk
- AI governance is a proxy for management quality - enable, don't just restrict



Partner

**Data Privacy, Security, Safety &
Risk Management, White Collar
Defense**

T: +1 646.414.6831

kmcgee@lowenstein.com

Education

Boston University (J.D. 2001)

University of Chicago (M.A.
1996)

Sarah Lawrence College (B.A.
1994)

Admissions

New York

U.S. District Court for the Eastern
District of New York

U.S. District Court for the Southern
District of New York

KATHLEEN A. MCGEE



- Nearly two decades as prosecutor and leading regulator
- Former Bureau Chief of NY Attorney General's Bureau of Internet and Technology
- Author of New York SHIELD Act
- Experience with DOJ, SEC, FTC, and state Attorneys General
- Expertise in technology, data commodification, cybersecurity/privacy, consumer protection, AI, and data governance
- Testified before U.S. Congress on data breach enforcement



THANK YOU

NEW YORK PALO ALTO ROSELAND SALT LAKE CITY SAN FRANCISCO WASHINGTON, D.C. WILMINGTON

© 2026 LOWENSTEIN SANDLER LLP