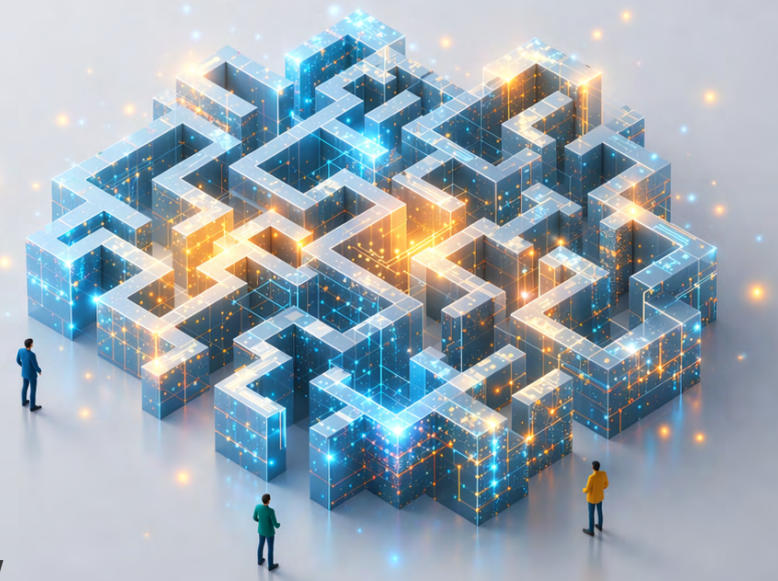
THE
kyndryl
institute



Trend Topic: **Sovereignty**

By

Victoria Espinel

CEO of the Business Software Alliance

Victoria Espinel is CEO of the Business Software Alliance, advancing enterprise software companies' leadership on artificial intelligence, privacy, cybersecurity, and digital trade. Victoria has grown the organization's worldwide presence in over 30 countries, she frequently testifies before Congress, and is a leading voice in media, including the Wall Street Journal, the New York Times, Financial Times, and Bloomberg News.

Prior to BSA, Victoria served as the first White House "IP Czar" under President Obama and the first chief US trade negotiator for intellectual property and innovation under President Bush.

Explore more from The Kyndryl Institute
kyndryl.com/institute

How to mitigate uncertainty to protect AI adoption

Uncertainty has always been a companion to technological change.

What's different about our moment — the AI moment — is the sheer number of dimensions along which that uncertainty is unfolding simultaneously.

There is the uncertainty about the technology itself: how capabilities will evolve, which tools are sufficiently mature for enterprise-wide deployment, and how to successfully enable the workforce to use them. Additionally, there is a lack of clarity regarding genuine AI deployment -not only at an individual enterprise-level but also across whole industries. While there are myriad surveys and reports that assess whether employees are using AI, or the extent of company investment into AI, there is still a gap in terms of evaluating the depth and breadth of AI usage in the enterprise.

Regulatory uncertainty adds to the mix, as governments worldwide grapple with how to address the risks of AI in a way that builds trust in technology and encourages innovation.

And then there is the ever-present uncertainty of geopolitics. For enterprises operating across borders, what is playing out on the global stage today is reshaping how teams think about digital sovereignty, international data flows and even basic technological access.[1]

Taken together, this multi-dimensional uncertainty has become, in my view, the single greatest barrier to AI adoption at the enterprise level. The organizations best poised to successfully navigate this moment will stop treating uncertainty as a reason to pause and start treating its management and mitigation as a core strategic competency.

Multi-dimensional uncertainty has become, in my view, the single greatest barrier to AI adoption at the enterprise level.

Building governance that can bend without breaking

Internal governance practices that can evolve with technology and respond to dynamic regulatory and geopolitical currents offer a path forward for organizations to further their AI adoption.

If the back-and-forth over the EU AI Act shows us anything, it is that AI regulation won't follow a straight line.[2] We see regulators in the EU as well as other jurisdictions around the world wrestle with the balance between safeguards that build trust and enable innovation, even as our understanding of AI and its implications grows.

Many regulatory proposals have additionally focused on data protection as well as citizens and businesses' access to data and information. Policymakers are looking more carefully at measures affecting how data is stored, processed and governed under the laws of the jurisdiction in which an organization operates.

For organizations operating across borders and jurisdictions, data is now a non-negotiable focal point for internal governance. Practically, this means knowing where data lives, what kind of data the organization holds and where the gaps are.

Achieving that requires a data retrospective: auditing past IT decisions to assess current data readiness. For most enterprises, this includes a hard look at their cloud strategy. Indeed, 75% of leaders said they are increasingly concerned about the geopolitical risks of storing and managing data in global cloud environments. What complicates this further: 70% of CEOs admitted that they arrived at their current cloud environment by organic sprawl, rather than by deliberate design.[3]

While the instinct in a moment like this might be to pull everything as close to home as possible, reactionary data strategies carry their own risks.

