ACEC RESEARCH INSTITUTE
FIRM OF THE FUTURE

LEADING THROUGH AI RISK

THE ENTERPRISE FRAMEWORK FOR ENGINEERING FIRM LEADERS

AUGUST 2026

TABLE OF CONTENTS

ACKNOWLEDGMENTS

The ACEC Research Institute gratefully acknowledges the many individuals and organizations whose time, expertise, and thoughtful perspectives made this research possible. This study benefited from the participation of engineering firm leaders, public infrastructure owners, technology providers, AI consultants, insurance and legal professionals, and representatives of the engineering licensing community, all of whom generously shared their experiences and insights throughout the research process. Their willingness to discuss both the opportunities and challenges associated with artificial intelligence significantly strengthened the quality and practical relevance of this report.

The Institute also extends its appreciation to the members of the ACEC Risk Committee and the ACEC Technology Committee for their guidance, thoughtful feedback, and ongoing support throughout the development of this research. Their perspectives helped shape the study's direction and ensured that the findings remain grounded in the realities facing engineering firms today.

While this report reflects the collective knowledge and experience shared by many contributors, the findings, conclusions, and recommendations presented are those of the ACEC Research Institute and are intended to support continued discussion and informed decision-making across the engineering profession.

READER'S NOTE

This report is part of the ACEC Research Institute's broader Firm of the Future research initiative, which examines how artificial intelligence and other emerging technologies are reshaping the engineering profession. Previous studies explored the strategic implications of AI adoption, workforce transformation, and the future evolution of engineering firms. This report builds upon that foundation by addressing a complementary question: as engineering firms increasingly adopt AI, what organizational risks emerge, and how can those risks be identified, governed, and mitigated? Together, these studies provide engineering leaders with a comprehensive body of research to help navigate the opportunities, challenges, and responsibilities associated with AI-enabled transformation.

Transparency Statement

AI-assisted tools were used to support qualitative analysis, organization of research findings, and editorial drafting during preparation of this report. All research decisions, interpretations, conclusions, recommendations, and final editorial content reflect the independent judgment and responsibility of the author.

Artificial intelligence is introducing new risks across every aspect of the engineering enterprise, requiring firms to manage organizational capability—not just technology.

INTRODUCTION AND RESEARCH OVERVIEW

Artificial intelligence is transforming engineering practice at an unprecedented pace. While much of the current discussion focuses on technological capability, this report examines a different question: What new risks does AI create for engineering firms, and how can those risks be managed responsibly? Drawing upon an extensive literature review and interviews with leaders representing every major stakeholder group within the engineering ecosystem, this research identifies the principal AI-related risks facing engineering firms and presents a practical framework for mitigating them.

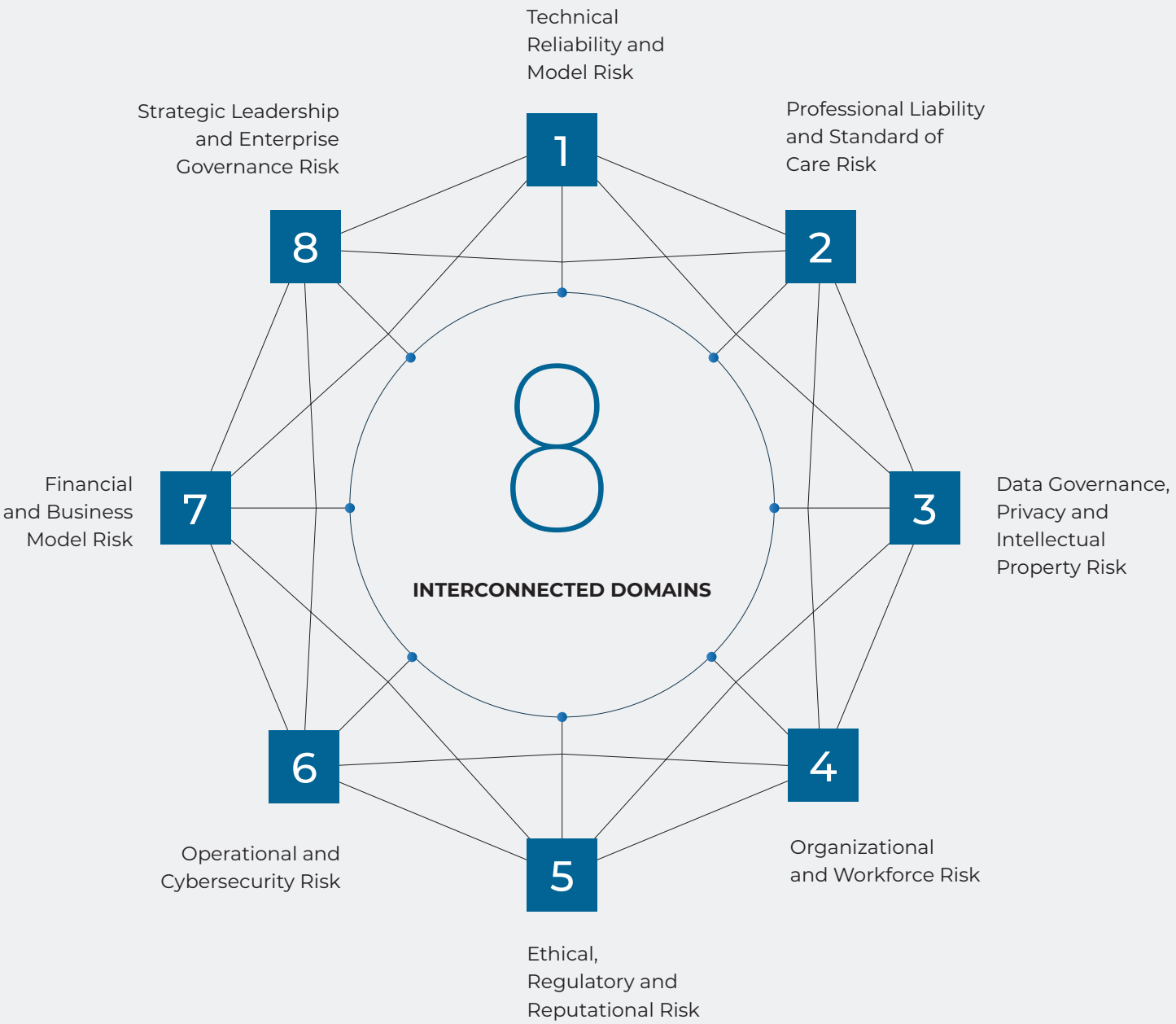
New AI-enabled tools are changing how engineers search for information, develop designs, analyze alternatives, prepare documentation, communicate with clients, and manage projects. These technologies offer significant opportunities to improve productivity, enhance decision-making, strengthen quality, and create new forms of value for clients. At the same time, they introduce new categories of risk that extend well beyond the technology itself.

Unlike many emerging technologies, AI influences nearly every aspect of an engineering organization. Its adoption has implications for technical quality, professional responsibility, data governance, workforce development, ethics, cybersecurity, business operations, financial performance, and organizational leadership. As a result, engineering firms can no longer view AI solely as a technology initiative. Managing AI effectively requires an enterprise-wide approach to risk management, governance, and organizational readiness.

Recognizing this need, the ACEC Research Institute conducted this study to identify the most significant AI-related risks facing engineering firms and to provide practical guidance for mitigating those risks. The research combined an extensive review of published literature 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. The findings informed the development of a comprehensive AI Risk Framework organized around eight interconnected domains that together represent the principal organizational risks associated with AI adoption.

Perhaps the most important finding was not simply the identification of these risks, but the strong convergence of perspectives across the stakeholder groups interviewed. Although participants approached AI from very different professional perspectives, they consistently identified many of the same organizational challenges and reached similar conclusions regarding how engineering firms should respond. This convergence suggests that AI risk is becoming increasingly well understood across the engineering ecosystem and that responsible adoption depends less on individual technologies than on the organizational capabilities required to govern them effectively.

The research identified eight interconnected domains that collectively define the AI risk landscape for engineering firms:



1

Technical Reliability and Model Risk – AI-generated outputs require rigorous verification, validation, and professional review to ensure technical accuracy and protect public safety.

2

Professional Liability and Standard of Care Risk – The licensed engineer remains responsible for engineering decisions regardless of how AI is used during project delivery.

3

Data Governance, Privacy and Intellectual Property Risk – High-quality, well-governed organizational data has become a strategic asset and a prerequisite for successful AI implementation.

4

Organizational and Workforce Risk – AI is changing how engineers develop professional judgment, requiring firms to rethink learning, training, mentoring, and career development.

5

Ethical, Regulatory and Reputational Risk – Maintaining public trust requires transparency, accountability, and responsible governance of AI-enabled engineering practices.

6

Operational and Cybersecurity Risk – AI must be integrated into existing quality management, cybersecurity, business continuity, and enterprise risk management processes.

7

Financial and Business Model Risk – Competitive advantage will increasingly depend upon using AI to create greater client value rather than simply improving internal efficiency.

8

Strategic Leadership and Enterprise Governance Risk – Successful AI adoption ultimately depends upon leadership establishing the governance, culture, and organizational capabilities necessary to manage AI responsibly.

Collectively, these findings demonstrate that AI risk is fundamentally organizational rather than purely technological. While individual AI tools will continue evolving rapidly, the long-term success of engineering firms will depend upon their ability to strengthen the organizational capabilities that enable responsible adoption. Throughout the interviews, participants consistently emphasized that governance, engineering judgment, workforce development, data stewardship, and leadership are becoming increasingly important—not less important—as AI capabilities continue to advance.

The research also challenges several common assumptions about AI. Participants consistently rejected the notion that AI will replace professional engineering judgment or diminish the role of licensed engineers. Instead, they emphasized that AI increases the importance of human oversight, independent verification, ethical decision-making, and organizational accountability. Similarly, stakeholders viewed AI as a catalyst for broader business transformation rather than simply another software application to be deployed within the IT department.

The practical implication for engineering firms is clear. AI risk cannot be managed through technology alone. Effective risk mitigation requires coordinated action across engineering, operations, information technology, legal, human resources, executive leadership, and other functional areas. Organizations that integrate AI governance into existing business processes, invest in workforce development, strengthen data governance, and establish clear accountability will be better positioned to realize AI's benefits while protecting clients, preserving professional standards, and maintaining public trust.

Artificial intelligence will continue reshaping engineering practice for years to come. The profession's fundamental responsibility, however, remains unchanged. Engineers will continue to protect the health, safety, and welfare of the public while delivering trusted, high-quality engineering services. The challenge facing engineering firms is therefore not whether to adopt AI, but how to do so responsibly. This report provides a practical framework for understanding AI-related risks and offers guidance to help engineering firms strengthen governance, improve organizational readiness, and mitigate risk while embracing the opportunities that artificial intelligence creates.

The long-term success of engineering firms will depend upon their ability to strengthen the organizational capabilities that enable responsible adoption.

1 ENGINEERING AT AN INFLECTION POINT

Engineering has always evolved through technological innovation, yet its defining responsibility has never changed: protecting the health, safety, and welfare of the public through sound engineering judgment. From hand calculations to computer-aided design, building information modeling (BIM), and advanced simulation tools, each generation of technology has expanded the profession's capabilities while leaving its fundamental obligations intact.

Artificial intelligence represents the next major evolution in that progression. Unlike previous technologies, however, AI has the potential to influence decisions across nearly every function of an engineering firm—from technical analyses and project delivery to business operations, workforce development, client service, and strategic decision-making. As a result, AI introduces risks that are organizational as much as they are technical.

The opportunities are significant. AI offers the potential to improve productivity, accelerate project delivery, reduce repetitive work, enhance decision support, strengthen knowledge management, improve asset performance, and allow engineers to devote more time to higher-value activities requiring creativity, collaboration, and professional judgment. Across the engineering industry, firms are actively experimenting with AI tools, technology providers are rapidly integrating AI into engineering software, infrastructure owners are beginning to incorporate AI into project delivery and asset management, and regulators, insurers, and professional organizations are working to understand the implications of this rapidly evolving technology.

At the same time, AI introduces important questions that extend well beyond technology itself. How should engineering firms govern AI? What new risks accompany AI-assisted engineering work? How should firms balance innovation with professional responsibility? How should organizations protect confidential information, intellectual property, and client trust? How will AI affect engineering judgment, workforce development, business models, and the long-term competitiveness of engineering firms? And perhaps most importantly, what responsibilities remain uniquely human in a profession where public safety depends upon the quality of engineering decisions?

These questions are becoming increasingly urgent.

AI capabilities continue to evolve at a pace that exceeds the development of industry standards, organizational policies, regulatory guidance, and accepted professional practices. Many engineering firms are already adopting AI through individual experimentation, enterprise software platforms, and emerging business applications, often without comprehensive governance frameworks or a clear understanding of the associated risks. Meanwhile, clients increasingly expect greater efficiency, technology providers continue expanding AI capabilities, regulators are evaluating how existing professional standards apply to AI-assisted practice, and competitors are exploring new business models enabled by AI.

Collectively, these developments place the engineering profession at an important inflection point.

