

Hey! What's New? 2025-87

Seven Legal Considerations for Mitigating Risk in AI Implementation

An article in *CFO*, written By Emily Burrows, says that “for finance executives tasked with driving innovation and controlling risk, AI presents both an opportunity and a challenge. While the potential return on investment is clear, the legal and regulatory risks are often less visible but equally significant. Here are seven key legal considerations to help finance leaders understand and mitigate risk when supporting or overseeing AI initiatives.”

1. Data privacy and protection are paramount: Burrows notes that “AI systems often rely on large volumes of data, including sensitive personal, financial and business information. Compliance with data privacy laws is critical,” as various regulations impose strict requirements on the collection, processing, storage and sharing of personal data. “Organizations should ensure that:

- Data used for AI is collected and processed lawfully, with appropriate consent where required.
- Data minimization principles are followed, using only the data necessary for the intended AI application.
- Robust data security measures are in place to prevent unauthorized access, breaches or misuse.”

Burrows adds that “non-compliance with data privacy laws can result in significant fines, litigation and reputational harm, regardless of industry.”

2. Consider bias, fairness and discrimination: According to Burrows, “AI systems can inadvertently perpetuate or amplify biases present in training data, leading to unfair or discriminatory outcomes.” To mitigate these risks, she says, “organizations should:

- Establish procedures for human oversight of high-impact AI decisions.
- Conduct regular audits of AI models to identify and address potential biases.
- Use diverse and representative datasets for training and validation.”

3. Regulatory landscape and compliance uncertainty: The legal framework surrounding AI is evolving rapidly. “Organizations should:

- Monitor emerging laws and regulatory guidance across key jurisdictions.
- Designate a cross-functional team to oversee AI governance and compliance.
- Document the purpose, risk classification and safeguards for each AI use case.
- Plan for future disclosure obligations (e.g., impact assessments or risk ratings).”

Burrows believes that “proactive compliance management reduces the risk of enforcement actions and supports sustainable AI adoption across all sectors.”

4. Intellectual property and licensing strategies: AI projects involve unique intellectual property questions related to data ownership and IP rights in AI-generated works. “Organizations should ensure that their investments in AI translate into sustainable competitive advantages, not legal vulnerabilities. Risk mitigation strategies include:

- Secure licenses for all third-party datasets or pre-trained models.
- Address IP ownership in all agreements with employees, contractors and vendors.
- Explore trade secrets, copyright or patent protections for key AI assets.

- Maintain internal records of model development, versions and authorship.”

5. Contractual risk allocation: “AI projects often involve collaboration with vendors, consultants and technology partners. Well-drafted contracts are essential to allocate risk, define responsibilities and establish clear expectations,” Burrows advises.

6. Transparency, oversight and risk management: Burrows warns that “AI is increasingly scrutinized by stakeholders — investors, regulators, customers and the public — who expect responsible and ethical use. For organizations, this means ensuring that AI risk is incorporated into broader enterprise risk management practices. Key risks include misuse of AI tools due to a lack of access controls or training, the inability to explain or justify decisions made by AI systems and unchecked model drift leading to inaccurate or unpredictable outputs.”

7. Cybersecurity and incident response: “AI systems can introduce new cybersecurity vulnerabilities, including risks related to data integrity, model manipulation and adversarial attacks. Organizations must prioritize cybersecurity to protect AI assets and maintain trust. Best practices include:

- Integrating AI systems into the organization’s broader cybersecurity framework.
- Conducting regular security assessments and penetration testing of AI applications.
- Developing and testing incident response plans specific to AI-related threats.
- Training staff on AI security risks and best practices.”

Burrows suggests that “a strong cybersecurity posture is essential to safeguard sensitive data and maintain regulatory compliance in any industry.”

Learn considerably more at [7 legal considerations for mitigating risk in AI implementation | CFO.com](#).