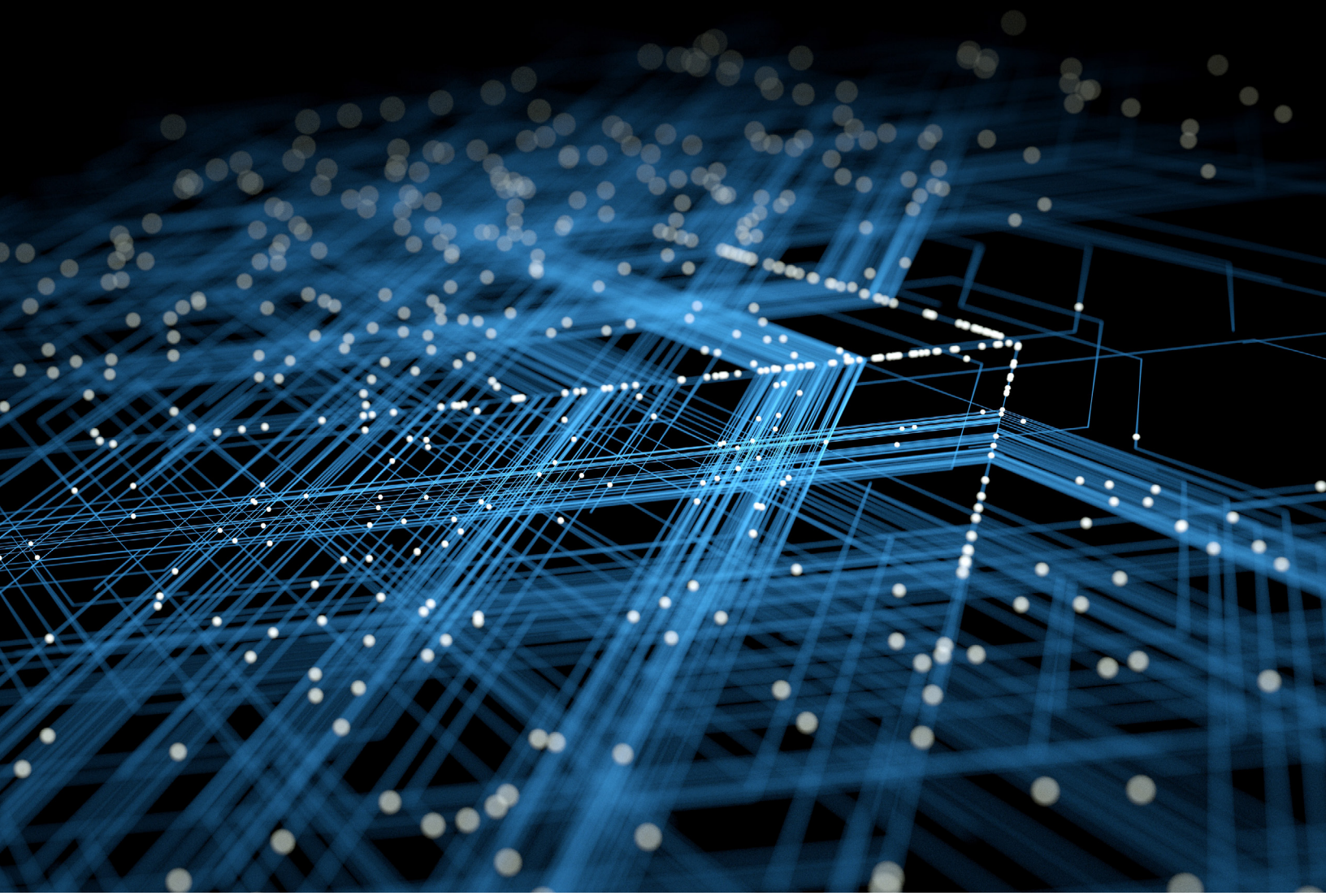
Construction Quarterly

Building a Smart & Sustainable Approach to AI

November 2025

forvis mazars

The construction industry is buzzing with talk of new technology. Robotics, advanced automation, machine learning, generative artificial intelligence (AI), natural language processing—the list keeps growing. The sentiments are that these tools will revolutionize the way we work, with an underlying message of full adoption in order to stay ahead.



