



LEADING THROUGH AI RISK

A Practical Guide for Human Resources & Learning 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 Human Resources & Learning Leaders

Human Resources and Learning leaders have an important role in responsible AI adoption because many of the controls that determine whether AI is used effectively ultimately depend on people. Employee education, competency development, mentoring, organizational culture, leadership development, acceptable-use expectations, knowledge management, and continuous learning all influence the firm's exposure to AI-related risk.

HR does not own every AI risk. But HR has responsibilities within every domain and should work closely with executive leadership, engineering leaders, technology professionals, project delivery teams, and risk management and legal professionals.

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

1. Technical Reliability and Model Risk

AI-generated outputs can be inaccurate, incomplete, misleading, or difficult to explain. Engineering firms therefore need employees who understand AI's limitations and know when and how AI-assisted work must be independently evaluated.

Questions Human Resources & Learning Leaders Should Ask

- Are we training employees to recognize hallucinations, uncertainty, and other limitations of AI?
- Have we developed guidance to help employees understand appropriate AI use cases?
- Are we encouraging responsible experimentation while reinforcing professional expectations?

2. Professional Liability and Standard of Care Risk

Engineering firms remain responsible for their work regardless of the technologies used to produce it. HR and Learning functions help ensure professional judgment, responsible charge, and accountability remain embedded in employee development.

Questions Human Resources & Learning Leaders Should Ask

- Have we incorporated AI-related responsibilities into engineering training programs?
- Do our training and development programs reinforce that AI supplements, but never replaces, professional engineering judgment?
- Does our continuing education address AI governance, responsible charge, and evolving professional expectations?

3. Data Governance, Privacy and Intellectual Property Risk

As AI becomes more integrated into engineering work, employees need to understand how to handle confidential information, which AI platforms they may use, how organizational knowledge should be managed, and their responsibilities for privacy and intellectual property.

Questions Human Resources & Learning Leaders Should Ask

- Are we educating employees about the appropriate handling of confidential information?
- Are we providing clear guidance regarding approved AI platforms?
- Are we training staff on organizational knowledge management practices?
- Are we reinforcing employee responsibilities regarding privacy and intellectual property?

4. Organizational and Workforce Risk

AI is changing how engineers work, learn, develop professional judgment, and progress through their careers. Firms need to rethink training, mentoring, competency development, and career development as routine work becomes increasingly AI-enabled.

Questions Human Resources & Learning Leaders Should Ask

- Do our training and mentoring programs strengthen engineers' ability to critically evaluate AI-assisted work while reinforcing sound engineering judgment at every career stage?
- Have we updated our competency models to reflect AI-enabled engineering practice?
- Have we incorporated AI into onboarding, continuing education, and leadership development?
- Do we recognize and reward continuous learning?

5. Ethical, Regulatory and Reputational Risk

Engineering firms depend on ethical practice, client confidence, and public trust. Employees need clear expectations concerning responsible AI use and a culture in which concerns can be raised.

Questions Human Resources & Learning Leaders Should Ask

- Have we incorporated AI ethics into employee education and professional development?

- Are we reinforcing organizational expectations regarding responsible AI use?
- Do employees feel able to raise ethical concerns involving AI without fear of retaliation?

6. Operational and Cybersecurity Risk

AI is increasingly embedded in everyday work. Employees need to understand which tools are approved, how AI affects cybersecurity, how operational concerns should be reported, and how their responsibilities may change as AI capabilities evolve.

Questions Human Resources & Learning Leaders Should Ask

- Are we educating employees about approved AI tools and acceptable use?
- Are we reinforcing cybersecurity awareness related specifically to AI?
- Are we encouraging employees to report operational concerns involving AI technologies?
- Are we promoting continuous learning as AI capabilities evolve?

7. Financial and Business Model Risk

AI is expected to change more than productivity. It may affect roles, skills, service delivery, client value, and the long-term business model of engineering firms. HR therefore has a role in preparing the workforce for how engineering work itself may evolve.

Questions Human Resources & Learning Leaders Should Ask

- Are we preparing employees for evolving engineering roles?
- Are we aligning professional development with the firm's future organizational needs?
- Are we recognizing the skills that support innovation, collaboration, and AI-enabled engineering practice?
- Are we encouraging continuous organizational learning?

8. Strategic Leadership and Enterprise Governance Risk

AI has become an enterprise leadership issue. HR contributes by building AI literacy, preparing leaders, and supporting the organizational learning required for responsible adoption.

Questions Human Resources & Learning Leaders Should Ask

- Are we building AI literacy across every level of the organization?
- Have we redesigned leadership development for an AI-enabled profession?
- Are we encouraging continuous learning and interdisciplinary collaboration?
- Are we preparing future leaders to govern AI responsibly?

The Role of HR in Managing AI Risk

Taken together, these questions illustrate an important point from the research: **HR's role in AI risk management extends far beyond AI training.** HR and Learning functions help determine whether employees understand AI's limitations, whether professional judgment continues to develop, whether confidential information is handled appropriately, whether employees understand the firm's ethical expectations, whether emerging skills are incorporated into workforce development, and whether current and future leaders are prepared to govern AI responsibly.

The full study concludes that AI risk cannot be effectively managed through isolated policies or individual technology investments. Effective mitigation requires coordinated action across the organization, with each function contributing its expertise to a shared governance structure.

For Human Resources and Learning leaders, the objective is therefore not to become experts in every aspect of AI. It is to ensure that the people, competencies, learning systems, leadership development, and organizational culture required for responsible AI adoption are keeping pace with the technology.

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.***](#)