Scaling AI Securely

The leadership playbook for turning AI investment into enterprise value

A Global Leader in Technology Services

Experis®
ManpowerGroup



©Experis 2026 Scaling AI Securely

Table of contents

1 Introduction 3-4

Executive summary..... 3
Foreword: Innovation at a crossroads 4

2 Scaling AI business transformation 5-9

The illusion of plug-and-play AI 5-7
The new enterprise attack surface..... 7
Governance becomes competitive advantage..... 8-9

3 Creating competitive differentiation ... 10-13

Redesigning organizations for the agent era.....10-12
The human layer of AI transformation 11-12

4 Tech leader executive playbook 13-15

Five actions tech leaders should take now..... 13-14
Experis global expertise 15

Introduction



Executive summary

AI investment is accelerating, but many organizations are still struggling to turn experimentation into measurable business value: The gap is not simply technological. It is rooted in business alignment, data readiness, cybersecurity, governance, workforce capability, and the ability to integrate AI into how work actually gets done.

The idea of "plug-and-play" AI business transformation is a myth: Projects that perform well in pilot environments often stall when they encounter legacy systems, fragmented data, unclear ownership, security requirements, and real-world workflows. Technology alone cannot overcome these barriers.

As AI moves deeper into the enterprise, every new model, agent, dataset, and integration creates both opportunity and risk. Organizations must secure a growing attack surface, establish clear accountability, redesign workflows, and build the skills required for people to use and oversee AI effectively. Without these foundations, promising pilots struggle to scale and investments fail to deliver their full return.

The next phase of AI adoption requires a shift in focus. The question is no longer whether organizations should invest in AI. It is how leaders can scale AI securely, responsibly, and effectively. Experis research underscores the challenge. While 66% of IT professionals say their organizations are increasing AI investment, only 9% say AI is fully integrated into operations and strategy.[1]

Foreword: Innovation at a crossroads

In our recent conversations with clients, it has become clear AI has moved beyond experimentation. Across industries, organizations are investing heavily in AI, automation, cloud infrastructure, and increasingly autonomous systems. **For many executive teams, the question is no longer whether to invest, but how to turn that investment into results.**

That is where ambition often runs ahead of execution. Models and tools are improving quickly, but enterprise deployment remains difficult. Business outcomes are uneven, while security, governance, and workforce readiness often lag behind the technology.

A successful pilot is not the same as a scalable solution. In day-to-day operations, AI must work with inconsistent data, legacy systems, governance requirements, uneven adoption, and a fast-changing threat landscape. **The biggest barriers increasingly come from the systems around the technology, not the technology itself.**

This challenge will grow as AI becomes more autonomous. Systems will not only generate content or answer questions, but they will also make decisions, coordinate tasks, interact with business systems, and take actions once handled by people. Leaders need stronger oversight, clearer accountability, and a workforce equipped to use these tools responsibly.

Organizations that are making progress treat AI as an enterprise transformation, not another technology rollout. They tie initiatives to business priorities, build governance early, make security part of operational resilience, redesign workflows instead of automating broken ones, and invest in people alongside technology.

This report explores how organizations can navigate the next phase of AI transformation. Drawing on research from technology leaders around the world, as well as broader market insights on AI adoption, cybersecurity, governance, and organizational change, we examine the leadership decisions that will determine whether AI investments become sustainable competitive advantages or expensive experiments.

The future of AI will not belong to the organizations with the most advanced models. It will belong to the organizations that can integrate those models into the flow of work, govern them responsibly, secure them effectively, and enable people to use them confidently.



Kye Mitchell

Kye Mitchell
Experis US Brand Leader



James Hallahan

James Hallahan
Experis Europe Brand Leader

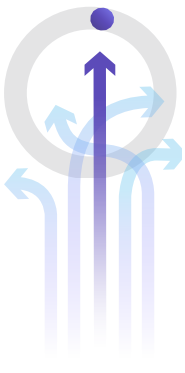
Scaling AI business transformation



The illusion of plug-and-play AI

AI tools can create impressive results in a controlled environment, but enterprise operations are less forgiving. **A production system must work with real data, existing applications, established controls, uneven user behavior, and business processes that were rarely designed with AI in mind. The difficulty is not proving that a model can perform a task. It is building the surrounding system that allows the model to perform reliably, repeatedly, and at an acceptable level of risk.**

That distinction helps explain the widening gap between AI activity and AI value. A recent global study found that only 5% of companies were generating AI value at scale. Another 35% were scaling and beginning to generate value, while 60% reported little material value despite substantial investment.[2] The leading group did not simply automate more tasks. It built the strategy, operating model, talent, technology, and data capabilities required to reshape core work.



