KPMG

Voice of the CIO

A recurring conversation with CIOs on IT-related issues

March 2026

AI use accelerates, but CIOs are still in the early innings

Despite the rapid acceleration of artificial intelligence (AI), chief information officers (CIOs) still find themselves in the early innings of integrating the technology into enterprise operations.

CIOs are grappling with the fast pace of change, noting how quickly new AI announcements can impact market dynamics and business models. From the potential "death of SaaS" to the proliferation of powerful AI capabilities, the landscape is evolving at a breakneck speed, making it challenging for organizations to keep up.

Nevertheless, CIOs are forging ahead to reap the benefits of AI's promise. Many companies are using agile principles to help guide their AI journey, namely, actively exploring AI's role in uncovering value, establishing proper governance, preparing data, and developing essential skill sets, all while balancing new cybersecurity threats. Progress varies, with some organizations having more advanced deployments in engineering and customer support, while others are still in the early stages of experimentation and ideation. But wherever they are on their AI journey, CIOs are committed to creating strategic approaches to navigate the complexities of AI adoption and integration.

On the CIO agenda

Organizational evolution

Embracing democratization, agile implementation, and strategic governance

Quantifying value, measuring efficiency

Determining tangible ROI from AI remains elusive

Shaping the future AI workforce

Talent, training, and evolving roles

Organizational evolution

Embracing democratization, agile implementation, and strategic governance

The integration of AI is fundamentally reshaping organizational structures and prompting a re-evaluation of traditional information technology (IT) models. Many organizations are transitioning from a project-based approach to a platform-centric product model, aiming to foster continuous innovation and better leverage technology. This shift—employing agile principles—is crucial for adapting to the dynamic AI landscape, allowing for faster adoption, experimentation, and evolution.

A key aspect of this transformation is the "democratization of technology," where the idea of "everyone can be a builder" is gaining traction, challenging conventional boundaries between IT and the business. However, this concept requires a clear definition of what "building" entails, as it can range from complex application development to leveraging AI tools for individual productivity. One CIO of an environmental services company advocated that "everyone should have the opportunity to be a part of the build process," acknowledging that while not all will achieve advanced technical mastery, they can still contribute valuable ideas.

However, there is a delicate balance between encouraging AI adoption while at the same time ensuring security, data privacy, and regulatory compliance. Implementing widespread AI access requires robust governance frameworks to prevent uncontrolled tool sprawl and ensure security and compliance. Clearly, a free-for-all isn't the answer. Rather, what's required is a new governance strategy that provides "a little bit of freedom" but also robust guardrails for tracking usage and preparing for regulatory oversight.

Companies are developing "citizen IT" frameworks and expanding them to cover AI use cases, providing guidelines and centralized support through an AI Center of Excellence (CoE). Governance committees are crucial for reviewing AI initiatives, particularly to manage risks related to data, legal implications, and ethical concerns. The goal is to avoid stifling innovation while maintaining control, a balance often achieved through policy-driven restrictions for high-risk areas and process-driven flexibility for other initiatives. As the CIO of a consumer electronics company put it, the role of compliance and privacy in this new era should be: "Your job isn't to block. It's to say yes but keep us safe."

This mindset shift emphasizes enabling responsible AI adoption across the enterprise, acknowledging that IT cannot manage everything, but must provide the necessary infrastructure and guidance.

> "It still feels like we're in the first inning of AI for large enterprises."
>
> —Marcus Murph, US Technology Consulting leader

Quantifying value, measuring efficiency

Determining tangible ROI from AI remains elusive

A significant and continuing challenge for CIOs is measuring the tangible value and efficiency gains from AI investments.

A CIO from a pharmaceutical company highlighted the difficulty in capturing efficiency, noting that individual benefits often don't translate into broader organizational impact. Senior leaders frequently question the absence of tangible efficiency gains, illustrating a gap between perceived and actual value. This challenge reflects the "diffusion of innovation curve," where the initial "magic" created by innovators struggles to be industrialized for early and late majority adopters who require proven value.

While some teams report substantial productivity increases, these gains are often "fragmented" across individual users or specific, easy use cases like customer support. Boards and senior leadership often have high expectations for "massive efficiencies," sometimes citing figures as high as 80 percent. However, the CIO of a pharmacy-benefit management firm noted that such high figures are often seen in new or "greenfield code" development, with "brownfield" (modifying existing code) yielding more modest gains of 20 percent to 30 percent. This disparity highlights the need to differentiate between notional opportunities and real, finance-validated productivity gains, focusing on profit-and-loss impact rather than inflated estimates.