When reevaluating data governance frameworks, leaders might consider their internal policies the way they would 'good' and 'bad' regulation.

- Governance should be sufficient without being restrictive: focus on identifying and guarding against risks rather than broad prohibitions.
- It should be targeted: hone in on genuine gaps and high-risk areas rather than attempting to cover everything at once.
- It should be specific to the industry and the company's actual AI use cases: for example, a bank may have specific needs and high-risk use cases that won't apply the same way for a biopharmaceutical research firm, which will have its own risks and protocols.

- And it should be treated as a living framework, subject to continuous review as both the technology and the regulatory landscape evolve: Treat governance tools as needing continuous revision, not as a static document.

Business leaders seeking to assess the effectiveness of their governance strategy might inquire whether data has become more trustworthy, usable and controlled by assessing data quality and usage across the organization. They might look at volume of incidents involving unauthorized access or exposure of sensitive data. They might also examine in which ways high-quality data is not being leveraged, and assess the extent to which their governance practices for AI, privacy, and security are being practiced consistently across their organization.

> While the instinct in a moment like this might be to pull everything as close to home as possible, reactionary data strategies carry their own risks.

Close the gap between access and effective use

The second greatest barrier to scaling AI is workforce enablement.

AI tools are now available at scale across enterprises. Employees are encouraged to use them, experiment with them and find their own footing. But access alone does not guarantee value — and the gap between access and effective use is important for business leaders and senior managers to assess.

Without a deliberate approach to workforce enablement, AI adoption will remain fragmented. Some teams will move quickly, while others will stall. The result is an organization moving at multiple speeds and struggling to generate consistent results.

Enterprise AI's visibility problem compounds this challenge. In the absence of clear guidance and structured enablement, employees have increasingly turned to unsanctioned tools — what is now commonly called 'shadow AI.' [4]

This practice signals genuine enthusiasm from employees to figure out how to make use of AI tools to their advantage, but it also clouds organizational insight into how AI is being used across the enterprise. When employees feed work into AI tools that are not fully integrated into an enterprise environment, with a company's security and privacy practices embedded, it risks sending sensitive data (such as client information, proprietary strategy or financial details) beyond an organization's control.

The answer is not to crack down.
Nor is it general workforce training. Rather, it is role-based enablement.

Effective AI use is fundamentally role-specific. A software developer, a risk analyst, a marketing lead, a customer service representative; each will use AI, even the same tool, in meaningfully different ways. The prompts, the workflows, the judgement about when to rely on AI output and when to override it: these are highly contextual processes and skills.

This is where most organizations remain underinvested: not in acquiring new AI talent, but in helping existing talent integrate AI meaningfully into their day-to-day work. For instance, training a team to effectively utilize intelligent contract management can have real-world payoffs. When teams leverage AI to review and summarize contracts, identify important provisions for certain team members to review, and pinpoint variances with a businesses' standard approaches, it helps reduce a day-long contractual review to a matter of minutes.

Measuring what matters

Measuring a workforce's enablement strategy is critical to understanding if it works or not.

Every organization will need to develop KPIs specific to its own context, but one metric applies broadly: adoption — and not just whether employees are using AI tools, but how deeply they are using them. An organization where only senior leaders are engaging with AI, or where usage is superficial and sporadic, is not realizing the value of its investment. The goal is organization-wide adoption that is embedded in day-to-day workflows, which could be measured by AI usage, workflow integration and, ultimately, business impact.

Adoption metrics alone aren't enough, however. The more powerful signal comes from connecting AI performance metrics to the metrics the business already tracks. The question to ask is not "how is our AI performing?", but "how is AI specifically contributing to the outcomes we already care about — and can we measure that?"

What that looks like in practice will differ by industry. A manufacturer might track whether AI is accelerating design cycles or improving responsiveness to market signals. A financial institution might measure whether loan processing times have improved, whether default rates have shifted or whether credit analysis is producing better outcomes for customers and the business alike. These are not new metrics: they are existing business goals, with AI's contribution made legible and accountable.

The instinct to build an elaborate measurement framework from scratch is understandable, but often counterproductive. A focused set of KPIs that are genuinely tied to the mission and the business will tell leaders more than a sprawling dashboard ever could.

Governance that applies flexible frameworks to manage risk and build trust in AI, paired with developing workforce skills aligned to business outcomes, will help organizations stay competitive and agile in a rapidly evolving regulatory, technological and geopolitical landscape.

References

1 A 'Kill Switch' Could Shutter Europe's Access to US Tech. Here's How. Tech Policy. Aug 2025.

2 MEPs support postponement of certain rules on artificial intelligence. European Parliament. March 2026.

3 Kyndryl Readiness Report. Kyndryl. 2025.

4 Shadow AI Has Already Moved Into Your Organization. Forbes. March 2026.