LEADING THROUGH AI RISK

A Practical Guide for Risk Management & Legal Leaders

About This Guide

Artificial intelligence is rapidly changing engineering practice. While much of the discussion surrounding AI focuses on technology, the ACEC Research Institute's *Leading Through AI Risk: The Enterprise Framework for Engineering Firm Leaders* found that the risks associated with AI extend across virtually every aspect of an engineering organization, including technical quality, professional responsibility, data governance, workforce development, ethics, cybersecurity, financial performance, and organizational leadership.

The research combined an extensive literature review with in-depth interviews involving 21 leaders representing engineering firms, public infrastructure owners, technology providers, AI consultants, insurance and legal professionals, and the engineering licensing community. One of the study's central findings was that managing AI risk is fundamentally an organizational challenge rather than simply a technology challenge.

The Eight Domains of AI Risk

1 Technical Reliability and Model Risk	**2 Professional Liability and Standard of Care Risk**
3 Data Governance, Privacy and Intellectual Property Risk	**4 Organizational and Workforce Risk**
5 Ethical, Regulatory and Reputational Risk	**6 Operational and Cybersecurity Risk**
7 Financial and Business Model Risk	**8 Strategic Leadership and Enterprise Governance Risk**

Although each domain represents a distinct category of risk, AI risks do not remain within individual departments. Workforce training affects technical reliability, data governance influences cybersecurity and intellectual property protection, and weak organizational oversight can create legal liability. Effective AI risk management therefore requires coordinated governance across the enterprise.

What This Means for Risk Management & Legal Leaders

Risk management and legal leaders help firms identify, interpret, and manage the liability, contractual, regulatory, insurance, data protection, vendor, incident response, and enterprise risk implications of AI adoption.

Risk management and legal do not own every AI risk. Their role is to work across the enterprise with executive leadership, engineering, technology, project delivery, and human resources to ensure AI policies and practices remain aligned with professional, contractual, regulatory, and organizational obligations.

How to use this guide: Each question below is a direct translation of a Risk Management & Legal Leaders action identified in the published report.

1. Technical Reliability and Model Risk

Technical reliability can create legal and organizational exposure when AI-assisted workflows are poorly documented, governance policies become outdated, or vendors introduce unmanaged security or contractual risks.

Questions Risk Management & Legal Leaders Should Ask

- Are we documenting AI-assisted workflows where appropriate?
- Are we periodically reviewing AI governance policies?
- Are we evaluating vendor capabilities, security practices, and contractual responsibilities?

2. Professional Liability and Standard of Care Risk

AI does not change professional responsibility. Risk management and legal leaders help firms evaluate professional liability, contractual provisions, insurance coverage, and emerging legal and regulatory expectations.

Questions Risk Management & Legal Leaders Should Ask

- Are we reviewing professional liability implications associated with AI-assisted services?
- Are we evaluating contracts for provisions addressing AI, confidentiality, ownership of work product, and professional responsibility?
- Are we periodically assess insurance coverage as AI adoption expands?
- Are we monitoring emerging legal and regulatory developments affecting AI-assisted engineering practice?

3. Data Governance, Privacy and Intellectual Property Risk

AI raises questions involving confidentiality, data protection, intellectual property, vendor practices, and technology evaluation. Risk management and legal leaders help establish policies and controls addressing these exposures.

Questions Risk Management & Legal Leaders Should Ask

- Are we reviewing contractual obligations governing confidential information?
- Have we developed policies regarding AI use and data protection?
- Are we monitoring evolving intellectual property regulations?
- Are we periodically assess vendor security practices and data governance capabilities?
- Have we established procedures for evaluating new AI technologies before organizational deployment?

4. Organizational and Workforce Risk

Workforce AI use creates policy, responsibility, regulatory, and contractual considerations. Risk management and legal leaders help ensure acceptable-use guidance and organizational responsibilities remain clear and current.

Questions Risk Management & Legal Leaders Should Ask

- Have we updated policies addressing acceptable AI use by employees?
- Have we clarified organizational responsibilities regarding AI-assisted work?
- Are we ensuring workforce guidance aligns with evolving regulatory and contractual expectations?

5. Ethical, Regulatory and Reputational Risk

AI regulation and legal expectations continue to evolve. Risk management and legal leaders help firms monitor change, review policies, evaluate emerging legal risks, and connect AI governance to enterprise risk management.

Questions Risk Management & Legal Leaders Should Ask

- Are we monitoring evolving regulatory guidance affecting AI?
- Are we periodically reviewing al policies for alignment with contractual and professional obligations?
- Are we evaluating emerging legal risks associated with AI-assisted services?
- Are we coordinating al governance with existing enterprise risk management processes?

6. Operational and Cybersecurity Risk

AI introduces vendor, incident response, cybersecurity, and operational readiness considerations. Risk management and legal leaders help ensure these risks are addressed through contracts, procedures, coordination, and periodic assessment.

Questions Risk Management & Legal Leaders Should Ask

- Are we reviewing vendor contracts supporting AI services?
- Have we developed incident response procedures addressing AI-related events?
- Are we coordinating cybersecurity, operational risk, and AI governance activities?
- Are we periodically assess operational readiness as AI adoption expands?

7. Financial and Business Model Risk

AI investments and AI-enabled services create financial, contractual, pricing, and business-model risks. Risk management and legal leaders help firms assess these exposures alongside strategic opportunities.

Questions Risk Management & Legal Leaders Should Ask

- Are we evaluating aI investments using both financial and strategic criteria?
- Are we monitoring contractual implications associated with AI-enabled services?
- Are we assessing emerging business risks alongside new revenue opportunities?
- Are we reviewing pricing strategies as AI capabilities mature?

8. Strategic Leadership and Enterprise Governance Risk

Enterprise AI governance must remain connected to existing risk management processes. Risk management and legal leaders monitor regulation, review policies, and evaluate emerging enterprise risks as AI capabilities evolve.

Questions Risk Management & Legal Leaders Should Ask

- Are we coordinating enterprise AI governance with existing risk management processes?
- Are we monitoring regulatory developments?
- Are we periodically reviewing organizational AI policies?
- Are we evaluating emerging enterprise risks associated with evolving AI capabilities?

The Role of Risk Management & Legal Leaders in Managing AI Risk

Taken together, these questions show that risk management and legal leaders have responsibilities across the entire AI lifecycle, from governance policies and vendor evaluation to professional liability, contracts, data protection, regulation, incident response, investment risk, and enterprise governance.

The full study concludes that effective AI risk mitigation requires coordinated enterprise governance rather than isolated compliance activity. Risk management and legal leaders therefore help connect emerging AI practices to the firm's existing risk management, contractual, insurance, and compliance structures.

For risk management and legal leaders, the objective is not to eliminate AI-related uncertainty. It is to help the firm identify emerging exposures early, establish defensible policies and processes, and adapt governance as technology, regulation, contracts, and business models evolve.

For the complete AI Risk Framework, research findings, and recommendations for engineering firms, read

Leading Through AI Risk: The Enterprise Framework for Engineering Firm Leaders.