Why This Study Was Conducted

Although AI has become one of the most widely discussed technologies in business, relatively little research has examined AI specifically through the lens of engineering practice. Existing literature provides valuable insights into AI ethics, cybersecurity, privacy, intellectual property, algorithmic bias, governance, and regulatory issues. Likewise, engineering literature increasingly explores AI applications across planning, design, construction, infrastructure management, and operations.

However, most existing research examines these topics independently. While numerous publications have explored the technical capabilities, opportunities, and risks associated with artificial intelligence, relatively little research has examined AI risk through the unique lens of professional engineering. Even fewer studies have considered AI risk from the combined perspectives of engineering firms, public and private clients, technology providers, insurers, legal professionals, licensing authorities, and AI consultants.

This study was designed to address that gap by developing a comprehensive framework for understanding AI risk and identifying practical strategies that engineering firms can use to mitigate those risks.

Rather than focusing exclusively on AI capabilities or technology trends, the study seeks to answer two practical questions that engineering leaders are increasingly asking:

- What are the potential risks associated with AI adoption across engineering firms?
- What can firms—and the engineering industry more broadly—do to manage those risks while capturing AI's potential benefits?

These questions recognize that responsible AI adoption requires more than selecting software or developing technical expertise. It requires leadership, governance, organizational preparedness, and a clear understanding of how AI intersects with the engineering profession's longstanding obligations to clients and society.

Why Engineering Is Different

The engineering profession occupies a unique position within the broader AI landscape. Unlike many industries, engineering decisions have direct consequences for public safety, environmental stewardship, economic investment, and the performance of critical infrastructure. Bridges, transportation systems, water treatment facilities, energy systems, buildings, and other essential infrastructure are expected to perform safely and reliably for decades. Decisions made during planning and design often influence communities for generations.

Consequently, engineering firms operate within an environment characterized by professional licensure, established standards of care, contractual obligations, regulatory oversight, quality assurance processes, and ethical responsibilities that extend beyond commercial considerations. AI therefore introduces a distinct set of challenges for engineering organizations.

In many industries, AI errors may primarily affect efficiency, customer experience, or financial performance. Within engineering, AI-related errors may also affect public safety, project performance, legal liability, professional licensure, organizational reputation, and client trust. The consequences of poor governance may therefore extend well beyond technology itself.

At the same time, engineering firms cannot afford to ignore AI. Many participants in this study observed that the greater long-term risk may not be adopting AI too quickly, but rather failing to adapt as clients, competitors, technology providers, and infrastructure owners increasingly embrace AI-enabled ways of working. Responsible AI adoption therefore requires balancing two competing realities: managing the risks associated with AI while avoiding the strategic risks associated with inaction.

Research Approach

To better understand this evolving landscape, the ACEC Research Institute conducted one of the industry's most comprehensive qualitative examinations of AI risk management in engineering.

The research began with an extensive review of academic literature, professional guidance, regulatory publications, legal analyses, industry reports, and emerging frameworks related to artificial intelligence, enterprise risk management, engineering practice, cybersecurity, ethics, governance, and organizational transformation. This review informed the development of a comprehensive AI Risk Framework designed specifically for engineering firms.

The framework then served as the foundation for 21 in-depth interviews representing six stakeholder groups that collectively shape AI adoption across the engineering ecosystem:

Engineering firm leaders representing firms of varying sizes.

Public-sector infrastructure owners and clients.

Technology vendors serving the engineering industry.

Insurance and legal professionals specializing in engineering risk.

Professional licensing and regulatory authorities.

AI consultants working with engineering organizations on strategy and implementation.

This multi-stakeholder approach was intentional. Each group experiences AI from a different perspective. Engineering firms focus on implementation. Clients focus on quality and accountability. Technology providers focus on innovation and capability. Legal and insurance experts focus on liability and risk allocation. Licensing authorities focus on professional responsibility and public protection. AI consultants focus on organizational transformation and strategic readiness. Taken together, these perspectives provide a more complete understanding of AI risk than any single stakeholder group could offer independently.

As with any qualitative research, the purpose of this study was not to measure the prevalence of specific views across the engineering profession, but to explore how experienced stakeholders understand emerging AI risks and identify areas of common concern. The 21 participants were intentionally selected to represent diverse perspectives across the engineering ecosystem and to provide informed insights based on their professional experience with AI adoption. Accordingly, the convergence observed throughout this report should be interpreted as reflecting common themes among these informed stakeholder groups rather than a statistical measure of industry-wide agreement.

A Central Finding

Although participants discussed dozens of individual risks—including hallucinations, cybersecurity, data governance, intellectual property, legal liability, workforce disruption, organizational readiness, business model transformation, and competitive pressure—one overarching theme consistently emerged across the stakeholder groups represented in this study.

> Artificial intelligence does not reduce the engineering profession's responsibility. Instead, it raises the standard for governance, engineering judgment, and organizational leadership.

Engineering firms may increasingly rely on AI to support analysis, automate repetitive work, improve decision-making, and accelerate project delivery. Yet every stakeholder group—from engineering executives and public clients to attorneys, insurers, technology providers, licensing officials, and AI consultants—returned to the same underlying principle: engineers remain responsible for the quality of the work they deliver. This finding fundamentally reframes the discussion surrounding AI risk.

The most significant challenge facing engineering firms is not simply selecting the right AI tools. It is building organizations capable of governing AI responsibly while preserving the professional judgment, accountability, and public trust that define engineering practice.

About This Report

The chapters that follow examine the emerging AI risk landscape, present a practical framework for understanding AI risk in engineering firms, synthesize findings from the literature review and stakeholder interviews, and explore each of the eight AI risk domains in detail. Throughout the report, the emphasis remains on helping engineering firms better understand AI risks and strengthen their ability to govern, manage, and mitigate those risks while continuing to fulfill their professional responsibility to protect the public.

2 THE EMERGING AI RISK LANDSCAPE

Artificial intelligence has progressed from a specialized research topic to one of the most significant technological developments affecting business and society. Within only a few years, advances in machine learning, generative AI, large language models, computer vision, and autonomous agents have transformed AI from a collection of niche applications into an increasingly accessible capability that is reshaping how organizations create knowledge, make decisions, automate work, and deliver value.

For engineering firms, this transformation presents extraordinary opportunities. AI has the potential to accelerate design, automate repetitive tasks, improve knowledge management, strengthen project delivery, enhance infrastructure operations, support predictive analytics, and increase organizational productivity. As AI capabilities continue to evolve, many firms anticipate that AI will become deeply embedded within virtually every aspect of engineering practice.

Yet AI also introduces new forms of uncertainty. Unlike previous generations of engineering technology, AI is capable of generating recommendations, creating original content, identifying patterns, and supporting decisions that have traditionally depended upon human expertise. Consequently, organizations are no longer evaluating only the performance of software—they are evaluating how intelligent systems influence professional judgment, organizational decision-making, client relationships, workforce development, and enterprise risk.

This distinction is critical. Previous generations of engineering software generally improved how engineers performed specific tasks. Artificial intelligence has the potential to influence how organizations make decisions, manage knowledge, develop talent, interact with clients, and govern professional practice. As AI capabilities expand, engineering firms must therefore evaluate not only whether AI works, but how AI changes the way the organization itself operates.

This shift has fundamentally changed how researchers, technology providers, regulators, and business leaders think about AI risk.

The Evolution of AI Risk

Early discussions surrounding artificial intelligence focused primarily on technical issues. Researchers examined algorithmic performance, data quality, computational limitations, cybersecurity vulnerabilities, privacy protection, and system reliability. As AI applications expanded beyond research laboratories into commercial environments, attention increasingly shifted toward questions of algorithmic bias, explainability, transparency, accountability, and ethical decision-making.

The rapid emergence of generative AI accelerated this evolution. Unlike traditional software, generative AI systems produce original text, images, computer code, analyses, and recommendations that often appear authoritative regardless of their accuracy. Organizations quickly recognized that AI-related risks extended far beyond technology infrastructure. Hallucinations, misinformation, intellectual property concerns, confidentiality, cybersecurity, regulatory uncertainty, workforce disruption, and organizational governance became central topics within both academic research and industry practice.

As AI matured, the conversation expanded again. Increasingly, researchers began viewing AI as an enterprise issue rather than simply an information technology issue. Organizations recognized that AI implementation influences strategic planning, organizational structure, risk management, human resources, legal compliance, finance, operations, ethics, customer relationships, and corporate governance. Successful AI adoption therefore depends as much upon leadership, organizational readiness, and governance as upon technical capability.

Today, AI risk is widely recognized as multidimensional. Rather than existing as isolated technical concerns, AI risks interact across organizations in complex ways. A cybersecurity vulnerability may expose confidential client information. Poor data governance may increase hallucinations. Weak organizational oversight may create legal liability. Workforce challenges may influence quality assurance. Ethical failures may damage client trust and organizational reputation. These interdependencies have led researchers to advocate increasingly comprehensive approaches to AI governance.

For engineering firms, this interconnectedness has important implications. AI risks rarely originate and remain within a single department. Decisions regarding technology selection may influence professional liability. Workforce training affects technical reliability. Data governance shapes cybersecurity, intellectual property protection, and organizational knowledge. Effective AI risk management therefore requires coordinated governance across the enterprise rather than isolated solutions developed within individual functions.

AI Risk in the Engineering Profession

While many AI risks are common across industries, engineering presents several characteristics that distinguish it from other sectors.

Engineering firms design and manage infrastructure systems upon which communities depend for transportation, water, energy, public safety, environmental protection, communications, and economic development. Consequently, engineering decisions frequently carry long-term consequences extending well beyond individual organizations.

Professional engineering also operates within an established framework of licensure, standards of care, quality assurance, contractual obligations, regulatory oversight, and ethical responsibilities. Engineering firms are expected to exercise independent professional judgment while protecting the health, safety, and welfare of the public. These obligations remain regardless of the technologies used during project delivery.

Artificial intelligence therefore introduces a unique challenge. Engineering organizations must simultaneously pursue innovation while preserving professional accountability. AI may improve efficiency, expand analytical capabilities, and automate repetitive work, yet firms remain responsible for ensuring the accuracy, completeness, and reliability of every engineering deliverable. This balance between innovation and responsibility distinguishes engineering from many other industries adopting AI.

What the Literature Tells Us

The literature reviewed for this study consistently identifies several broad categories of AI risk relevant to engineering organizations. At the technical level, researchers emphasize concerns regarding hallucinations, model reliability, explainability, cybersecurity, data quality, privacy, and system security. At the organizational level, the literature highlights governance, organizational readiness, workforce development, change management, policy development, leadership, and enterprise risk management.

Legal and regulatory publications focus on professional liability, intellectual property, contractual obligations, privacy regulation, standards of care, and evolving compliance requirements. Ethics literature emphasizes fairness, transparency, accountability, human oversight, bias mitigation, responsible decision-making, and public trust. Business literature increasingly examines AI's influence on competitive advantage, business model innovation, productivity, workforce transformation, organizational resilience, and long-term strategic positioning.

Collectively, this body of research demonstrates that AI risk extends far beyond technology itself. Organizations adopting AI must consider not only whether AI performs effectively, but also how AI affects governance, decision-making, organizational culture, client relationships, regulatory compliance, and strategic competitiveness.

Limitations of Existing Research

Although the existing literature provides valuable insights into specific AI risks, several important limitations remain. First, much of the current research examines individual categories of risk in isolation. Technical publications often emphasize cybersecurity, algorithms, or model performance. Legal analyses focus on liability and regulation. Ethics research concentrates on fairness, transparency, and accountability. Business literature examines organizational transformation and competitive strategy. Comparatively little research integrates these perspectives into a unified view of enterprise AI risk.

Second, relatively little research focuses specifically on engineering firms. Much of the published literature reflects experiences from technology companies, financial services, healthcare, manufacturing, or other sectors where organizational structures, regulatory environments, professional responsibilities, and operational risks differ substantially from those of consulting engineering firms.

Finally, existing research rarely incorporates the perspectives of the multiple stakeholder groups that collectively influence engineering practice. Engineering firms, infrastructure owners, technology providers, insurers, legal experts, licensing authorities, and AI strategy advisors each experience AI through different professional lenses. Understanding AI risk therefore requires integrating these complementary perspectives rather than relying upon any single viewpoint.

These limitations suggest that engineering leaders need a more comprehensive framework for understanding AI risk—one that reflects both the breadth of existing research and the realities of engineering practice.

From AI Risks to AI Governance

One of the clearest observations emerging from the literature is that AI risk cannot be effectively managed through technology alone. Organizations increasingly recognize that successful AI adoption depends upon governance structures capable of integrating technical controls with organizational leadership, policy development, workforce education, quality assurance, legal compliance, and ethical decision-making.

This represents an important evolution in thinking.

The central question is no longer whether AI creates risk. The literature overwhelmingly demonstrates that it does. Instead, the more important question has become how organizations should govern AI in ways that enable innovation while maintaining accountability, protecting stakeholder trust, and managing enterprise risk.

For engineering firms, this challenge is particularly significant. AI must be integrated into organizations that already operate under demanding professional standards, regulatory expectations, contractual obligations, and public responsibilities. Effective governance therefore requires understanding not only individual AI risks, but also how those risks interact across the engineering enterprise.