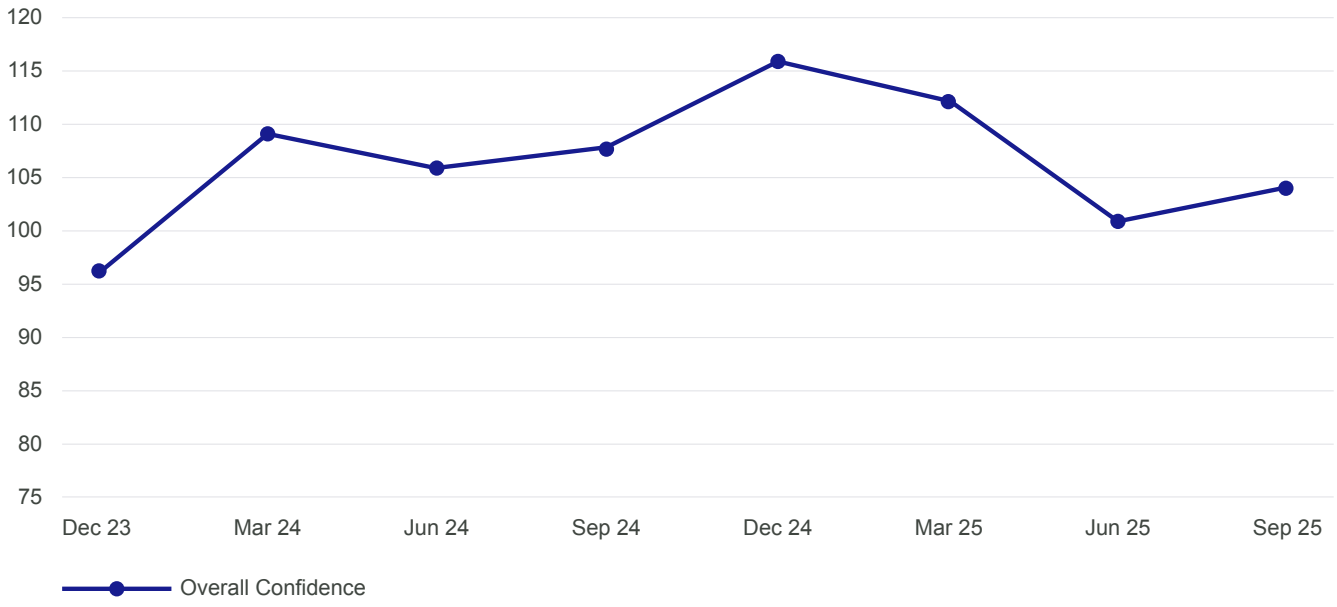
But for many, these technologies still feel elusive. It's overwhelming enough to understand what they are, and even more daunting to figure out how to implement them. Where do you even begin?

The truth is, you don't have to use everything. And you certainly don't have to do it all at once. The key is to quiet the noise and start small. While waiting too long could put you at a competitive disadvantage, moving too fast can be just as risky. This quarter, we want to examine how to build a foundation for sustainable innovation, and next quarter, we'll explore practical ways to adopt some of this new technology so that you're not left behind.

Industry Sentiment Is Improving, but Fears Around AI Persist

Each quarter, the Construction Financial Management Association (CFMA) releases an index tracking construction leaders' confidence in the industry. This past quarter, confidence ticked up slightly from Q2. Overall sentiment remains cautious but slightly optimistic.

Overall CONFINDEX Confidence Index



The findings don't surprise us. In the comments section of the report and in our own conversations with construction company CFOs and CEOs, we're hearing much of the same: backlogs may still be strong, but several factors such as interest rates, tariffs, and the uncertain political environment result in leaders feeling unsure about what's next.

At the forefront of many of our conversations, though, especially these past few quarters, is AI. Construction leaders are concerned about how to implement AI and how to do so safely.

One respondent put it this way: "It's here, we need it, but can we safely benefit from it?" Data security is certainly a concern, but leaders are also worried about how AI could affect their projects. Another respondent said, "The pace at which AI is being peddled by consultants has the potential for the industry to mismanage its impact on project execution."