Only 5% of companies were generating AI value at scale.

A CIO view of the current state of global AI implementation[1]

Implementation
We are actively integrating AI into some areas
32%

Exploration
We are researching and running pilot projects
30%

Scaling
AI is being scaled across the organization
19%

Not started
We have not yet begun exploring AI integration
10%

Fully Integrated
AI is embedded into our operations and strategy
9%

Our own research shows the same tension from the perspective of technology leaders. Most C-suite tech leaders say their companies are increasing AI investment, and 60% say their organizations are implementing AI in at least some areas. Yet only 9% say AI is fully integrated into operations and strategy.[1] More than half report a positive return from AI investment, but the unevenness across company sizes, sectors, and markets suggests that early returns do not always equal enterprise scale.

Start with the business, not the model

A technically viable use case can still be a weak business investment. Leaders need to know which workflow will change, who owns the outcome, what risk the organization is accepting, and how value will be measured. Without those decisions, pilots tend to accumulate around local enthusiasm rather than enterprise priorities.

The need for stronger alignment is clear. **Nearly half of technology leaders, 48%, now rank aligning IT strategy with business objectives among the most important responsibilities of the CIO, up from 34% in 2025.** Even so, reported alignment between business and technology strategy remained statistically unchanged at 77%, compared with 80% the previous year. Meanwhile, 44% cite keeping up with rapid technological change as a top barrier, and 61% of CIOs say senior leaders do not know enough about the role and what it requires.[1]

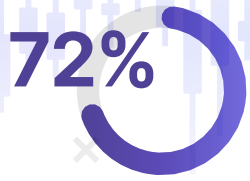
2026 global CIO priorities[1]

1. Align IT with business strategy
2. Enhance cybersecurity
3. Digital transformation
4. Cost savings
5. Tech talent
6. Regulatory compliance

These findings point to a leadership issue. **AI cannot be owned by IT alone when its impact extends into operations, finance, risk, legal, customer experience, and the workforce. Business leaders must co-own the choice of problems, the redesign of workflows, and the measurement of results.** Technology leaders must translate technical possibilities into decisions the rest of the enterprise can act on.

Modernize the foundations for scale

Data and architecture also determine whether promising use cases survive production. IBM's 2025 CEO study found that 68% of surveyed CEOs viewed integrated enterprise-wide data architecture as critical for cross-functional collaboration, while 72% viewed proprietary data as central to unlocking generative AI value.3 At the same time, half said rapid investment had left their organizations with disconnected, piecemeal technology. Only 16% of AI initiatives had scaled enterprise-wide.



of CEOs say proprietary data is the key to unlocking generative AI value.[3]

For leaders, this makes modernization part of the AI strategy rather than a separate infrastructure program. The practical questions include whether data can be accessed with the right permissions, whether models can connect safely to core systems, whether outputs can be monitored, and whether the organization can change or remove a platform without disrupting critical work.

The new enterprise attack surface

As AI moves into core operations, cybersecurity expands beyond networks, devices, and applications. **Organizations must also protect models, training and retrieval data, prompts, agent identities, automated actions, integrations, and the cloud environments connecting them. A weakness in any one layer can affect the reliability of the entire workflow.**

This is why cybersecurity must be treated as a condition for AI growth. In our own research, 78% of senior tech leaders said their organizations are increasing cybersecurity investment. Cybersecurity is also the most important technology skill, cited by 46%, ahead of AI and machine learning at 37% and cloud computing at 31%. Yet readiness is not advancing at the same pace. Only 72% say their risk strategy is aligned with cybersecurity readiness, down from 77% in 2025. The same proportion regularly conduct cybersecurity training, little changed from 74% the previous year.[1]

A renewed CIO focus on cybersecurity



78% are increasing their cybersecurity budget



Cybersecurity is the #1 in-demand skill for tech talent



Cybersecurity remains the top worry keeping CIOs awake at night

Agents raise the stakes

The shift toward agentic AI adds a new category of exposure because agents can move across systems and take action. **The key risk is no longer limited to whether an answer is inaccurate. Leaders must ask what the system is permitted to do, which data it can access, how its identity is managed, and what happens when an action is unexpected.**

Access controls therefore need to reflect the task, not simply the user or application. Agents should not inherit broad permissions because implementation is easier that way. Organizations also need traceability across prompts, data sources, decisions, actions, and exceptions so security teams can understand what happened and intervene when necessary.