Many participants also emphasized a less frequently discussed dimension of AI risk: the risk of failing to adapt. As clients, competitors, software providers, and infrastructure owners increasingly incorporate AI into engineering practice, organizations that delay adoption indefinitely may face growing strategic disadvantages. Responsible AI leadership therefore requires balancing two realities simultaneously: managing the risks associated with AI while avoiding the equally significant risks associated with organizational inaction.

The next chapter introduces an integrated AI Risk Framework developed specifically for engineering firms. Building upon the literature reviewed for this study, the framework organizes AI risk into eight interrelated domains that collectively capture the technical, organizational, legal, ethical, operational, financial, and strategic dimensions of responsible AI adoption.

The framework is more than a method for classifying AI risks. It provides engineering leaders with a practical way to understand where risks emerge, how they interact across the organization, and how they can be mitigated through effective governance, sound engineering judgment, and disciplined organizational leadership.

3 AN AI RISK FRAMEWORK FOR ENGINEERING FIRMS

The previous chapter demonstrated that artificial intelligence introduces a broad spectrum of technical, operational, legal, ethical, financial, and strategic risks. It also highlighted an important limitation in the existing literature: these risks are typically discussed independently, often within the boundaries of individual disciplines. Cybersecurity research focuses on cyber threats. Legal publications emphasize liability and regulation. Ethics literature examines fairness and accountability. Business publications discuss organizational transformation and competitive strategy.

Engineering firms, however, do not experience AI risk one domain at a time. They experience AI as an enterprise capability that simultaneously affects engineering practice, organizational knowledge, workforce development, business operations, client relationships, and strategic decision-making. Decisions made in one area frequently influence risks in another. As a result, engineering firms require a framework that reflects how AI risk actually emerges and is managed across the organization—not how it is discussed in individual disciplines.

Why a Framework Is Necessary

Every engineering firm already manages risk. Organizations routinely evaluate project risks, contractual risks, safety risks, financial risks, cybersecurity risks, operational risks, and strategic risks. These risks are typically managed through governance processes, quality assurance programs, enterprise risk management systems, professional standards, and executive oversight. Artificial intelligence should not be viewed as a separate category of organizational risk operating outside these existing management systems.

The purpose of this framework is not to create a new category of organizational risk. Rather, it provides engineering leaders with a practical way to understand how AI influences existing risks, where new risks emerge, and how governance can be strengthened to address them. In this sense, the framework serves as an organizing model for enterprise AI risk management rather than a standalone compliance tool.

Consequently, firms require a framework that enables leaders to understand:

WHERE AI RISKS ORIGINATE?

HOW RISKS INTERACT?

WHICH ORGANIZATIONAL FUNCTIONS ARE AFFECTED?

WHO SHOULD BE RESPONSIBLE FOR MANAGING EACH RISK?

HOW GOVERNANCE SHOULD EVOLVE AS AI CAPABILITIES MATURE?

Rather than creating entirely new management systems, engineering firms should integrate AI governance into existing organizational structures while recognizing that AI creates important new relationships between technology, engineering practice, and business strategy.

Principles Guiding the Framework

Several principles shaped the development of this framework.

AI Risk Is Enterprise Risk

Perhaps the most important principle underlying the framework is that AI risk should not be treated solely as an information technology issue. AI influences engineering workflows, project delivery, organizational governance, professional liability, workforce development, financial performance, client relationships, regulatory compliance, and long-term competitiveness. Executive leadership, not only technology leadership, must therefore play a central role in AI governance.

AI Risks Are Interconnected

Individual AI risks rarely occur in isolation. A technical failure may expose confidential information. Weak governance may lead to inappropriate AI use. Poor workforce training may increase hallucinations entering engineering deliverables. Insufficient quality assurance may create professional liability. Financial pressures may encourage organizations to prioritize efficiency over appropriate oversight. Understanding these interactions is often more important than understanding individual risks independently.

AI Risk Is Dynamic

Artificial intelligence continues to evolve rapidly. New foundation models, enterprise platforms, agentic AI systems, engineering-specific applications, regulatory guidance, and client expectations continue to emerge. Consequently, AI governance cannot remain static. Organizations should view AI risk management as a continuous process requiring ongoing monitoring, policy refinement, workforce education, and organizational learning.

Responsible Innovation Requires Balance

The purpose of AI governance is not to slow innovation. Nor is it to encourage rapid adoption without sufficient safeguards. Rather, effective governance enables organizations to capture AI's benefits while maintaining professional responsibility, client trust, organizational resilience, and public confidence. The objective is responsible innovation.

The Eight Domains of AI Risk

Taken together, the literature review and stakeholder interviews suggest that AI risk can be understood through eight interrelated domains. Although each domain represents a distinct category of risk, they are intentionally organized as an integrated framework because engineering firms experience these risks simultaneously rather than independently.

1

Technical Reliability and Model Risk

This domain addresses the technical performance of AI systems, including hallucinations, model accuracy, explainability, validation, reliability, and the ability of engineers to understand and verify AI-generated outputs. Although these risks often receive the greatest public attention, they represent only one component of enterprise AI governance.

2

Professional Liability and Standard of Care Risk

Engineering firms remain professionally responsible for every deliverable regardless of the technologies used during project execution. This domain examines how AI influences engineering judgment, quality assurance, contractual obligations, professional liability, responsible charge, and standards of care.

3

Data Governance, Privacy and Intellectual Property Risk

AI depends upon data. Consequently, organizations must address data quality, confidentiality, privacy, cybersecurity, intellectual property, knowledge management, and ownership of organizational information. As AI becomes increasingly integrated into engineering workflows, data governance becomes a strategic organizational capability rather than simply a technical function.

4

Organizational and Workforce Risk

Successful AI implementation depends upon people as much as technology. This domain examines workforce readiness, organizational culture, employee training, change management, talent development, workforce transformation, and the evolving relationship between engineers and AI.

5

Ethical, Regulatory and Reputational Risk

Engineering organizations operate within established ethical standards, professional licensure requirements, regulatory frameworks, and public expectations. This domain considers fairness, transparency, accountability, bias, regulatory compliance, organizational reputation, client trust, and broader societal implications associated with AI adoption.

6

Operational and Cybersecurity Risk

AI influences day-to-day organizational operations while simultaneously introducing new cybersecurity considerations. This domain addresses operational resilience, system integration, cybersecurity, third-party technology risks, business continuity, incident response, and organizational resilience.

7

Financial and Business Model Risk

Artificial intelligence influences far more than operational efficiency. Organizations must consider investment decisions, return on investment, pricing strategies, utilization, client expectations, commoditization, competitive differentiation, emerging revenue models, and long-term business sustainability.

8

Strategic Leadership and Enterprise Governance Risk

The final domain recognizes that AI has become a leadership issue. Executive teams must establish governance structures, define organizational strategy, assign accountability, oversee AI adoption, measure organizational maturity, manage enterprise risk, and continuously adapt as AI capabilities evolve. Because this domain influences every other category, it serves as the integrating mechanism through which engineering firms coordinate responsible AI adoption across the enterprise.

Understanding the Relationships Between the Domains

Although each domain can be examined independently, the framework is intentionally designed as an integrated system.

For example, an organization introducing generative AI into proposal development may initially view the initiative as a productivity improvement. However, successful implementation also requires trusted organizational data, cybersecurity protections, intellectual property safeguards, employee training, governance policies, executive oversight, quality assurance procedures, and consideration of long-term business strategy.

Similarly, deploying AI to support engineering analysis involves more than evaluating technical accuracy. Firms must also consider engineering judgment, standards of care, professional liability, regulatory expectations, client confidence, organizational competence, and workforce development.

In practice, AI risks cascade across organizational boundaries. Consequently, governance decisions made by executive leadership often influence multiple risk domains simultaneously. Viewing AI through an enterprise framework helps organizations recognize these interdependencies before individual risks become organizational failures.

This interconnected perspective represents one of the framework's most important contributions. Rather than encouraging organizations to manage AI risks within isolated departments, it emphasizes that effective mitigation depends upon coordinated governance across the enterprise. The framework therefore shifts the discussion from managing individual AI technologies to managing the organizational capabilities required to use AI responsibly.

From Framework to Practice

The framework presented in this chapter establishes the conceptual foundation for the remainder of this report. The chapters that follow move beyond theory by examining how leaders from across the engineering ecosystem understand these risks in practice. Drawing upon interviews with engineering firms, public infrastructure owners, technology providers, insurance and legal experts, professional licensing authorities, and AI consultants, the report explores where stakeholders agree, where their perspectives differ, and what engineering firms can do to govern AI responsibly.

Taken together, the literature, the framework, and the interview findings provide a comprehensive view of AI risk management specifically tailored to the engineering profession. Rather than asking whether organizations should adopt AI, the framework shifts the conversation toward a more important question:

How can engineering firms adopt AI in ways that strengthen innovation while preserving engineering judgment, professional responsibility, organizational resilience, and public trust?

The framework presented in this chapter should therefore be viewed as a practical management tool rather than a theoretical model. It provides engineering leaders with a structured way to understand how AI risks interact across the organization, identify where governance responsibilities reside, and evaluate how individual decisions influence enterprise-wide risk. The chapters that follow build upon this foundation by translating the framework into practical guidance informed by the collective experience of leaders from across the engineering ecosystem.

4 TECHNICAL RELIABILITY AND MODEL RISK

RELIABLE AI DEPENDS UPON RELIABLE ORGANIZATIONS.

AI reliability is not determined solely by the technology itself. It depends on trusted data, disciplined governance, robust quality assurance, and sound engineering judgment.

What Is the Risk?

Technical reliability is often the first risk organizations associate with artificial intelligence. Public discussion frequently focuses on hallucinations, inaccurate outputs, fabricated citations, algorithmic bias, model drift, explainability, and other technical limitations of modern AI systems. These concerns are legitimate because engineering firms cannot rely on information that is inaccurate, incomplete, or impossible to verify.

However, the literature suggests that technical failures are only part of the challenge. Unlike conventional engineering software, generative AI produces probabilistic rather than deterministic outputs. AI systems can generate responses that appear technically correct while containing subtle errors, unintended omissions, unsupported assumptions, or incomplete analyses. As AI becomes integrated into engineering workflows, firms must ensure that these outputs do not compromise engineering quality, professional judgment, or client confidence.

For engineering firms, the fundamental risk is therefore not simply that AI makes mistakes. The greater risk is that incorrect or poorly understood AI-generated information influences engineering decisions without appropriate validation and professional review.

What Did We Learn?

The interviews revealed a broader understanding of technical reliability than is commonly reflected in the literature. While nearly every participant acknowledged hallucinations and technical inaccuracies, very few viewed them as the profession's greatest concern. Instead, participants consistently emphasized that technical reliability depends less on AI itself than on the systems engineering firms establish to govern its use.

Engineering judgment remains the primary safeguard.

> I don't really care whether you use AI. I care whether the answer is right.
>
> **PUBLIC INFRASTRUCTURE OWNER**

Participants across the stakeholder groups interviewed consistently emphasized that AI should support—not replace—engineering judgment. Engineering firm leaders described AI as another engineering tool requiring the same professional skepticism applied to structural analysis software, hydraulic models, or other computational technologies. Legal experts emphasized that liability arises not because AI occasionally produces incorrect information, but because engineers fail to appropriately review and validate AI-assisted work. Licensing authorities reinforced that engineers remain responsible for understanding and exercising responsible charge over all work they sign and seal. Together, these perspectives demonstrate that technical reliability depends as much upon disciplined engineering review as upon the performance of the AI system itself.

TRUSTED DATA MATTERS AS MUCH AS TRUSTED AI.

Technology vendors and AI consultants consistently argued that organizations often overestimate the importance of selecting the "right" AI model while underestimating the importance of the data supporting that model. Several participants explained that hallucinations frequently occur because AI lacks sufficient engineering context rather than because the underlying technology is fundamentally unreliable.

Organizations with well-governed enterprise knowledge, project histories, engineering standards, and structured data are far more likely to receive reliable outputs than organizations relying exclusively on publicly available information.

PUBLIC CLIENTS FOCUS ON OUTCOMES—NOT TECHNOLOGY.

Public infrastructure owners expressed surprisingly little concern regarding whether engineering firms use AI. Instead, they consistently emphasized confidence in engineering deliverables. Clients assume engineering firms will select appropriate tools while maintaining the same standards of quality, accuracy, and accountability regardless of how work is produced.

RELIABILITY IS AN ORGANIZATIONAL CAPABILITY.

Perhaps the most significant finding emerging from the interviews is that technical reliability should not be viewed solely as a software characteristic. Rather, reliable AI depends upon reliable organizations. Organizations with disciplined governance, experienced engineers, trusted data, robust QA/QC procedures, and effective validation processes consistently expressed greater confidence in AI adoption than organizations relying primarily on the technology itself.

What Can Engineering Firms Do?

The interviews identified several practical actions engineering firms can take to strengthen technical reliability while enabling responsible AI adoption.