Data security and project viability are both valid concerns, but they're not insurmountable. We think there are plenty of opportunities to adopt AI: construction companies even have the opportunity to be early adopters of certain solutions. However, there's a tactical path to follow.

The Challenge With AI in Construction

Construction leaders see AI's potential, but they worry about two things: (1) data security, and (2) its impact on project execution.

Strategize & Prepare for AI

Before implementing any new technology, whether it's cutting-edge or well-tested, your systems and your people must be prepared to handle it. When we talk with clients about their AI strategy, we take the same structured approach we use for any major technology adoption. It's a four-step process:

In This Quarter's Report:

1 **Strategize**

2 **Prepare**

Coming Soon:

3 **Protect & Contol**

4 **Implement & Optimize**

In this quarter's report, we want to focus on the first two steps, Strategize and Prepare, which is everything that should happen before new technology goes live. Steps three and four will be covered at a later time.

Step 1: Strategize

An effective AI strategy begins with thoughtful planning and alignment across all parts of your business. If you adopt AI without a well-defined strategy, you are exposing yourself to several risks, such as:

- Wasting time, money, and effort.
- Getting inconsistent or unreliable results.
- Losing visibility into what data is being used, who's using it, and how it's being used.
- Eroding employee trust.
- Missing opportunities for smaller, easier, and less costly wins.
- Throwing away the opportunity to hone best practices that you can apply to future larger-scale solutions.

In order to decrease risk, it is imperative to map out exactly how you'll use AI, why you want to use it in that way, and how it will make a difference. Here are a few things you can do:

Identify Clear Use Cases

Pinpoint the areas where AI could deliver meaningful value. Note existing challenges, then explore if AI could solve those problems. A few questions you can ask yourself are:

- What data-driven decisions do we make? And is the data we're using (1) reliable, and (2) easy to collect and interpret?
- Can this solution scale, or will it only apply in one specific situation?
- What are our employees struggling with most?
- What outcomes are important to us? Are we aiming to reduce costs, improve safety, boost productivity, enhance data accuracy, or something else?

AI should serve your business goals, not the other way around. In other words, don't adopt AI simply to keep up with trends or out of fear of being left behind; use it as a tool to reach goals that you already have.

Assess Operational Efficiencies

In construction, we haven't seen a situation where AI replaces people. However, we have seen that it helps individuals work more efficiently. Focus your energy here. What AI tools could help your team work smarter? Where could it save them time? Not only will this improve worker performance, but it could relieve some of the workforce pressures that have challenged the industry for decades.

Build a Road Map

Right now, AI can feel like the wild west. People are experimenting, but few are following any sort of map or plan. This enthusiasm is admirable and almost always comes from a good place, but it can also lead to confusion and risk. A clear road map establishes the following big-picture goals:

- **Priorities**: Identify which AI initiatives align closest with your business goals.
- **Timelines**: Set realistic milestones for evaluation, testing, and implementation.
- **Accountability**: Define who owns and oversees stages of the process.
- **Resources**: Allocate funding and worker hours to help make AI adoption successful.
- **KPIs**: Select the key performance indicators (KPIs) that will tell you if your solutions have been successful.

These thought exercises and simple tasks can help ensure that groundwork is present for sustainable success with the AI tools your organization chooses to adopt.

Step 2: Prepare

In the preparation phase of your AI adoption journey, your focus should shift from ideas to infrastructure. It's here where you'll build out your governance procedures, controls, and safeguards that help ensure the responsible, secure, and effective use of AI. Here are a few things you can do:

Strengthen & Update Cybersecurity Protocols for AI

Before you implement new technology, your systems must be ready to protect your company and customer data. AI tools are still evolving, and many are not well tested, so it's important that your security solutions protect against potential weaknesses in those third-party (or even proprietary) software solutions. A few simple cybersecurity best practices to apply to AI include:

- Increase your patch frequency. AI-driven attacks move faster than traditional ones, and your defenses should move just as quickly.[1]
- Ensure multifactor authentication (MFA) across your entire organization, especially for cloud-based AI tools.[2]
- Train your team on how to spot AI-enabled threats like deepfakes and sophisticated phishing emails.[3]
- Maintain strong audit trails so you know how AI is being used and by whom.
- Regularly test AI models, both for efficacy and for security.
- Always have human oversight over AI-driven processes.