AI is both a security tool and a security challenge

Security teams are also using AI to increase the speed and efficiency of defense. **Recent research found that 91% of respondents were using or experimenting with AI-powered cybersecurity solutions, and 84% said AI-enhanced security tools were helping teams become more effective and efficient.** At the same time, 86% reported at least one breach in the previous 12 months, and 56% cited a lack of cybersecurity skills as a top cause of security breaches.[4]



56%

of tech leaders say cybersecurity skills gaps are the leading cause of security breaches.[4]

The lesson is not to slow AI adoption, but tech leaders must connect it to secure engineering from the beginning. **Security leaders should be involved when use cases are selected, data paths are designed, vendors are evaluated, and workflows are changed.** Controls added after deployment are more likely to create delays, workarounds, and distrust.

Make security a shared operating discipline

Secure AI is not solely the responsibility of the Chief Information Security Officer (CISO). Business owners must define acceptable outcomes and exceptions. Technology teams must build and maintain the architecture. Legal and risk teams must translate obligations into usable controls. Workforce leaders must support training and adoption. Employees must understand when and how to question, escalate, or override AI-supported decisions.

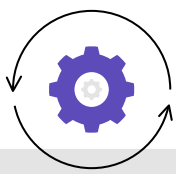
Governance becomes competitive advantage

Governance is often described as a constraint on innovation. In practice, weak governance creates uncertainty, delays, duplicated review, and inconsistent decisions. **Strong governance gives teams a repeatable path from idea to production. It clarifies which risks require escalation, who has authority to approve or stop a deployment, and how systems will be monitored after launch.**

Recent enterprise research found that regulation and risk had become the leading barrier to generative AI development and deployment. Most surveyed companies expected fewer than 30% of their experiments to reach full scale within six months, while 69% expected it would take at least a year to implement a comprehensive governance strategy.[5]

Effective governance is the greatest hurdle

50% of c-suite executives say translating responsible AI principles into operational processes is their greatest barrier to progress.[5]





Another recent responsible AI survey connected governance directly to value. Fifty-eight percent of executives said responsible AI initiatives improve ROI and organizational efficiency, 55% reported benefits for customer experience and innovation, and 51% cited stronger cybersecurity and data protection. The challenge was operationalization, with 50% identifying the move from principles to scalable processes as their biggest hurdle.[5]

Governance must keep moving after launch

Traditional controls often emphasize approval before deployment. AI requires equal attention after deployment because models, data, users, and operating conditions change. Governance should include ongoing monitoring, feedback loops, incident response, documentation, periodic review, and clear standards for modification or retirement.

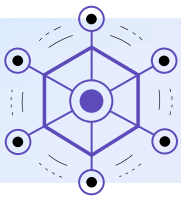
Agentic systems make this especially important. The more autonomy a system has, the more precisely leaders must define its scope, escalation points, and human oversight. **Governance should answer who owns the outcome, who can inspect the system, who can pause it, and what evidence is required before the system can resume operation.**

Growing sovereignty tension

Data sovereignty adds another layer of complexity. **Most technology leaders (81%) describe digital sovereignty as a high or critical priority. At the same time, 67% expect their organizations to increase investment in offshore and nearshore IT delivery.**[1] The tension is understandable when business leaders want greater control over data and infrastructure while also drawing on global technology, skills, and delivery capacity.

The answer is not complete technological independence. It is clarity about what must remain under direct control, what can be entrusted to partners, where data may be stored or processed, and how the organization can maintain continuity if a provider, platform, regulation, or geopolitical condition changes.