Executive Leadership

- Establish clear organizational policies defining appropriate AI use.
- Ensure AI governance receives executive oversight rather than remaining solely an IT responsibility.
- Invest in enterprise knowledge management and trusted organizational data.

Engineering Leaders

- Require human review of AI-generated engineering work before it influences project decisions.
- Update QA/QC procedures to explicitly address AI-assisted workflows.
- Define engineering activities requiring mandatory professional review regardless of AI involvement.
- Reinforce that engineers remain accountable for all technical decisions.

Project Delivery Leaders

- Integrate approved AI tools and workflows into day-to-day project execution.
- Ensure AI-assisted work receives appropriate technical review before incorporation into project deliverables.
- Reinforce adherence to established QA/QC procedures while using AI to improve project efficiency.
- Share lessons learned, emerging risks, and successful AI practices across project teams to support continuous organizational improvement.

Technology Leaders

- Prioritize enterprise AI platforms capable of protecting confidential information.
- Improve engineering data quality, organization, and accessibility.
- Validate AI tools before broad organizational deployment.
- Monitor AI performance as models evolve.

Human Resources & Learning

- Train employees to recognize hallucinations, uncertainty, and AI limitations.
- Develop guidance on appropriate use cases.
- Encourage responsible experimentation while reinforcing professional expectations.

Risk Management & Legal

- Document AI-assisted workflows where appropriate.
- Periodically review AI governance policies.
- Evaluate vendor capabilities, security practices, and contractual responsibilities.

Collectively, these actions shift technical reliability from a technology problem to an organizational capability supported by governance, engineering practice, workforce development, and leadership.

What Questions Should Every Engineering Firm Ask?

- Do our engineers independently validate AI-generated technical information before relying upon it?
- Have we clearly defined where AI may—and may not—be used within engineering workflows?
- Are our QA/QC procedures keeping pace with AI-assisted engineering?
- Are we relying on trusted organizational data or publicly available information of uncertain quality?
- Can our engineers explain how AI-assisted conclusions were reached?
- Does every employee understand that AI supports—but never replaces—professional engineering judgment?

What Comes Next?

Artificial intelligence will continue to improve. Engineering-specific AI models will become more accurate, more explainable, and more deeply integrated into engineering workflows. Over time, many of today's technical limitations—including hallucinations, poor contextual understanding, and inconsistent outputs—are likely to diminish as AI systems gain access to better engineering data, richer organizational knowledge, and more sophisticated validation capabilities.

Ironically, those improvements will make technical reliability even more important—not less. As AI-generated work becomes increasingly accurate and persuasive, the challenge for engineers will shift from recognizing obvious errors to identifying subtle inaccuracies, incomplete assumptions, and conclusions that appear reasonable but require deeper professional scrutiny. Confidence in AI should never replace confidence in engineering judgment.

The interviews consistently suggest that the firms best positioned for this future will not be those with access to the most advanced AI tools. They will be the organizations that build disciplined validation processes, maintain trusted organizational knowledge, strengthen quality assurance, and reinforce a culture in which engineers critically evaluate AI-assisted work rather than simply accepting it.

Ultimately, technical reliability will remain less a function of artificial intelligence than of organizational discipline. AI may become increasingly capable, but the engineering firms that earn the greatest confidence—from clients, regulators, and the public—will be those that combine advanced technology with rigorous engineering judgment and consistently reliable engineering practices.

> "Trust but verify."
>
> **TECHNOLOGY VENDOR**

5 PROFESSIONAL LIABILITY AND STANDARD OF CARE RISK

PROFESSIONAL RESPONSIBILITY CANNOT BE DELEGATED.

Artificial intelligence may support engineering work, but responsibility for engineering decisions—and the duty to protect the public—always remains with licensed professionals.

What Is the Risk?

Professional liability has always been an inherent part of engineering practice. Engineering firms are responsible for delivering work that meets the applicable standard of care, complies with contractual obligations, and protects the health, safety, and welfare of the public. Those responsibilities do not change simply because artificial intelligence becomes part of the engineering process.

AI does, however, introduce new questions regarding how engineering work is produced, reviewed, documented, and defended. As AI becomes increasingly capable of generating calculations, drafting reports, developing design alternatives, summarizing technical information, and assisting with engineering analyses, firms must determine where professional responsibility begins and ends. Questions naturally arise regarding accountability for AI-assisted work, the standard of care expected when AI is used, documentation of engineering decisions, and the responsibilities of engineers who sign and seal work products incorporating AI-generated information.

The legal profession is still developing answers to many of these questions. Nevertheless, the interviews conducted for this study consistently suggest that one principle is already well established. Artificial intelligence may change how engineering work is performed, but it does not change who is responsible for the outcome.

What Did We Learn?

While stakeholders approached professional liability from different perspectives, there was remarkable consistency regarding the profession's continuing responsibility.

> "The engineer has to remain in responsible charge of the work."
>
> **LICENSING AUTHORITY**

PROFESSIONAL RESPONSIBILITY REMAINS UNCHANGED.

Perhaps no theme emerged more consistently across the interviews than this one. Engineering firm leaders, public clients, legal experts, insurance professionals, licensing authorities, technology providers, and AI consultants consistently expressed the view that that responsibility for engineering decisions remains with the engineering firm and the licensed professionals overseeing the work.

Several participants noted that AI should be viewed no differently than any other engineering tool. Engineers have long relied on sophisticated software to support structural analysis, hydraulic modeling, traffic forecasting, and numerous other technical disciplines. The responsibility for reviewing and validating those results has always remained with the engineer. AI does not change that expectation.

AI DOES NOT CREATE LIABILITY—POOR PROFESSIONAL PRACTICE DOES.

Several participants challenged a common misconception that AI itself creates legal exposure. Instead, legal and insurance professionals consistently explained that liability arises when organizations fail to exercise reasonable professional care. Hallucinations, inaccurate outputs, or incomplete analyses become legal problems only if they influence engineering decisions without appropriate review.

From this perspective, AI functions much like any other engineering resource. Errors become significant when engineers rely upon them without exercising appropriate professional judgment.

RESPONSIBLE CHARGE BECOMES INCREASINGLY IMPORTANT.

The licensing perspective added an important dimension to the discussion. Participants emphasized that responsible charge extends beyond reviewing final deliverables. Licensed engineers must understand the work being performed, maintain meaningful involvement throughout engineering activities, and possess sufficient knowledge to independently evaluate AI-assisted analyses before certifying engineering documents. This expectation becomes increasingly important as AI systems assume more sophisticated engineering tasks.

Responsible charge cannot become passive oversight. It requires active professional engagement.

DOCUMENTATION AND DEFENSIBILITY MATTER.

Several participants observed that AI may increase expectations regarding documentation. Engineering firms should be prepared to explain how AI contributed to engineering work, how outputs were reviewed, what assumptions were accepted or rejected, and how final engineering decisions were reached. Participants generally did not advocate documenting every AI interaction. Rather, they emphasized documenting engineering judgment. The ability to explain why a particular engineering decision was made remains more important than documenting every technological tool used during the design process.

A couple participants also noted that litigation involving AI-assisted engineering work is beginning to evolve. Questions may increasingly extend beyond whether AI was used to how engineering decisions were reviewed, validated, and documented. Looking ahead, firms should also recognize that as AI becomes more widely adopted, future questions may include why particular AI-assisted review processes were—or were not—used in support of engineering judgment.

CLIENTS CARE ABOUT ACCOUNTABILITY—NOT TECHNOLOGY.

Public infrastructure owners consistently reinforced an important point. Most clients expressed relatively little interest in whether engineering firms use AI. Instead, they expect firms to maintain consistent quality, transparency, accountability, and professional responsibility regardless of the technologies supporting project delivery.

A couple participants also observed that some infrastructure owners are beginning to incorporate AI-specific provisions into engineering contracts. Rather than prohibiting AI outright, these provisions often address acceptable AI use, confidentiality, disclosure requirements, approval processes, or restrictions associated with sensitive projects. As client expectations evolve, engineering firms should anticipate increasing contractual variation and ensure that AI governance policies remain aligned with project-specific contractual obligations.

> “It’s our duty and responsibility to protect the health, safety, and welfare of the public.
>
> **ENGINEERING FIRM – SMALL FIRM**

What Can Engineering Firms Do?

The interviews identified several practical actions engineering firms can take to reduce professional liability while supporting responsible AI adoption.

Executive Leadership

- Clearly communicate that AI does not change the firm's professional responsibilities.
- Integrate AI governance into existing enterprise risk management and quality programs.
- Periodically review AI policies as technology, regulations, and industry practices evolve.

Engineering Leaders

- Maintain existing standards of professional review regardless of AI involvement.
- Define engineering activities requiring licensed oversight.
- Reinforce responsible charge throughout AI-assisted workflows.
- Ensure engineers understand both the capabilities and limitations of AI tools.

Project Delivery Leaders

- Ensure AI-assisted work is assigned, reviewed, and incorporated into project deliverables in accordance with the firm's quality management procedures.
- Confirm that licensed engineers maintain appropriate involvement in engineering decisions and responsible charge throughout project delivery.
- Promote transparent documentation of engineering decisions and significant AI-assisted workflows where appropriate.
- Balance project efficiency with professional obligations, ensuring schedule pressures do not compromise engineering judgment or quality.

Technology Leaders

- Select AI platforms that support transparency and traceability.
- Maintain secure records of organizational knowledge supporting AI outputs.
- Integrate AI tools into existing engineering workflows rather than creating parallel processes.

Human Resources & Learning

- Incorporate AI responsibilities into engineering training programs.
- Reinforce that AI supplements—but never replaces—professional engineering judgment.
- Develop continuing education addressing AI governance, responsible charge, and evolving professional expectations.

Risk Management & Legal

- Review professional liability implications associated with AI-assisted services.
- Evaluate contracts for provisions addressing AI, confidentiality, ownership of work product, and professional responsibility.
- Periodically assess insurance coverage as AI adoption expands.
- Monitor emerging legal and regulatory developments affecting AI-assisted engineering practice.

Collectively, these actions strengthen the connection between AI adoption and established professional practice rather than treating AI as an entirely separate area of organizational risk.

What Questions Should Every Engineering Firm Ask?

- Have we clearly defined where licensed engineers must review AI-assisted work?
- Do our engineers understand that responsibility for engineering decisions cannot be delegated to AI?
- Are our QA/QC procedures explicitly addressing AI-assisted engineering activities?
- Can we explain and defend engineering decisions that incorporate AI-generated information?
- Are our contracts, insurance policies, and organizational procedures keeping pace with AI adoption?
- Are we preserving meaningful responsible charge throughout AI-assisted project delivery?

What Comes Next?

Artificial intelligence will continue reshaping engineering practice. Future AI systems will become increasingly capable of generating analyses, reviewing designs, producing technical documentation, and supporting complex engineering workflows. As these capabilities expand, engineering firms will face growing pressure to determine where AI appropriately supports professional practice and where independent engineering judgment must continue to prevail.

The interviews consistently suggest that advances in AI will not reduce professional responsibility. Instead, they are likely to raise expectations for how engineering firms demonstrate responsible charge, document engineering decisions, validate AI-assisted work, and maintain professional accountability. Clients, regulators, licensing boards, insurers, and the public will increasingly expect firms to show not only that AI was used effectively, but that licensed professionals exercised appropriate oversight throughout the engineering process.

The firms best prepared for this future will treat engineering judgment as a strategic asset rather than simply an individual competency. They will strengthen mentoring, reinforce quality management systems, clearly define the appropriate role of AI within engineering practice, and ensure that professional responsibility remains embedded throughout every stage of project delivery.

Ultimately, artificial intelligence may transform how engineering is practiced, but it will not transform what it means to be a professional engineer. As AI capabilities continue to advance, engineering judgment, responsible charge, and accountability will become even more important sources of public trust and professional distinction.

6 DATA GOVERNANCE, PRIVACY AND INTELLECTUAL PROPERTY RISK

AI AMPLIFIES ORGANIZATIONAL KNOWLEDGE.

As AI becomes more capable, an engineering firm's competitive advantage will depend less on the AI tools it uses and more on the quality, integrity, and governance of the knowledge those tools access.

What Is the Risk?

Artificial intelligence depends on data. Whether AI is generating technical reports, retrieving organizational knowledge, assisting with engineering analyses, or supporting project decisions, the quality of its outputs is fundamentally tied to the quality of the information upon which it relies. For engineering firms, this creates a new category of organizational risk.

Historically, many firms have viewed data management as an operational or information technology function. AI changes that perspective. As organizations increasingly rely on AI to search project files, summarize technical standards, identify lessons learned, generate proposals, analyze engineering documents, and support decision-making, organizational data becomes a strategic asset rather than simply a repository of information.

Poorly organized, outdated, inaccurate, or incomplete information can reduce AI effectiveness, increase the likelihood of inaccurate outputs, expose confidential information, and create uncertainty regarding intellectual property ownership and data privacy.

Conversely, firms possessing well-managed engineering knowledge will be better positioned to leverage AI effectively while protecting client information, proprietary expertise, and organizational trust.

The challenge is no longer simply managing data. It is governing organizational knowledge.

> It's not about the model. It's about how organizations govern the information feeding the model.
>
> **TECHNOLOGY VENDOR**

What Did We Learn?

