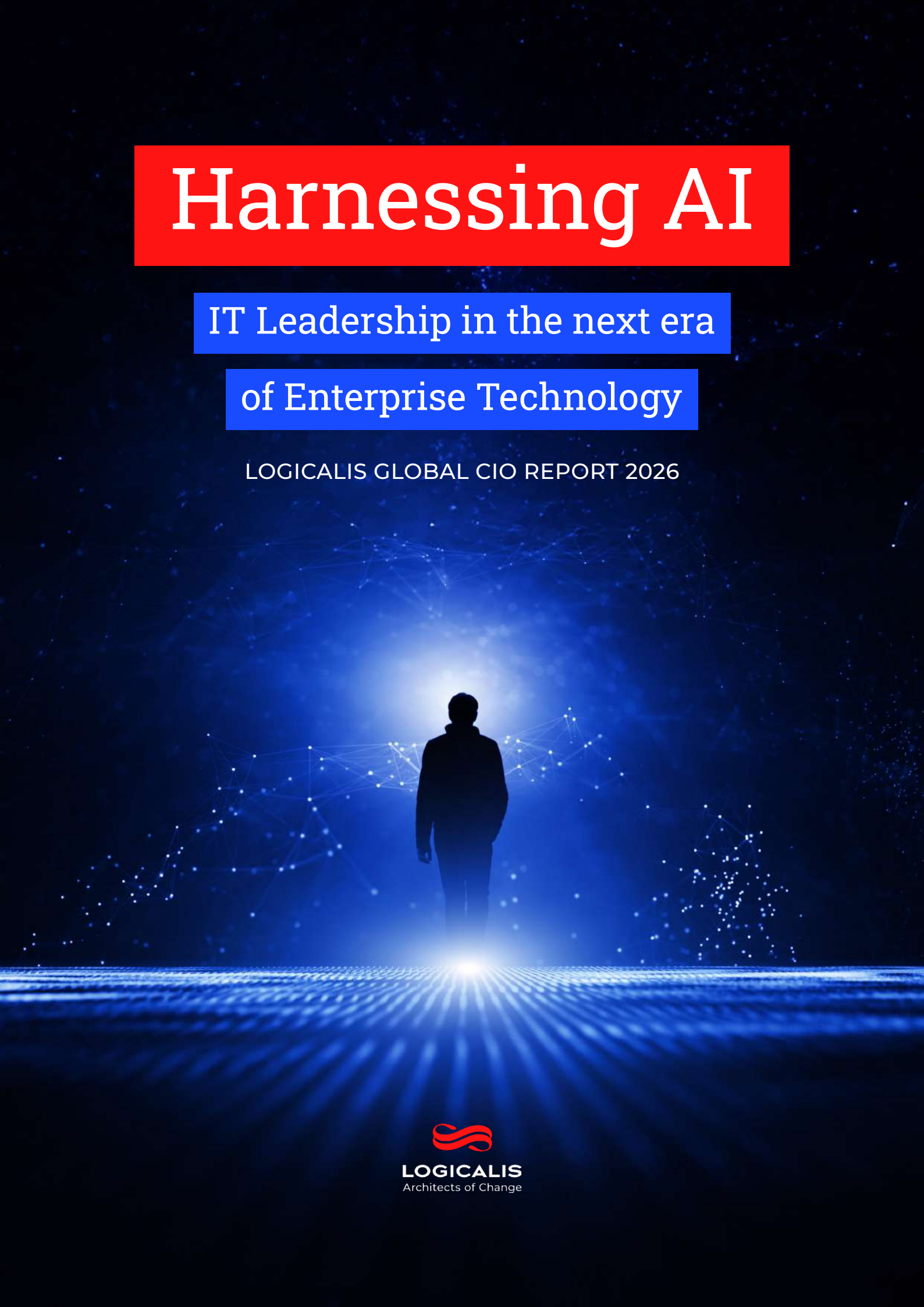
Harnessing AI

IT Leadership in the next era of Enterprise Technology

LOGICALIS GLOBAL CIO REPORT 2026



LOGICALIS
Architects of Change

Contents

Foreword

Bob Bailkoski
CEO Logicalis Group

The Logicalis CIO Report has always captured the defining currents shaping the technology landscape. But this year marks a profound inflection point. After more than a decade of steady transformation, we are entering an era where AI is not simply enhancing enterprise IT, it is reshaping the very foundations on which organisations operate and compete. The scale of change is unprecedented, and so is the opportunity.