Sovereignty surges



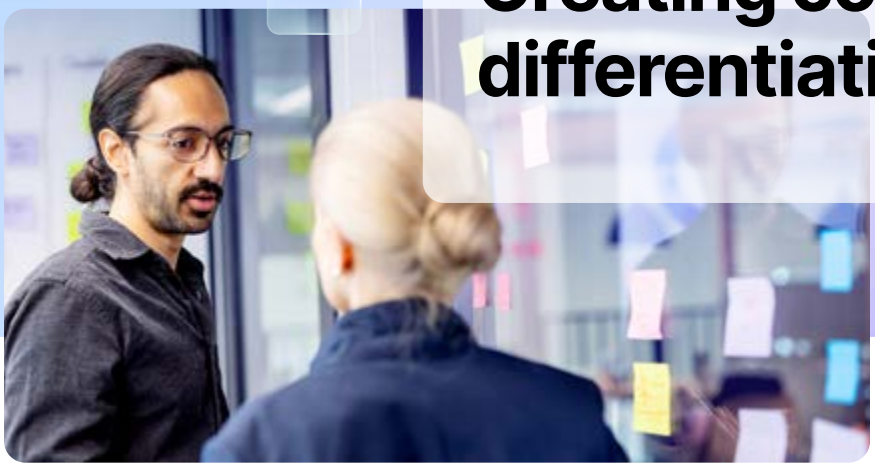
81% of CIOs and senior tech leaders say digital sovereignty is a high or critical priority.[1]

Treat regulation as a design requirement

The European Union AI Act illustrates why governance must be designed into operations. The regulation follows a risk-based approach and includes specific requirements affecting workplace and employment-related AI. Its penalty framework reaches up to €35 million or 7% of worldwide annual turnover for the most serious infringements, with additional tiers for other obligations and inaccurate information.[6]

For multinational organizations, compliance cannot be reduced to a one-time legal review. Teams need a practical way to connect local obligations with system inventories, risk classifications, data practices, human oversight, documentation, and vendor management.

Creating competitive differentiation



Redesigning organizations for the agent era

AI can accelerate work, but speed does not improve a process that is fragmented, duplicated, or poorly owned. Organizations that place agents on top of existing inefficiencies may create faster confusion. The first step is to understand how work currently moves across functions, systems, and decision points.

There is more recent research showing why workflow redesign matters. **Future-built companies move beyond isolated automation and reshape core functions. They pursue multiyear AI ambitions, adopt AI-first operating models, secure the necessary talent, and use fit-for-purpose technology and data.** One study estimates that 70% of potential AI value is concentrated in core business functions rather than support activity.[2]

70% of potential AI value is concentrated in core business functions rather than support activity.



Move from task automation to orchestration

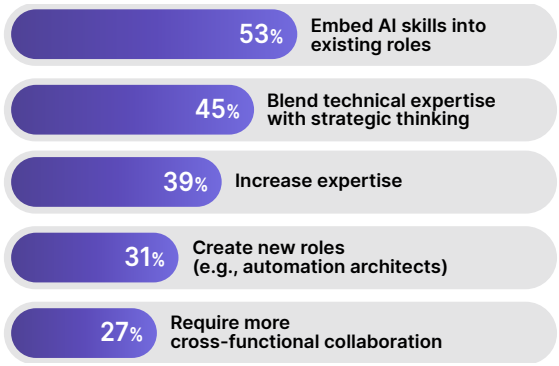
Agentic AI shifts the conversation from automating individual tasks to coordinating work across people and digital systems. That requires an orchestration layer that can make work visible, route it appropriately, apply controls, and measure results. It also requires explicit human ownership.

Leaders should define which decisions remain human-led, which are AI-assisted, and which may be executed by an agent within established limits. They should also determine how exceptions return to people, how performance is evaluated, and how lessons from real use improve the workflow over time.

Redesign roles with the workflow

Operating-model change is already reshaping technology work. Our research finds that 53% of organizations are embedding AI skills into existing roles, 45% are blending technical expertise with strategic thinking, and 39% are increasing role versatility across multiple areas. Nearly one-third are creating new roles such as data ethicists and automation architects. Far fewer report eliminating roles to reallocate headcount or reduce cost.[1]

Top CIO approaches for AI-augmented tech talent[1]



This pattern suggests that AI scale depends less on removing people than on redefining responsibilities. Workers need clarity about how AI changes decisions, handoffs, accountability, and service expectations. Managers need to know how to assess performance when results are produced by a combination of people and systems.