The interviews consistently revealed that data governance is one of the least understood—but potentially most important—dimensions of successful AI adoption. While the literature often discusses data privacy, cybersecurity, and intellectual property independently, participants viewed these issues as interconnected components of a broader organizational capability.

AI AMPLIFIES THE QUALITY OF ORGANIZATIONAL KNOWLEDGE.

One of the strongest themes emerging from the interviews was that AI performs only as well as the information available to it. Technology providers repeatedly emphasized that organizations often focus on selecting AI platforms before evaluating the quality, organization, accessibility, and governance of their engineering data. Several participants observed that unreliable outputs often result from incomplete or poorly organized organizational knowledge rather than limitations in the AI model itself.

DATA GOVERNANCE IS BECOMING A COMPETITIVE ADVANTAGE.

Several technology vendors argued that engineering firms possessing well-organized project information, engineering standards, lessons learned, specifications, and institutional knowledge will realize significantly greater value from AI than firms relying upon fragmented or poorly managed information. Participants described enterprise knowledge as an increasingly valuable business asset rather than simply archived project documentation. Organizations that successfully organize decades of engineering experience into trusted enterprise knowledge bases may gain significant advantages in productivity, consistency, knowledge transfer, and client service.

Several participants also observed that one of the greatest challenges facing engineering firms is not simply organizing existing project documentation, but capturing the institutional knowledge held by experienced engineers before it is lost through retirements, workforce turnover, or organizational change. While AI can significantly improve access to documented knowledge, it cannot retrieve expertise that has never been captured. As firms strengthen their knowledge management capabilities, they should recognize that preserving engineering judgment, lessons learned, and institutional experience represents an important long-term organizational priority.

PROTECTING ORGANIZATIONAL KNOWLEDGE BECOMES EVEN MORE IMPORTANT AS AI ADOPTION EXPANDS.

Engineering firms, public clients, legal professionals, and technology providers all emphasized protecting confidential information. Participants expressed concerns regarding:

- client-owned information,
- proprietary engineering methods,
- sensitive infrastructure data,
- personally identifiable information,
- and confidential business information.

Rather than discouraging AI adoption, participants generally recommended using enterprise AI platforms designed to protect organizational information rather than relying on unrestricted public AI systems. Public clients also emphasized maintaining confidence that sensitive project information will remain appropriately protected regardless of the technologies used during project delivery.

INTELLECTUAL PROPERTY REMAINS AN EVOLVING ISSUE.

Participants generally agreed that intellectual property law has not yet fully caught up with AI. Questions remain regarding ownership of AI-generated content, use of copyrighted materials during model training, reuse of engineering documents, and ownership of AI-assisted work products. Legal professionals encouraged firms to monitor emerging legal developments while establishing internal policies governing acceptable AI use.

At the same time, several participants emphasized that an organization's greatest intellectual property asset is often its accumulated engineering knowledge rather than any individual AI tool. Protecting that knowledge therefore becomes increasingly important as AI capabilities mature.

DATA GOVERNANCE EXTENDS BEYOND TECHNOLOGY.

Successful data governance therefore depends on coordinated leadership across the enterprise. Technology teams manage systems, engineers create knowledge, project teams maintain information, and leadership establishes governance. AI succeeds only when these responsibilities operate as an integrated organizational capability.

What Can Engineering Firms Do?

The interviews identified several practical actions engineering firms can take to strengthen data governance while supporting responsible AI adoption.

Executive Leadership

- Invest in long-term knowledge management rather than isolated AI tools.
- Recognize organizational knowledge as a strategic business asset.
- Develop enterprise data governance policies aligned with AI strategy.
- Assign organizational accountability for data governance.

Engineering Leaders

- Standardize documentation practices across projects.
- Preserve engineering assumptions, lessons learned, and technical decisions in searchable formats.
- Encourage consistent documentation that supports future knowledge reuse.
- Reinforce that engineering knowledge should remain accessible beyond individual project teams.

Project Delivery Leaders

- Promote consistent project documentation practices that improve the quality and usability of organizational knowledge.
- Ensure project information is stored in approved systems using established data management standards.
- Encourage project teams to capture lessons learned, engineering decisions, and reusable knowledge in searchable formats.
- Reinforce appropriate handling of client information and confidential data when using AI during project delivery.

Technology Leaders

- Implement secure enterprise AI environments whenever possible.
- Improve data quality, organization, metadata, and accessibility.
- Establish permissions governing access to confidential information.
- Continuously monitor data quality supporting AI applications.
- Integrate AI platforms with trusted enterprise knowledge rather than disconnected information sources.

Human Resources & Learning

- Educate employees regarding appropriate handling of confidential information.
- Provide guidance regarding approved AI platforms.
- Train staff on organizational knowledge management practices.
- Reinforce employee responsibilities regarding privacy and intellectual property.

Risk Management & Legal

- Review contractual obligations governing confidential information.
- Develop policies regarding AI use and data protection.
- Monitor evolving intellectual property regulations.
- Periodically assess vendor security practices and data governance capabilities.
- Establish procedures for evaluating new AI technologies before organizational deployment.

Collectively, these actions position data governance as an enterprise capability supporting both AI effectiveness and organizational resilience.

What Questions Should Every Engineering Firm Ask?

- Do we know where our most valuable engineering knowledge resides?
- Can our AI systems access trusted organizational information while protecting confidential data?
- Are our project files organized well enough to support effective AI use?
- Have we established clear policies governing employee use of public and enterprise AI platforms?
- Are we protecting client information, proprietary methods, and intellectual property appropriately?
- Are we treating organizational knowledge as a long-term strategic asset?

What Comes Next?

Artificial intelligence is rapidly changing the role of organizational knowledge within engineering firms. As AI systems become more capable, they will rely less on publicly available information and increasingly draw upon an organization's proprietary engineering knowledge, historical project experience, technical standards, design practices, lessons learned, and institutional expertise. The firms that have invested in organizing and governing these assets will be positioned to realize far greater value from AI than those relying primarily on generic models.

This shift will fundamentally change how engineering firms think about data governance. Information management will no longer be viewed primarily as an operational or information technology function. Instead, it will become a strategic capability that directly influences engineering quality, organizational learning, workforce development, client service, innovation, and long-term competitiveness. Decisions about how knowledge is captured, maintained, protected, and shared will increasingly become business decisions rather than simply technology decisions.

The interviews consistently suggest that engineering firms will compete less on access to AI technology and more on the quality of the knowledge that AI is able to use responsibly. While advanced AI models are becoming widely available, decades of engineering experience, trusted technical information, and institutional knowledge remain unique assets that cannot be easily replicated. Firms that deliberately invest in these assets today will create advantages that extend well beyond AI adoption itself.

Ultimately, the most valuable asset in an AI-enabled engineering firm may not be the AI platform it deploys, but the engineering knowledge it has accumulated over years of professional practice. Artificial intelligence will increasingly amplify the value of that knowledge, making its stewardship one of the profession's most important strategic responsibilities and one of the firm's most enduring competitive advantages.

> "Data is the fuel of AI."
>
> **PUBLIC INFRASTRUCTURE OWNER**

7 ORGANIZATIONAL AND WORKFORCE RISK

ENGINEERING JUDGMENT IS LEARNED, NOT DOWNLOADED.

Firms that fail to redesign mentoring and professional development risk weakening the very expertise that AI is intended to enhance.

What Is the Risk?

Artificial intelligence is transforming how engineering work is performed. Tasks that once required significant manual effort—including research, document preparation, code review, design iteration, proposal development, project administration, and portions of technical analysis—can increasingly be completed with AI assistance. These capabilities offer tremendous opportunities to improve efficiency and allow engineers to focus on higher-value work.

At the same time, they introduce important organizational and workforce questions. How will engineering firms prepare employees to work effectively with AI? How will younger engineers develop the technical judgment historically gained through experience? How will organizations preserve mentoring, collaboration, and professional growth as AI assumes more routine tasks? How will firms manage organizational change while maintaining employee engagement and client confidence?

The workforce risks associated with AI therefore extend well beyond concerns about job displacement. They involve the future development of engineering expertise itself. Engineering firms have always depended upon a continuous transfer of knowledge—from experienced professionals to younger engineers, from project teams to future projects, and from one generation of leaders to the next. AI has the potential to strengthen that process, but only if firms intentionally adapt how they develop people, transfer knowledge, and build professional capability.

What Did We Learn?

The interviews consistently revealed that workforce risk is less about replacing engineers than about redefining how engineering organizations develop talent. Participants viewed AI as an opportunity to augment people rather than reduce the importance of people. However, they also expressed concern that firms could unintentionally weaken the very experiences through which engineers develop professional judgment.

> Professional judgment and thinking can’t get shoved by the wayside.
>
> **ENGINEERING FIRM – SMALL FIRM**

ENGINEERING JUDGMENT IS LEARNED—NOT DOWNLOADED.

One of the strongest themes emerging from the interviews involved the development of engineering judgment. Several engineering leaders observed that early-career engineers traditionally build judgment by performing repetitive calculations, preparing technical documentation, checking drawings, researching standards, and participating in increasingly complex project work under the supervision of experienced professionals.

AI now has the potential to automate portions of these activities. Participants questioned how future engineers will gain the practical understanding historically acquired through performing this work themselves. Licensing officials similarly emphasized that competence develops through meaningful professional experience rather than simply producing engineering deliverables more efficiently. Collectively, these perspectives suggest that engineering firms must intentionally redesign professional development rather than assuming traditional learning pathways will remain unchanged.

Participants consistently emphasized that the challenge extends beyond training alone. Responsible AI use depends upon developing the professional competencies required to critically evaluate AI-assisted work, recognize when additional engineering analysis is necessary, and exercise independent engineering judgment. While training plays an important role, participants viewed these capabilities as professional competencies that must be deliberately developed and reinforced throughout an engineer's career rather than acquired through AI use alone.

AI CHANGES WORK—NOT THE VALUE OF PEOPLE.

Nearly every stakeholder rejected the idea that AI would eliminate the need for engineers. Instead, participants consistently described AI as changing the nature of engineering work. Routine and repetitive activities will increasingly become automated. The value engineers provide will increasingly center on problem definition, systems thinking, interdisciplinary collaboration, client communication, engineering judgment, innovation, and leadership.

CHANGE MANAGEMENT IS BECOMING A LEADERSHIP RESPONSIBILITY.

Engineering leaders repeatedly emphasized that AI adoption requires thoughtful organizational change rather than simply introducing new technology. Employees need clear expectations regarding appropriate AI use, training opportunities, leadership support, and confidence that AI is intended to enhance—not diminish—their professional contributions. Several participants noted that uncertainty often creates greater organizational resistance than the technology itself. Transparent communication and visible leadership therefore become essential components of successful AI adoption.

LEARNING MUST BECOME CONTINUOUS.

Technology providers and AI consultants consistently observed that AI capabilities are evolving too rapidly for firms to rely upon occasional training sessions. Instead, organizations should foster cultures of continuous learning in which employees regularly explore new capabilities, share experiences, evaluate emerging tools, and refine AI-assisted workflows. Several participants described AI literacy as becoming a core professional competency alongside traditional engineering expertise.

Participants also recognized that workforce development challenges differ across career stages. Early-career engineers must continue developing the engineering judgment needed to critically evaluate AI-generated outputs rather than accepting them at face value. More experienced engineers, by contrast, often face a different challenge: learning how to integrate AI effectively into established engineering practice while maintaining professional responsibility and recognizing opportunities to improve quality, efficiency, and client value. These differing needs suggest that workforce development strategies should be tailored to engineers at different stages of their careers.

ORGANIZATIONAL CULTURE DETERMINES SUCCESS.

Perhaps the most important organizational finding emerging from the interviews is that AI implementation ultimately reflects organizational culture. Firms encouraging curiosity, collaboration, responsible experimentation, and continuous improvement expressed considerably greater confidence regarding AI adoption than organizations approaching AI primarily through fear or restriction. Participants consistently emphasized that culture—not technology—determines whether AI becomes a competitive advantage.

> The greatest long-term risk is not inaccurate AI—it is professionals losing the expertise required to identify inaccuracies.
>
> **PUBLIC INFRASTRUCTURE OWNER**

What Can Engineering Firms Do?

The interviews identified several practical actions engineering firms can take to prepare their organizations and workforce for AI.

Executive Leadership

- Clearly communicate how AI supports the firm's long-term strategy.
- Position AI as an investment in employees rather than a replacement for employees.
- Establish organizational expectations regarding responsible AI use.
- Invest in workforce development alongside technology investments.

Engineering Leaders

- Preserve mentoring opportunities even as AI automates routine work.
- Redesign professional development programs to emphasize engineering judgment, systems thinking, and critical evaluation.
- Encourage engineers to validate AI outputs rather than accept them uncritically.
- Provide supervised opportunities for younger engineers to develop technical competence.

Project Delivery Leaders

- Model responsible AI use in day-to-day project delivery and reinforce adherence to the firm's AI policies and ethical standards.
- Promote transparency with clients regarding AI use when required by firm policy, contractual obligations, or project circumstances.
- Recognize and escalate ethical, regulatory, or client concerns related to AI use through appropriate organizational channels.
- Foster a project culture where team members feel comfortable questioning or reporting inappropriate AI use.