Use AI to Protect Against AI-Enabled Threats

Don't leave AI to the criminals: AI tools can be some of your strongest defenses.[4] A few ways you can use these tools to protect against cyberattacks include:

- Using AI to generate mock phishing or vishing messages to test employee readiness.[5]
- Monitoring user activity and detecting unusual behavior patterns using AI analytics.
- Instructing AI to analyze large volumes of data to spot anomalies.
- Automating responses with AI if certain malware, ransomware, or intrusion attempts are noted.[6]
- Utilizing AI to predict or test for vulnerabilities in the system.[7]

1 "AI-Based Attacks: Navigating the Modern Arms Race in U.S. Cybersecurity," bizjournals.com, Oct 1, 2025.
2 Ibid.
3 Ibid.
4 Ibid.
5 Ibid.
6 Ibid.
7 Ibid.

Step 2: Prepare

Update Internal Controls

Internal controls should always be a focus of good governance, but with AI, it's especially crucial to protect your data. It is critical to make sure AI secures data and doesn't alter it behind the scenes. Some controls to consider are:

- Limiting who can upload or feed data into the AI system, particularly for project plans, schedules, and financial models.
- Labeling what's confidential so that AI systems don't inadvertently expose project plans, proprietary designs, or bids to others without proper permissions.
- Encrypting and backing up key datasets to safeguard data integrity and regularly testing that the data hasn't changed.
- Requiring human sign-offs and oversight before applying AI-generated recommendations.
- Regularly questioning AI assumptions so that errors aren't propagated across multiple projects.

Build an AI Policy

This policy will serve as the company's manual, detailing how to use AI within your organization. Some areas it should outline are:

- The purpose of the policy and who it applies to.
- What types of AI tools it covers.
- Who is responsible for approving new uses for AI.
- Who is on the cybersecurity team, and what decisions they have the power to make.
- When AI can be used, by whom, and in what situations.
- How the data will be protected and stored.
- What the process is for vetting third-party vendors that use AI.
- How AI protocols will be monitored.

Your AI policy should also address the ethical use of AI. This includes ensuring AI is used transparently, that it doesn't introduce bias, that it avoids compromising safety or employee well-being, and that it's using fairly obtained information.

Prepare Your Workforce

Before you implement an AI tool, train employees on how it works and how they can use it. Your employees will act as first responders when interacting with the AI tools. Their involvement can help identify issues during the implementation and testing phases, reinforcing the importance of education and that employees know what to look for when testing. It's equally crucial to secure executive buy-in, since your leaders set the tone of corporate culture: how they view and talk about AI can help inform employees and support their comfort with adoption.

Quiet the Noise

Don't let the AI noise overwhelm you. Yes, learn about new AI solutions and talk to cohorts about what they're doing, but don't let those facts alone guide your decisions. Step back, look inward, and focus on your business's needs. Start with a few practical actions you can take today. Even if those actions are simple, they'll build a solid foundation that will make it easier to tackle your next set of priorities. By starting small and expanding thoughtfully, your organization will gain confidence and set itself up for long-term success.

Contributors

Daniel Gaston
Partner & Construction Leader
daniel.gaston@us.forvismazars.com

Daniel Miles, III
Partner
dan.miles@us.forvismazars.com

Aprille Bell
Partner & National Sector Leader
aprille.bell@us.forvismazars.com

Ryan Kauzlick
Director
ryan.kauzlick@us.forvismazars.com

Mark Wilkerson
Partner
mark.wilkerson@us.forvismazars.com

Janeen Butler
Senior Manager
janeen.butler@us.forvismazars.com

Scott Yandle
Partner
scott.yandle@us.forvismazars.com

Sarah Windham
Assistant Managing Partner
sarah.windham@us.forvismazars.com

For more information and construction industry insight, visit forvismazars.us/construction.