Top skills CIOs want[1]

1. Cybersecurity
2. AI & machine learning
3. Cloud computing
4. Software development
5. Collaboration & teamwork

The human layer of AI transformation

The talent question is broader than whether an organization can recruit enough AI specialists. Secure scale requires a connected portfolio of technical, governance, leadership, and workforce capabilities. Those capabilities must be available where decisions are made, not isolated in a small center of excellence.

Our recent CIO research illustrates the broad range of skills IT teams around the world need. **Cybersecurity is the most cited technology skill at 46%, followed by AI and machine learning at 37% and cloud computing at 31%.** Collaboration, software development, DevOps, adaptability, problem-solving, communication, and leadership also appear among the priorities. This mix reflects the reality that enterprise AI is both a technical system and a business change program.

Build four dimensions of capability

1

Technical capability:

AI, data, cloud, cybersecurity, software engineering, architecture, testing, and platform integration.

2

Governance capability:

Risk classification, policy, monitoring, compliance, audit, vendor evaluation, and responsible AI.

3

Leadership capability:

Business alignment, investment decisions, accountability, communication, and change leadership.

4

Workforce capability:

AI literacy, adoption, trust, collaboration, continuous learning, and human oversight.

Close the adoption gap

A system can be technically deployed without being meaningfully adopted. Experis found that alignment between new technology implementation and worker adoption fell in 2026. **When teams do not understand how a tool fits their work, what they remain accountable for, or when they should challenge its output, adoption becomes inconsistent and risk increases.**

Training should therefore move beyond feature demonstrations. Employees need practice applying AI within real workflows, evaluating outputs, recognizing limitations, protecting data, and escalating concerns. Managers need support redesigning roles and measures. Leaders need a shared language for value, risk, and human oversight.

Develop leaders as deliberately as specialists

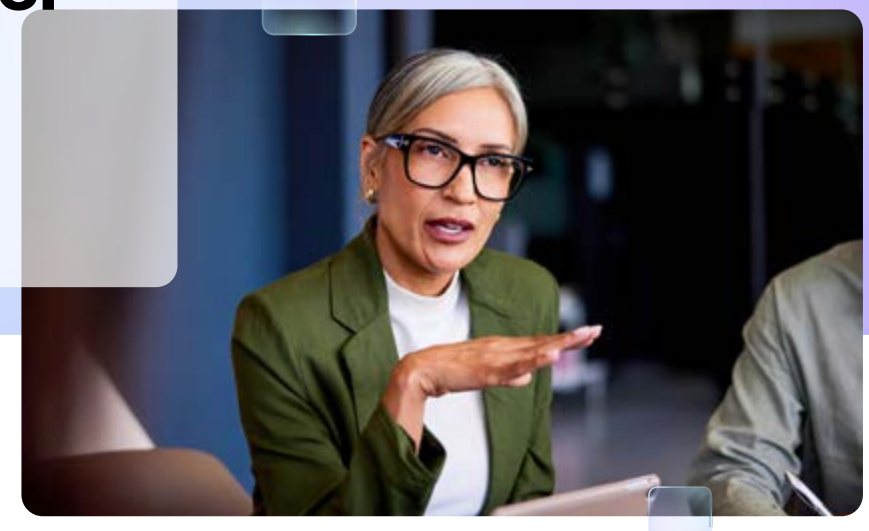
The leadership pipeline deserves equal attention. Only 58% of organizations in the Experis study regularly conduct programs to develop future technology leaders, which was down from 63% in 2025.[1] That decline comes as leadership roles require a more complex combination of technical judgment, business understanding, communication, governance, and change capability.



Only 58% of organizations regularly develop future technology leaders, down from 63% in 2025.

Organizations should combine internal development, targeted recruitment, specialist partners, and flexible delivery models. **The objective is not to fill every capability with a permanent role. It is to ensure the enterprise can access the right expertise, maintain accountability, and transfer knowledge as technology and risk evolve.**

Tech leader executive playbook



Five actions tech leaders should take now

The path from AI experimentation to enterprise value requires focused action. **These five priorities give technology leaders a practical roadmap to align investment with business outcomes, strengthen security and governance, redesign work for AI, and build the capabilities needed to scale with confidence.**

Together, these actions create an enterprise system for secure AI scale. They connect investment to outcomes, innovation to control, automation to accountability, and technology to the people who make it valuable.