Technology Leaders

- Select AI tools that enhance collaboration rather than isolate users.
- Support enterprise knowledge sharing across project teams.
- Develop AI environments that encourage responsible experimentation.
- Monitor AI adoption to identify training needs and workflow improvements.

Human Resources & Learning

- Develop training and mentoring programs that strengthen engineers' ability to critically evaluate AI-assisted work while reinforcing sound engineering judgment at every career stage.
- Update competency models to reflect AI-enabled engineering practice.
- Incorporate AI into onboarding, continuing education, and leadership development.
- Recognize and reward continuous learning.

Risk Management & Legal

- Update policies addressing acceptable AI use by employees.
- Clarify organizational responsibilities regarding AI-assisted work.
- Ensure workforce guidance aligns with evolving regulatory and contractual expectations.

Collectively, these actions help engineering firms prepare not only for AI adoption but for the broader transformation of engineering work.

What Questions Should Every Engineering Firm Ask?

- How will our younger engineers develop professional judgment as AI automates more routine work?
- Are we investing as much in people as we are in technology?
- Do our employees understand where AI adds value—and where human judgment remains essential?
- Have we redesigned mentoring and professional development for an AI-enabled workplace?
- Does our organizational culture encourage responsible experimentation and continuous learning?
- Are we preparing today's engineers for tomorrow's profession?

What Comes Next?

Artificial intelligence will continue reshaping how engineers learn, collaborate, and perform technical work. Routine analyses, documentation, research, and many repetitive engineering tasks will increasingly be supported by AI, allowing engineers to work more efficiently and focus on higher-value activities. At the same time, these changes will fundamentally alter how professional experience is acquired within engineering firms.

The interviews consistently identified this as one of the profession's most significant long-term challenges. Engineering judgment has traditionally been developed through progressive responsibility, repeated exposure to technical problems, mentorship, project experience, and learning from both successes and mistakes. As AI assumes a greater share of routine work, firms will need to rethink how those experiences are intentionally created for future generations of engineers.

The firms best prepared for this future will view workforce development not as a training initiative, but as a strategic investment in professional capability. They will redesign mentoring programs, create opportunities for engineers to exercise independent judgment, encourage thoughtful use of AI rather than passive reliance upon it, and ensure that technology strengthens—rather than replaces—the development of engineering expertise.

Ultimately, artificial intelligence will change how engineers gain experience, but it cannot replace the experience itself. The engineering firms that distinguish themselves in the years ahead will be those that deliberately cultivate engineering judgment while embracing AI as a tool to enhance, rather than substitute for, professional growth. In an AI-enabled profession, developing future engineers may become one of the most important investments a firm can make.

8 ETHICAL, REGULATORY AND REPUTATIONAL RISK

THE GREATEST ETHICAL RISK IS NOT SIMPLY VIOLATING A REGULATION, IT IS LOSING THE TRUST UPON WHICH PROFESSIONAL ENGINEERING DEPENDS.

Trust is earned through transparency, accountability, and responsible governance.

What Is the Risk?

Engineering has long been recognized as a profession grounded in public trust. Every licensed engineer accepts a responsibility that extends beyond clients, projects, and commercial interests to include protecting the health, safety, and welfare of the public. Artificial intelligence does not alter that responsibility—but it does introduce new ethical, regulatory, and reputational questions that engineering firms must address.

As AI becomes integrated into engineering practice, organizations must consider issues such as transparency, accountability, bias, fairness, explainability, disclosure, regulatory compliance, and the responsible use of AI-generated information. They must also consider how AI may influence client confidence, public perception, and the reputation of both individual firms and the engineering profession.

These risks extend beyond legal compliance.

Engineering firms may satisfy every contractual requirement and still make decisions that weaken client trust or raise ethical concerns. Conversely, organizations that demonstrate transparency, responsible governance, and professional integrity may strengthen their reputations while building confidence in the responsible use of AI.

The central risk is therefore not simply violating a regulation. It is losing the trust upon which professional engineering depends.

> Engineering organizations occupy positions of trust with their clients.
>
> **ENGINEERING FIRM – LARGE FIRM**

What Did We Learn?

The interviews consistently revealed that ethics, regulation, and reputation are deeply interconnected.

Participants rarely discussed these issues separately. Instead, they viewed them collectively as part of the broader responsibility engineering firms have to earn and maintain the confidence of clients, regulators, employees, and the public.

PUBLIC TRUST REMAINS THE PROFESSION'S MOST VALUABLE ASSET.

Perhaps the strongest finding emerging from the interviews is that AI should never compromise the public's confidence in engineering decisions. Public-sector owners repeatedly emphasized that they expect engineering firms to continue delivering work that is accurate, transparent, and professionally defensible regardless of the technologies used during project delivery. Engineering leaders similarly recognized that reputation has become increasingly important as AI adoption accelerates. One poorly governed use of AI could undermine years of client trust. Several participants observed that engineering firms have spent decades establishing reputations based upon competence, integrity, and technical excellence. AI should reinforce those qualities—not place them at risk.

TRANSPARENCY BUILDS CONFIDENCE.

Participants generally agreed that engineering firms should be prepared to explain how AI contributes to engineering work when appropriate. Importantly, transparency was not viewed as disclosing every interaction with AI. Rather, it was described as being able to explain engineering decisions, validation processes, quality controls, and the role AI played in supporting—not replacing—professional judgment.

ETHICAL AI BEGINS WITH ORGANIZATIONAL CULTURE.

Technology providers, AI consultants, and engineering leaders consistently emphasized that ethical AI is less about algorithms than organizational values. Organizations demonstrating strong cultures of integrity, accountability, quality, and professional responsibility were generally viewed as better prepared to adopt AI responsibly. Several participants observed that ethical failures often result from weak governance, poor incentives, or insufficient oversight rather than flaws within AI itself. This reinforces a recurring theme throughout the report: governance shapes outcomes.

REGULATION WILL CONTINUE EVOLVING.

Participants widely acknowledged that regulatory guidance regarding AI remains in its early stages. Engineering firms therefore cannot rely solely on regulatory compliance when making AI decisions. Instead, organizations should monitor evolving standards while continuing to apply existing engineering ethics, professional licensure requirements, and standards of care. Several legal and regulatory participants emphasized that engineering's existing ethical framework already provides a strong foundation for responsible AI adoption. The challenge is applying those principles to new technologies.

REPUTATION IS INCREASINGLY FRAGILE.

Participants also discussed the speed with which reputational damage can occur. An inappropriate use of AI, failure to protect confidential information, biased decision-making, or poorly governed AI implementation could rapidly affect client confidence and organizational credibility. Conversely, firms that demonstrate thoughtful governance, transparency, and responsible AI leadership may strengthen their reputations as trusted advisors during a period of significant technological change.

> "The greatest risk lies in users accepting AI-generated information without exercising professional judgment.
>
> **PUBLIC INFRASTRUCTURE OWNER**

What Can Engineering Firms Do?

The interviews identified several practical actions engineering firms can take to strengthen ethical governance while protecting client confidence and organizational reputation.

Executive Leadership

- Establish organizational principles for the responsible use of AI.
- Communicate that AI adoption must align with the firm's values and professional responsibilities.
- Periodically review AI governance as regulations and client expectations evolve.
- Reinforce that protecting public trust is a strategic priority.

Engineering Leaders

- Ensure engineering decisions remain transparent and professionally defensible.
- Encourage open discussion regarding ethical questions arising from AI use.
- Continue emphasizing engineering judgment, quality assurance, and accountability.
- Review AI-assisted work with the same professional rigor applied to traditional engineering processes.

Project Delivery Leaders

- Implement approved AI workflows consistently across project teams while maintaining established operational procedures.
- Ensure project teams can continue delivering quality work when AI tools are unavailable, limited, or inappropriate for a particular task.
- Identify operational challenges, workflow improvements, and emerging AI risks encountered during project delivery and communicate them to organizational leadership.
- Promote consistent adoption of AI practices that improve project delivery while preserving resilience, quality, and client service.

Technology Leaders

- Select AI platforms supporting transparency, security, and explainability.
- Monitor AI systems for bias, inappropriate outputs, and unintended consequences.
- Implement governance controls protecting confidential information and client data.

Human Resources & Learning

- Incorporate AI ethics into employee education and professional development.
- Reinforce organizational expectations regarding responsible AI use.
- Encourage employees to raise ethical concerns without fear of retaliation.

Risk Management & Legal

- Monitor evolving regulatory guidance affecting AI.
- Periodically review AI policies for alignment with contractual and professional obligations.
- Evaluate emerging legal risks associated with AI-assisted services.
- Coordinate AI governance with existing enterprise risk management processes.

Together, these actions help ensure that ethical responsibility becomes part of everyday organizational practice rather than a reaction to regulatory change.

What Questions Should Every Engineering Firm Ask?

- Would our clients be confident in how we are using AI if we explained our process?
- Are our AI practices aligned with our professional and ethical responsibilities?
- Can we explain and defend engineering decisions supported by AI?
- Have we established clear expectations regarding responsible AI use throughout the organization?
- Are we monitoring emerging regulatory developments while maintaining our existing ethical standards?
- Are we strengthening—or risking—the reputation our firm has spent years building?

What Comes Next?

Artificial intelligence will continue raising new ethical, legal, and regulatory questions for the engineering profession. Expectations surrounding transparency, accountability, explainability, bias, documentation, and responsible AI governance will continue to evolve as AI becomes more deeply integrated into engineering practice. New regulations will undoubtedly emerge, but the interviews consistently suggest that engineering firms cannot afford to wait for regulations before establishing responsible AI practices.

As AI adoption expands, clients, regulators, insurers, and the public are likely to place greater emphasis on demonstrating responsible governance rather than simply complying with minimum requirements. Engineering firms will increasingly be expected to explain how AI was used, how engineering decisions were validated, how professional judgment was exercised, and how risks were managed throughout the project lifecycle. Transparency itself may become an important measure of professional competence.

The interviews also suggest that trust will become an increasingly important competitive differentiator. Organizations that consistently demonstrate ethical leadership, responsible AI governance, transparency, and professional accountability are likely to strengthen relationships with clients and reinforce public confidence. In contrast, firms that treat ethics solely as a compliance obligation may find themselves responding to reputational challenges rather than preventing them.

Ultimately, the greatest ethical challenge associated with artificial intelligence is not simply avoiding misconduct or complying with future regulations. It is preserving the trust upon which the engineering profession has always depended. As AI continues to evolve, that trust will remain one of the profession's most valuable assets—and one of the clearest measures of responsible engineering leadership.

9 OPERATIONAL AND CYBERSECURITY RISK

OPERATIONAL RESILIENCE DEPENDS UPON GOVERNANCE, NOT TECHNOLOGICAL PERFECTION.

AI becomes a business asset only when it is securely integrated into existing operational, quality, and risk management systems.

What Is the Risk?

As artificial intelligence becomes embedded throughout engineering firms, it increasingly influences the organization's day-to-day operations. AI is no longer limited to isolated experiments or individual productivity tools. It is beginning to support proposal development, project management, engineering analysis, document production, knowledge retrieval, scheduling, client communication, quality management, and numerous other business processes. This integration creates significant opportunities to improve organizational efficiency and consistency.

It also introduces new operational risks. Engineering firms must now consider how AI systems are secured, monitored, governed, integrated, and maintained. They must understand the risks associated with third-party AI vendors, unauthorized employee use of public AI tools, cyber threats, operational disruptions, inaccurate AI outputs flowing through automated workflows, and increasing dependence on technologies that continue evolving rapidly.

Unlike traditional software implementations, AI systems often learn, change, and interact with other technologies in ways that require continuous oversight rather than one-time deployment. The challenge is therefore broader than cybersecurity alone. It is ensuring that AI becomes a resilient, trusted, and well-governed component of everyday business operations.

What Did We Learn?

Participants consistently viewed operational resilience as an emerging organizational priority. Although cybersecurity remained an important concern, interviewees spent considerably more time discussing governance, operational discipline, vendor management, and organizational preparedness than specific cyber threats.

> "Governance extends beyond standalone AI tools to encompass the firm's entire technology ecosystem."

ENGINEERING FIRM – LARGE FIRM

AI SHOULD BECOME PART OF NORMAL OPERATIONS—NOT OPERATE OUTSIDE THEM.

One of the clearest themes emerging from the interviews was that AI should not function as an isolated technology initiative. Several engineering leaders and technology providers emphasized integrating AI into existing operational processes, governance structures, quality systems, and business workflows rather than allowing employees to develop independent approaches. Participants repeatedly warned against fragmented AI adoption occurring through individual experimentation without organizational oversight. Several described this phenomenon as creating operational inconsistency rather than innovation.

SHADOW AI CREATES OPERATIONAL RISK.

A recurring concern involved employees independently using publicly available AI tools without organizational knowledge or governance. While most participants encouraged experimentation, they distinguished between responsible experimentation and unmanaged adoption. Unauthorized AI use may expose confidential information, create inconsistent work products, increase cybersecurity vulnerabilities, and complicate quality assurance. Several participants observed that organizations often underestimate the extent to which employees are already using AI in their daily work. This creates operational blind spots that leadership may not recognize until problems emerge.