Cybersecurity also remains a top concern, especially with the emergence of weaponized AI. Bad actors are leveraging AI to launch sophisticated attacks, such as generating new malware or highly convincing phishing emails, creating an "arms race" against traditional defenses. This development necessitates a shift from protecting specific high-value targets to securing "every door, every window" as AI-powered bots can attack every available surface. The infiltration of code libraries by malicious actors also poses a threat to AI-generated code.

Legal and compliance issues further complicate AI adoption, particularly concerning data privacy, data loss, and copyright. Legal teams are often hesitant to allow sensitive data into AI tools. The use of AI summarization for meetings, for instance, raises questions about transcript retention and discoverability, requiring careful navigation of legal boundaries.

To help alleviate these conflicts, CIOs should consider encouraging direct engagement between legal teams and tech providers' legal departments to address specific concerns and understand risk. Another tactic, supported by the CIO of a food manufacturer, is to expand the data governance committee beyond traditional oversight roles (e.g., chief legal officer) to include business leaders who can champion the advantage offered by technology.

"In many of the discussions that I've had, the thinking is if we deploy this tool, we can save X many headcount. That's the wrong thinking. It should be if we deploy this, we can do 10 times as many things as we did before."

—CIO for electronic consumer products company

Shaping the future AI workforce

Talent, training, and evolving roles

The advent of AI is profoundly impacting the talent and workforce landscape, necessitating significant adjustments in skill sets, training, and recruitment strategies. CIOs observe a shift where AI is not only replacing jobs but also transforming them, requiring employees to learn how to effectively work *with* AI. The notion that AI will lead to "massive amounts of people leaving" is now considered a fallacy. While some roles may indeed be phased out, the expectation is that job roles will shift rather than being eliminated *en masse*, creating a need for continuous upskilling, and that new roles, such as AI engineers, are emerging.

Nevertheless, CIOs recognized that there's a noticeable fear among some employees, especially in middle management and traditional IT staff, about job displacement. The CIO of an industrial products company highlighted the resistance among even some existing software engineers to adopt new coding agents. Leaders must emphasize that AI will empower, rather than eliminate, roles. As the CIO of a healthcare company put it, "AI will replace people who don't use AI. But AI will not replace an entire section of people."

Forward-looking organizations are actively focusing on training and talent acquisition. For example, a chemical manufacturer CIO described weekly meetings where team members share their AI successes, fostering excitement and peer learning.

Some companies are even prioritizing young talent in recruitment who demonstrate an aptitude for generative AI tools, recognizing that these individuals often hit the ground running with advanced capabilities.

For instance, the CIO of an industrial-products company pointed to its strategy of leveraging its large internship program to identify and prioritize students who demonstrate AI tool proficiency, even over those with perfect academic records, noting that such interns can "outproduce like second-year engineers."

However, conversations around the changing workforce roles also raise concerns about the escalating cost of retaining highly skilled AI engineers. The long-term implications for the workforce structure, particularly the potential reduction in entry-level jobs, are also a topic of discussion, leading to questions about how to maintain a balanced "pyramid" of talent within organizations. The overarching goal is to prepare the existing workforce for new roles and new ways of working, fostering a culture of adaptability and continuous learning.

> "We're telling them that there are roles that will be transformed, there are roles that will be removed, and there will be roles that will be new."
>
> —CIO of consumer products marketing company

Key considerations

- **Strategic governance and risk management:** Create flexible governance frameworks that support innovation while ensuring security, legal, and compliance requirements. Promote collaboration between legal and tech teams to address data use, intellectual property, and retention policies.
- **Quantify value and highlight impact:** Focus on measuring AI's effect on business results, clearly separating productivity improvements from strategic expansion. Use demos to involve leadership and demonstrate both AI's potential and implementation effort.
- **Invest in workforce transformation:** Address employee concerns about AI by focusing on upskilling and role evolution. Create training and recruitment programs to attract AI talent and help current staff integrate AI into their work.

Additional resources

Sophisticated AI collaboration: An inside look at high-impact use

From automation to AI: Tech leaders are focused on ROI

Revolutionize Your Software Development with Agentic AI

Why knowledge engineering is the key to AI agent value

Marcus Murph
US Technology Consulting Leader
KPMG LLP
T: 214-840-2671
E: marcusmurph@kpmg.com

John Celi
Principal, CIO Advisory
KPMG LLP
T: 617-988-1000
E: jceli@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**