1. Align AI investment with business outcomes

2. Treat cybersecurity as a business critical priority

3. Build governance before scale

4. Redesign workflows before deploying agents

5. Invest in capability, not just technology

"Saying that we're going faster or that it's better quality isn't ROI. If we save time thanks to AI, the real question is: what are we going to do with that time? The value of a project must be measured in terms of revenue or profitability." *– CIO, luxury goods sector, France*



1. Align AI investment with business outcomes:

Require every material initiative to identify the business owner, workflow, outcome, adoption measure, risk owner, and value metric before it moves toward scale.

What business outcome will change?

Who owns the result after deployment?

What evidence will justify continued investment?



2. Treat cybersecurity as a business-critical priority:

Extend security design across models, data, agents, identities, integrations, vendors, and automated actions.

What can the system access and do?

How will unexpected behavior be detected?

Who has authority to intervene?



3. Build governance before scale:

Create a repeatable path for classification, approval, monitoring, escalation, and retirement.

Which decisions require human review?

What documentation and testing are required?

How will controls adapt after launch?



4. Redesign workflows before deploying agents:

Map end-to-end work and remove fragmentation before adding autonomy.

Where does work break today?

Which activities should be human-led, AI-assisted, or agent-executed?

How will exceptions return to people?



5. Invest in capability, not just technology

Build a portfolio of technical, governance, leadership, and workforce capabilities using internal development and external expertise.

Which capabilities are strategic to own?

Where can partners accelerate progress?

How will knowledge transfer and continuous learning occur?

Experis global expertise

As AI reshapes the cybersecurity landscape, organizations face a dual challenge: harnessing the power of emerging technologies while managing an increasingly complex risk environment. From securing AI-enabled systems and protecting critical data assets to modernizing infrastructure and strengthening governance, success requires more than technology investments alone. It requires the right combination of strategy, specialized expertise, and execution. That's where Experis helps organizations move from experimentation to impact.



AI & data expertise

Transform data into actionable intelligence with services spanning data modernization, AI modeling, automation, advanced analytics, and governance. Organizations gain greater visibility, stronger decision-making, and more responsible AI adoption.



DevSecOps & secure engineering

Embed security throughout the technology lifecycle by integrating development, operations, and security practices. This helps accelerate innovation while reducing risk and improving resilience.



Cloud & application modernization

Modernize legacy systems, migrate to cloud environments, and build scalable architectures designed to support emerging AI and cybersecurity requirements. Organizations benefit from greater agility and a technology foundation built for future growth.



Governance, quality & compliance

Strengthen trust in digital initiatives through quality engineering, automated testing, performance validation, and security testing. The result is improved reliability, reduced operational risk, and greater confidence in technology investments.



Accelerated time-to-value

Leverage proven methodologies, specialized expertise, and agile delivery models to move from strategy to measurable outcomes faster. Experis emphasizes faster results and tangible business impact.

[1] Experis 2026 CIO Outlook [2] BCG [3] IBM Institute for Business Value [4] Fortinet [5] Deloitte [6] European Union

Stay connected

Experis global resources for tech leaders

Access specialized technology talent and services backed by a global network supporting clients across industries and markets. Deep domain expertise helps organizations navigate complex transformation challenges with confidence.

The path from AI experimentation to measurable business impact requires more than new tools. It requires the right combination of technology expertise, workforce strategy, and execution support. As a global leader in technology services, Experis® helps organizations turn technology potential into business impact through AI, data, cloud, application modernization, quality engineering, and specialized talent solutions.

To learn more, visit *experis.de*, or follow us on *LinkedIn*.

Research methodology

Experis commissioned a survey of 1,930 senior tech leaders across 12 countries from January 28 – March 4, 2026. Respondents included CIOs, CTOs, CISOs, and other senior tech leaders with decision-making authority over IT budgets and hiring. In addition, in-depth qualitative interviews were completed in each market.

Contact us:

Email: experis.sales@de.experis.com
Phone: +49 (0) 69 153030

Manpower® Experis® ManpowerGroup Talent Solutions® ManpowerGroup® | ManpowerGroup®