Participants also observed that AI is making it increasingly easy for individual employees to create custom tools, workflows, and AI agents to support project delivery. While these solutions may improve productivity, they also introduce new operational risks related to ownership, maintenance, documentation, testing, version control, and long-term support. Unlike traditional software organizations, many engineering firms have limited experience managing internally developed AI-enabled tools throughout their lifecycle. As AI adoption expands, organizations should establish governance processes that distinguish experimental innovation from operational systems relied upon in project delivery.

VENDOR RELATIONSHIPS REQUIRE GREATER SCRUTINY.

Technology providers, consultants, and legal professionals all emphasized that engineering firms increasingly depend upon external AI vendors. Consequently, organizations should understand:

- how vendors use organizational data,
- where information is stored,
- how models are updated,
- what security controls exist, and
- how business continuity will be maintained if vendors change products, pricing, or service offerings.

Operational resilience increasingly depends upon the resilience of the broader AI ecosystem.

CYBERSECURITY REMAINS ESSENTIAL—BUT IT IS EVOLVING.

Participants consistently viewed cybersecurity as a foundational requirement for AI adoption. However, several technology providers noted that AI changes the nature of cybersecurity itself. AI may strengthen cybersecurity by improving threat detection, monitoring networks, and identifying unusual activity.

At the same time, AI can also increase attack sophistication, automate phishing campaigns, expose confidential information through improper prompts, and create new vulnerabilities that organizations must continuously monitor. The relationship between AI and cybersecurity therefore continues evolving.

OPERATIONAL RESILIENCE DEPENDS UPON GOVERNANCE.

Perhaps the strongest operational finding emerging from the interviews is that resilient organizations rely upon disciplined governance rather than technological perfection. Participants consistently described operational resilience as the product of:

- clearly defined policies,
- enterprise oversight,
- approved technologies,
- workforce education,
- incident response planning,
- vendor management,
- and continuous monitoring.

These capabilities reduce operational risk regardless of how AI technologies continue evolving.

What Can Engineering Firms Do?

The interviews identified several practical actions engineering firms can take to strengthen operational resilience while supporting responsible AI adoption.

Executive Leadership

- Integrate AI governance into existing operational risk management processes.
- Establish organizational accountability for AI operations.
- Require periodic reviews of AI implementation across the enterprise.
- Encourage responsible innovation while maintaining operational discipline.

Engineering Leaders

- Integrate AI into existing engineering workflows rather than creating parallel processes.
- Monitor AI-assisted work for operational consistency.
- Reinforce established QA/QC procedures as AI adoption expands.
- Share operational lessons learned across project teams.

Project Delivery Leaders

- Ensure project teams consistently follow approved AI workflows, cybersecurity practices, and operational procedures during project delivery.
- Monitor project-level use of AI for compliance with firm policies and promptly report operational or cybersecurity concerns through established channels.
- Maintain project continuity by ensuring teams can effectively complete critical work when AI tools are unavailable or inappropriate for specific tasks.
- Share operational lessons learned and emerging AI-related risks to strengthen organizational resilience and improve future project delivery.

Technology Leaders

- Approve enterprise AI platforms before widespread organizational use.
- Monitor employee use of AI applications.
- Strengthen cybersecurity protections supporting AI-enabled workflows.
- Evaluate AI vendors for security, reliability, and long-term viability.
- Develop contingency plans for AI system disruptions.

Human Resources & Learning

- Educate employees regarding approved AI tools and acceptable use.
- Reinforce cybersecurity awareness related to AI.
- Encourage reporting of operational concerns involving AI technologies.
- Promote continuous learning as AI capabilities evolve.

Risk Management & Legal

- Review vendor contracts supporting AI services.
- Develop incident response procedures addressing AI-related events.
- Coordinate cybersecurity, operational risk, and AI governance activities.
- Periodically assess operational readiness as AI adoption expands.

Together, these actions help ensure AI strengthens organizational operations without introducing unnecessary operational complexity or unmanaged risk.

What Questions Should Every Engineering Firm Ask?

- Do we know how AI is currently being used throughout our organization?
- Are employees using approved AI platforms or public tools outside organizational oversight?
- Have we evaluated the operational resilience of our AI vendors?
- Are AI systems integrated into our existing governance and quality processes?
- Are we prepared to respond if an AI system fails or becomes unavailable?
- Does our cybersecurity strategy adequately address AI-enabled technologies?

What Comes Next?

Artificial intelligence will become increasingly embedded within the operational fabric of engineering firms. Rather than existing as a collection of standalone applications, AI will become integrated into project delivery, quality management, document control, knowledge management, client communication, scheduling, financial systems, and other core business processes. As organizations become more connected, operational performance will depend not only on the reliability of individual AI tools, but on how effectively the broader system is governed and managed.

This growing interconnectedness will reshape operational risk. A problem originating in one AI-enabled process may quickly affect project delivery, quality assurance, cybersecurity, client communication, or business continuity. At the same time, organizations will become increasingly dependent on external software providers, cloud platforms, and technology partners whose systems are tightly integrated with their own. Operational resilience will therefore require firms to think beyond individual technologies and manage AI as part of a larger enterprise ecosystem.

The interviews consistently suggest that the firms best prepared for this future will integrate AI into existing operational disciplines rather than creating parallel management structures. Quality management systems, cybersecurity programs, vendor oversight, business continuity planning, and risk management processes will remain essential, but they will increasingly evolve to account for AI-enabled operations. Firms that build upon these existing capabilities will be better positioned to adapt as technologies continue to mature.

Ultimately, the operational challenge is not managing a growing collection of AI tools—it is managing an increasingly interconnected organization. As AI becomes woven into everyday engineering practice, operational resilience will depend less on technological perfection than on disciplined management systems capable of adapting as technology continues to evolve.

10 FINANCIAL AND BUSINESS MODEL RISK

AI DOESN'T JUST CHANGE HOW ENGINEERING FIRMS WORK, IT CHANGES HOW THEY COMPETE.

Managing that transition responsibly will determine whether AI becomes a source of strategic advantage or strategic risk.

What Is the Risk?

Artificial intelligence is often discussed in terms of productivity. Engineering firms understandably ask how AI can reduce repetitive work, improve efficiency, shorten project schedules, and allow employees to accomplish more in less time. These benefits are real.

However, the interviews conducted for this study suggest that productivity represents only the beginning of AI's financial implications. As AI becomes increasingly integrated into engineering practice, firms must also consider how it affects profitability, pricing strategies, investment decisions, utilization, competitive positioning, service offerings, client expectations, workforce economics, and long-term business sustainability.

Historically, many engineering firms have generated revenue based largely on the time required to perform professional services. AI challenges that model by reducing the effort required for certain activities while simultaneously increasing the value firms may be able to deliver.

This creates both opportunity and risk. Organizations that successfully adapt may improve profitability, expand services, strengthen client relationships, and create new competitive advantages. Organizations that fail to adapt may find traditional business models increasingly difficult to sustain. The financial risk therefore extends beyond AI investment. It involves determining how engineering firms will create and capture value in an AI-enabled economy.

What Did We Learn?

The interviews consistently revealed that participants view AI as a business transformation rather than simply a technology investment. Although stakeholders discussed productivity gains, they devoted considerably more attention to competitive strategy, organizational adaptation, client expectations, and long-term business models.

AI CHANGES COMPETITIVE ADVANTAGE.

Several participants observed that AI itself is unlikely to become a lasting competitive advantage. As AI capabilities become increasingly accessible, most firms will eventually have access to similar technologies. The differentiator will instead become how effectively organizations integrate AI into engineering practice, organizational knowledge, client service, workforce development, and business strategy.

PRODUCTIVITY CREATES NEW BUSINESS QUESTIONS.

Engineering leaders generally viewed productivity improvements as desirable. However, several participants also acknowledged that increased efficiency raises difficult business questions. If engineering tasks require fewer labor hours, how should firms measure productivity? How should organizations evaluate return on investment? How should employee performance evolve? How should firms communicate AI-enabled value to clients? Participants generally viewed these as leadership questions rather than technology questions.

CLIENTS WILL INCREASINGLY FOCUS ON OUTCOMES.

Public-sector owners repeatedly emphasized that they purchase engineering expertise—not hours. Participants suggested that clients are ultimately interested in receiving high-quality engineering solutions delivered efficiently, transparently, and responsibly. As AI improves engineering productivity, firms may increasingly compete based upon insight, innovation, responsiveness, and problem-solving rather than simply the amount of effort expended. Several participants suggested this evolution could gradually reshape how engineering value is communicated.

INVESTMENT DECISIONS EXTEND BEYOND SOFTWARE.

Technology providers and AI consultants consistently observed that successful AI implementation requires investment in far more than technology. Organizations must also invest in workforce development, organizational knowledge, governance, data quality, process redesign, and change management. Several participants argued that firms focusing exclusively on AI software while underinvesting in organizational capabilities are unlikely to realize AI's full value.

BUSINESS MODEL INNOVATION IS BEGINNING—NOT ENDING.

Perhaps the most forward-looking finding from the interviews involved business model evolution. Participants discussed AI-native firms, new service offerings, expanded advisory roles, digital engineering capabilities, predictive infrastructure services, and outcome-oriented client relationships. While few believed these changes would occur overnight, most agreed that AI will gradually reshape how engineering firms create value. The interviews suggest that organizations should begin preparing now rather than waiting for competitive pressures to force change.

> "Many firms appear driven by fear that they are falling behind competitors rather than thoughtful evaluation of where AI creates meaningful business value.

ENGINEERING FIRM – LARGE FIRM

What Can Engineering Firms Do?

The interviews identified several practical actions engineering firms can take to strengthen their financial position while preparing for evolving business models.

Executive Leadership

- View AI as a strategic investment rather than simply a productivity initiative.
- Develop long-term business strategies that anticipate AI-enabled competition.
- Measure AI success using both operational and strategic outcomes.
- Encourage innovation while maintaining disciplined investment decisions.

Engineering Leaders

- Identify engineering activities where AI enhances value rather than simply reducing effort.
- Redesign workflows to allow engineers to focus on higher-value activities.
- Share successful AI applications across business units.
- Continue emphasizing engineering quality as the firm's primary differentiator.

Project Delivery Leaders

- Identify opportunities to use AI to improve project efficiency, quality, and client value while maintaining professional standards.
- Provide feedback on how AI affects project delivery, resource utilization, and client service to help inform organizational investment decisions.
- Share successful AI-enabled project practices that can be scaled across the organization to improve performance and return on investment.

Technology Leaders

- Prioritize AI investments supporting enterprise capabilities rather than isolated use cases.
- Integrate AI with organizational knowledge and operational systems.
- Continuously evaluate emerging AI technologies for business value.
- Monitor vendor capabilities as AI platforms evolve.

Human Resources & Learning

- Prepare employees for evolving engineering roles.
- Align professional development with future organizational needs.
- Recognize skills supporting innovation, collaboration, and AI-enabled engineering practice.
- Encourage continuous organizational learning.

Risk Management & Legal

- Evaluate AI investments using both financial and strategic criteria.
- Monitor contractual implications associated with AI-enabled services.
- Assess emerging business risks alongside new revenue opportunities.
- Review pricing strategies as AI capabilities mature.

Together, these actions help organizations move beyond viewing AI solely as a cost-saving initiative toward using AI as a catalyst for long-term business transformation.

What Questions Should Every Engineering Firm Ask?

- Are we treating AI as a technology purchase or as a business transformation?
- How will AI influence the way our firm creates value for clients?
- Are our investments in people, data, and governance keeping pace with our technology investments?
- How should we measure success beyond productivity alone?
- How might AI change the way our clients evaluate engineering services?
- Are we preparing for future business models rather than optimizing only today's operations?

What Comes Next?

Artificial intelligence will continue reshaping the economics of engineering practice. While many organizations initially adopt AI to improve productivity and reduce routine effort, the interviews consistently suggest that these benefits represent only the beginning of a much broader transformation. As AI becomes commonplace, productivity improvements alone are unlikely to provide a lasting competitive advantage because access to advanced AI capabilities will become increasingly widespread across the profession.

The more significant opportunity lies in how engineering firms redefine the value they create. AI has the potential to improve decision-making, strengthen quality, accelerate project delivery, enhance client collaboration, expand advisory services, and unlock new ways of delivering expertise throughout the infrastructure lifecycle. Firms that continue measuring success primarily through labor efficiency may capture short-term gains but overlook much larger strategic opportunities.

The interviews also suggest that competitive advantage will increasingly depend on how effectively organizations combine technology with engineering expertise, institutional knowledge, trusted client relationships, and sound business strategy. AI may automate certain activities, but it cannot replace the professional judgment, creativity, collaboration, and client confidence that define successful engineering firms. Those capabilities will become increasingly important as routine technical work becomes more automated.

Ultimately, artificial intelligence is unlikely to redefine the value of engineering—it will redefine how that value is created and delivered. The firms that thrive will not simply be those that become more efficient. They will be those that leverage AI to strengthen client outcomes, expand professional capabilities, and create new forms of value that competitors cannot easily replicate.

