LEADING THROUGH AI RISK

A Practical Guide for Technology 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 Technology Leaders

Technology leaders are responsible for many of the platforms, data environments, security controls, integrations, monitoring systems, and vendor relationships that enable AI use. Their decisions directly influence technical reliability, data protection, operational resilience, and enterprise governance.

Technology leaders do not own AI risk alone. The study emphasizes that AI governance cannot remain solely an IT responsibility. Technology leaders should work closely with executive leadership, engineering, project delivery, human resources, and risk management and legal professionals.

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

1. Technical Reliability and Model Risk

Technical reliability depends partly on the quality of AI platforms, engineering data, validation, and ongoing monitoring. Technology leaders establish the technical environment that supports reliable AI-assisted work.

Questions Technology Leaders Should Ask

- Are we prioritizing enterprise AI platforms capable of protecting confidential information?
- Have we improved engineering data quality, organization, and accessibility?
- Are we validating AI tools before broad organizational deployment?
- Are we monitoring AI performance as models evolve?

2. Professional Liability and Standard of Care Risk

Professional accountability requires AI systems that support transparency, traceability, secure knowledge records, and integration with established engineering workflows.

Questions Technology Leaders Should Ask

- Are we selecting AI platforms that support transparency and traceability?
- Are we maintaining secure records of organizational knowledge supporting AI outputs?
- Have we integrated AI tools into existing engineering workflows rather than creating parallel processes?

3. Data Governance, Privacy and Intellectual Property Risk

AI depends on secure access to high-quality organizational data. Technology leaders establish enterprise environments, permissions, metadata, monitoring, and integration with trusted knowledge sources.

Questions Technology Leaders Should Ask

- Have we implemented secure enterprise AI environments whenever possible?
- Have we improved data quality, organization, metadata, and accessibility?
- Have we established permissions governing access to confidential information?
- Are we continuously monitoring data quality supporting AI applications?
- Have we integrated aI platforms with trusted enterprise knowledge rather than disconnected information sources?

4. Organizational and Workforce Risk

Technology choices can either support collaboration and responsible experimentation or create isolated practices. Technology leaders help enable knowledge sharing and monitor adoption for emerging workforce and workflow needs.

Questions Technology Leaders Should Ask

- Are we selecting AI tools that enhance collaboration rather than isolate users?
- Are we supporting enterprise knowledge sharing across project teams?
- Have we developed AI environments that encourage responsible experimentation?
- Are we monitoring AI adoption to identify training needs and workflow improvements?

5. Ethical, Regulatory and Reputational Risk

Ethical and reputational risk is influenced by platform transparency, security, explainability, bias, unintended outputs, and protection of client information.

Questions Technology Leaders Should Ask

- Are we selecting AI platforms supporting transparency, security, and explainability?

- Are we monitoring AI systems for bias, inappropriate outputs, and unintended consequences?
- Have we implemented governance controls protecting confidential information and client data?

6. Operational and Cybersecurity Risk

AI creates new operational, cybersecurity, vendor, and continuity risks. Technology leaders approve platforms, monitor use, strengthen protections, evaluate vendors, and plan for disruptions.

Questions Technology Leaders Should Ask

- Have we approved enterprise AI platforms before widespread organizational use?
- Are we monitoring employee use of AI applications?
- Have we strengthened cybersecurity protections supporting AI-enabled workflows?
- Are we evaluating AI vendors for security, reliability, and long-term viability?
- Have we developed contingency plans for AI system disruptions?

7. Financial and Business Model Risk

Technology investments should support enterprise capabilities and long-term business value rather than isolated use cases. Technology leaders help integrate AI with organizational systems and continually evaluate platforms and vendors.

Questions Technology Leaders Should Ask

- Are we prioritizing AI investments supporting enterprise capabilities rather than isolated use cases?
- Have we integrated AI with organizational knowledge and operational systems?
- Are we continuously evaluating emerging AI technologies for business value?
- Are we monitoring vendor capabilities as AI platforms evolve?

8. Strategic Leadership and Enterprise Governance Risk

Technology leaders support enterprise governance by building secure AI environments, integrating trusted organizational knowledge, evaluating emerging technologies, and providing transparency, monitoring, and reporting.

Questions Technology Leaders Should Ask

- Have we developed secure enterprise AI environments?
- Have we integrated AI platforms with trusted organizational knowledge?
- Are we continuously evaluating emerging technologies?
- Are we supporting governance through transparency, monitoring, and reporting?

The Role of Technology Leaders in Managing AI Risk

Taken together, these questions show that technology leadership's role in AI risk management extends from platform selection and cybersecurity to data quality, knowledge integration, monitoring, vendor oversight, business continuity, and governance transparency.

The full study concludes that AI risk is an enterprise issue rather than simply an information technology issue. Technology leaders therefore provide essential technical capabilities and controls while participating in shared governance across the organization.

For technology leaders, the objective is to create secure, reliable, transparent, and integrated AI environments that enable responsible experimentation and business value without creating unmanaged technical, operational, data, or vendor risk.

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*.**