11 STRATEGIC LEADERSHIP AND ENTERPRISE GOVERNANCE RISK

SUCCESSFUL AI ADOPTION IS ULTIMATELY A LEADERSHIP CHALLENGE, NOT A TECHNOLOGY CHALLENGE.

The firms that manage AI risk most effectively will be those that align governance, engineering judgment, organizational knowledge, and strategic leadership across the enterprise.

What Is the Risk?

Artificial intelligence is often introduced into organizations through technology. But it should be governed through leadership. As engineering firms adopt AI across design, project management, business operations, knowledge management, client service, and decision-making, leaders face a challenge unlike any previous technology transformation. AI affects nearly every aspect of organizational performance while simultaneously introducing new technical, legal, operational, financial, workforce, and ethical considerations.

This creates a significant enterprise risk. When AI governance is fragmented across departments, organizations may develop inconsistent policies, duplicate investments, conflicting expectations, uneven adoption, and unmanaged risks. Conversely, firms that approach AI as an enterprise capability can align technology, people, data, governance, quality, and business strategy around a common vision.

The risk is therefore not simply poor AI implementation. The greater risk is organizational misalignment. Without effective leadership, even technically successful AI initiatives may fail to deliver lasting organizational value.

What Did We Learn?

The interviews consistently revealed that successful AI adoption depends far more on organizational leadership than technological sophistication. Participants repeatedly emphasized that AI governance is becoming an executive responsibility requiring coordination across the entire enterprise.

AI GOVERNANCE BEGINS WITH LEADERSHIP.

Perhaps the clearest finding across all stakeholder groups is that AI governance cannot be delegated exclusively to information technology departments. Technology providers emphasized organizational architecture. Engineering firms discussed operational implementation. Legal professionals focused on accountability. Licensing authorities emphasized responsible charge. AI consultants described organizational transformation. Despite these different perspectives, participants consistently pointed toward executive leadership as the integrating force bringing these functions together.

GOVERNANCE REQUIRES SHARED RESPONSIBILITY.

Participants consistently rejected the idea that AI governance belongs to one department. Instead, they described governance as a coordinated organizational effort. Executive leadership establishes vision. Engineering leaders oversee professional practice. Technology leaders manage platforms and infrastructure. Human resources prepares the workforce. Risk management and legal monitor compliance. Business leaders evaluate strategic opportunities. Successful organizations recognize that every function contributes to responsible AI adoption.

GOVERNANCE SHOULD ENABLE INNOVATION—NOT RESTRICT IT.

One of the most encouraging findings emerging from the interviews is that participants rarely viewed governance as bureaucracy. Instead, governance was consistently described as the mechanism allowing organizations to innovate with confidence. Well-designed governance provides clarity. It defines expectations. It establishes accountability. It reduces uncertainty. Most importantly, it enables employees to experiment responsibly within well-understood organizational boundaries. Participants repeatedly emphasized that governance should accelerate learning rather than discourage innovation.

AI MATURITY REFLECTS ORGANIZATIONAL MATURITY.

Several participants observed that AI readiness cannot be measured simply by counting software licenses or technology deployments. Instead, mature organizations demonstrate clear executive sponsorship, enterprise governance, trusted organizational data, workforce readiness, responsible engineering practices, effective change management, and continuous organizational learning. These characteristics reinforce that AI maturity reflects the maturity of the organization itself.

LEADERSHIP DETERMINES ORGANIZATIONAL CULTURE.

Perhaps the most significant finding emerging from the interviews is that leadership ultimately shapes every other dimension of AI risk. Leadership influences organizational culture. Culture influences employee behavior. Employee behavior influences governance. Governance influences trust. Trust influences successful AI adoption. Viewed this way, leadership becomes the foundation upon which every other risk domain depends.

> If your AI strategy is being driven by IT, you will fail.
>
> **AI CONSULTANT**

What Can Engineering Firms Do?

The interviews identified several practical actions engineering firms can take to strengthen enterprise governance while supporting responsible AI adoption.

Executive Leadership

- Develop a firm-wide AI vision aligned with organizational strategy.
- Establish cross-functional governance involving engineering, technology, operations, legal, risk management, and human resources.
- Assign executive accountability for AI governance.
- Monitor organizational AI maturity as part of enterprise planning.
- Encourage responsible experimentation while maintaining clear expectations.

Engineering Leaders

- Ensure AI governance aligns with professional engineering practice.
- Reinforce engineering judgment throughout AI-assisted workflows.
- Integrate AI into quality assurance and project delivery processes.
- Share successful practices across business units.

Project Delivery Leaders

- Implement organizational AI governance policies consistently across project teams and reinforce expectations for responsible AI use.
- Provide feedback to leadership on governance challenges, operational barriers, and emerging risks encountered during project delivery.
- Support continuous improvement by sharing successful implementation practices and lessons learned that can strengthen enterprise AI governance.

Technology Leaders

- Develop secure enterprise AI environments.
- Integrate AI platforms with trusted organizational knowledge.
- Continuously evaluate emerging technologies.
- Support governance through transparency, monitoring, and reporting.

Human Resources & Learning

- Build AI literacy across every level of the organization.
- Redesign leadership development for an AI-enabled profession.
- Encourage continuous learning and interdisciplinary collaboration.
- Prepare future leaders to govern AI responsibly.

Risk Management & Legal

- Coordinate enterprise AI governance with existing risk management processes.
- Monitor regulatory developments.
- Periodically review organizational AI policies.
- Evaluate emerging enterprise risks associated with evolving AI capabilities.

Together, these actions help organizations build governance systems that support innovation while protecting engineering quality, organizational resilience, and public trust.

What Questions Should Every Engineering Firm Ask?

- Do we have a clear organizational vision for AI?
- Who is ultimately accountable for AI governance within our firm?
- Are engineering, technology, legal, operations, and business leaders working together?
- Does our governance encourage responsible innovation rather than unnecessary restriction?
- Are we continuously evaluating our AI maturity as technology evolves?
- Are we leading AI adoption—or simply reacting to it?

What Comes Next?

Artificial intelligence will continue evolving far beyond the capabilities available today. New models, new regulations, new business applications, and new engineering workflows will continue emerging over the coming years, making it impossible for engineering firms to predict every technological or regulatory change that lies ahead. The interviews consistently suggest, however, that uncertainty itself has become one of the defining characteristics of AI leadership.

This research also suggests that the engineering firms most likely to succeed will not necessarily be those that adopt AI first or invest the most in technology. They will be the organizations that build the leadership capabilities needed to adapt responsibly as technology evolves. Throughout the interviews, participants repeatedly emphasized that effective AI governance depends upon leaders who can balance innovation with professional responsibility, encourage experimentation while managing risk, invest in people as much as technology, and create organizations capable of learning continuously.

Perhaps the most important finding emerging from this study is that artificial intelligence is not fundamentally changing the engineering profession's purpose. Engineers will continue protecting the health, safety, and welfare of the public. Firms will continue earning client trust through technical excellence, sound judgment, and professional integrity. What AI changes is the organizational capability required to fulfill those enduring responsibilities in an increasingly digital profession.

Ultimately, successful AI adoption is not a technology challenge—it is a leadership challenge. The firms that thrive will not simply implement better AI systems. They will build stronger organizations: organizations with disciplined governance, trusted knowledge, capable people, resilient operations, ethical cultures, and leaders prepared to navigate continuous change. Those capabilities will define not only how engineering firms manage AI risk, but how they compete, innovate, and serve society in the decades ahead.

CONCLUSION

Artificial intelligence represents one of the most significant technological developments the engineering profession has experienced in decades. Its capabilities will continue advancing, its applications will continue expanding, and its influence on engineering practice will continue growing. While the pace of technological change remains uncertain, one conclusion emerging from this research is clear: managing AI risk is no longer a future consideration—it is a present leadership responsibility.

Throughout this study, stakeholders consistently emphasized that the greatest AI risks facing engineering firms extend well beyond the technology itself. Technical reliability, professional liability, data governance, workforce development, ethics, operational resilience, business strategy, and leadership are deeply interconnected. Decisions made in one area inevitably influence the others. Effective AI risk mitigation therefore requires engineering firms to move beyond isolated policies or individual technology investments toward a coordinated, enterprise-wide approach to governance and risk management.

Perhaps the most striking finding of this research was the strong convergence of perspectives across stakeholder groups. Participants representing engineering firms, public infrastructure owners, technology vendors, AI consultants, insurance and legal professionals, and the engineering licensing community each brought unique perspectives to the discussion. Yet despite their different roles and responsibilities, they consistently identified many of the same organizational challenges and emphasized similar priorities for responsible AI adoption. That convergence provides confidence that the framework presented in this report reflects not simply one viewpoint, but a broad consensus emerging across the engineering ecosystem.

The research also reinforces an important reality about the engineering profession. Artificial intelligence does not change the engineer's fundamental responsibility to protect the health, safety, and welfare of the public. It does not diminish the importance of professional judgment, technical competence, ethical decision-making, or accountability. If anything, the interviews suggest that these responsibilities become even more important as AI assumes a greater role in engineering practice. Technology may accelerate analysis and improve efficiency, but responsibility remains with people.

For engineering firm leaders, the implications are both practical and strategic. AI risk cannot be managed by the information technology department alone, nor can it be addressed solely through new software, policies, or compliance requirements. Effective risk mitigation requires leadership commitment, cross-functional collaboration, disciplined governance, workforce investment, and continuous organizational learning. Firms that strengthen these capabilities will be better positioned not only to reduce AI-related risks, but also to realize AI's potential to improve engineering quality, strengthen client relationships, expand professional services, and create long-term competitive advantage.

This research intentionally avoids prescribing a single roadmap for AI adoption. Engineering firms vary considerably in their size, markets, organizational structure, technical maturity, and strategic priorities. There is no universal sequence of implementation that will be appropriate for every organization. Instead, the AI Risk Framework presented in this report is intended to provide a practical foundation that firms can adapt to their own circumstances as technologies, regulations, and business needs continue to evolve.

Ultimately, successful AI adoption will not be determined by which firms deploy the most advanced technologies or automate the greatest number of tasks. It will be determined by which organizations most effectively integrate AI into the enduring principles that have always defined professional engineering: technical excellence, sound judgment, responsible governance, ethical conduct, and an unwavering commitment to protecting the public.

Artificial intelligence will undoubtedly reshape how engineering firms work. It should never redefine why they exist.

AI risk is no longer a future consideration — it's a present leadership responsibility.

THANK YOU TO OUR CONTRIBUTORS

The ACEC Research Institute provides the engineering industry with cutting edge research, trend data, and economic analysis to help firm owners make decisions and delivers thought leadership that advances engineering's essential value to society.

The ACEC Research Institute wishes to extend its sincere appreciation to its generous contributors.

As of August 2026

Visionary Circle

ACEC Life/Health Trust – Est. 1965
Autodesk
benesch
CMT – Crawford, Murphy & Tilly
Deltek – Speed. Clarity. Control.
HDR
Kimley»Horn – Expect More. Experience Better.
morrissey goodale
RS&H
stv
Terracon
vhb

Founder Circle

ACEC
ACEC – American Council of Engineering Companies California
ACEC New York – American Council of Engineering Companies of New York
ACEC NC – American Council of Engineering Companies of North Carolina
ACEC Retirement Trust – Your Future Reimagined
ACEC Texas
AET
Bentley
BST Global
Burns McDonnell
DJ&A
HNTB
JMT
Mead & Hunt
olsson
Stanley Consultants

Chair Circle

ACEC Ohio · ARCADIS · ARDURRA · CDM Smith · CHARTWELL

chenmoore · Colliers Engineering & Design · ECS · FREESE NICHOLS · GFT

Gresham Smith (Genuine Ingenuity) · GUIDA GEOSPATIAL SOLUTIONS · halff · HANSON · Hazen

HED · HRGreen · IMEG · KCI · Kennedy Jenks

LAMP RYNEARSON · MARTIN/MARTIN CONSULTING ENGINEERS · MERRICK · moffatt & nichol · MOTT MACDONALD

MSA · OHM · Pennoni · PKF O'CONNOR DAVIES ACCOUNTANTS AND ADVISORS · PSOMAS

Sargent & Lundy · Schnabel ENGINEERING · SME · SSOE

SSR · Stolfus · Trilon · UES · WADE TRIM

walter p moore · Weston & Sampson · WILSON & COMPANY · Woodard & Curran · wsb

WSP · Jay & Ann Wolverton · Thunder Road Charitable Fund

President Circle

ACEC American Council of Engineering Companies of Michigan · CHA · EFCG · JENSEN HUGHES · SHANNON & WILSON

TYLin · Daphne & Jeff Bryant · M. Gayle Packer · Kenneth & Sheri Smith

Keystone Circle

BHC Birkhoff, Hendricks & Carter, L.L.P. · FOXXSTEM · SHELADIA ASSOCIATES, INC. · SUMMER CONSULTANTS INCORPORATED

ACEC RESEARCH INSTITUTE

FIRM OF THE FUTURE

@ACECResearch

ACEC Research Institute