Our research shows a striking surge in ambition. Organisations everywhere are accelerating their AI investment, recognising its potential to unlock new value, new models and new forms of intelligence across the enterprise. Yet ambition alone is no longer enough. CIOs are being asked to build the future while simultaneously safeguarding it. They are navigating a world where speed and stewardship must coexist, where innovation must advance in step with trust, governance and responsibility.

We have been here before, but never at this magnitude. A decade ago, in our 2015 survey, the rise of Shadow IT revealed how technology could outpace structures designed to contain it. Today, AI is moving even faster, permeating every corner of the organisation and redefining what leadership must look like. The stakes are higher because the systems themselves are becoming more autonomous, more powerful, and more consequential.

What emerges clearly is a new model of leadership. Few CIOs expect to carry this transformation alone. Instead, they are building ecosystems, networks of partners, specialists and trusted advisors who can amplify capability, accelerate progress and reinforce resilience. The fact that 94% of organisations plan to rely on Managed Service Providers over the next two to three years underscores a fundamental truth: leadership in the AI era is no longer about ownership but about orchestration.

This report offers a view into how CIOs are shaping this new frontier: setting vision, governing risk, building enterprise intelligence, and architecting a future powered by autonomous systems. Above all, it reflects an unmistakable shift. We are leading in an age of acceleration, and the organisations that thrive will be those whose leaders can unlock AI's full potential while ensuring it remains responsible, trusted and profoundly transformative.

Executive Summary

This year's CIO Report captures a moment of transition for enterprise technology leadership. AI is no longer emerging at the edges of the organisation, it is becoming central to how work is done, how decisions are made and how value is created. For CIOs, this marks a shift in responsibility that is both practical and structural. The question is no longer how to introduce AI, but how to manage it, scale it, and reduce as much organisational risk as humanly possible.

The research shows overwhelming appetite for AI, alongside growing awareness of the pressures it creates. CIOs are navigating a landscape defined by acceleration, fragmentation and rising expectations. They are being asked to move faster, deliver more value, and assume greater responsibility, often before the organisational foundation needed to support that responsibility is fully in place.

Setting the AI Agenda

Almost every organisation reports growing enthusiasm for AI, yet many CIOs believe adoption is already moving too fast. Strategic alignment remains fragile, long-term roadmaps are still forming, and confidence in governance frameworks is uneven. The result is a leadership challenge rather than a technical one. CIOs are being asked to regulate pace, define priorities and preserve coherence at a time when momentum is pushing relentlessly forward.

From Confidence to Capability

CIOs are confident in their relative AI maturity compared to peers, and initial experimentation is already delivering value in targeted areas. But scaling that value remains difficult. Skills shortages, data quality issues, infrastructure constraints and organisational resistance continue to hold progress back. This chapter shows that AI maturity is not about tools alone. It is about building repeatable, dependable capability that can survive audit, scrutiny and long-term operational demands.

Managing Security in the AI Era

As the threat landscape continues to grow, CIOs continue to grapple with known threats, while simultaneously preparing for unknown ones. AI is changing the nature of risk, introducing new vulnerabilities that are harder to detect, harder to trace and harder to own. Governance frameworks exist, but confidence in their effectiveness is limited. Visibility of AI use is incomplete

and accountability is fragmented. CIOs are increasingly becoming the custodians of trust in systems that act with growing independence, even when authority is distributed across the organisation.

The Next Frontier

Investment in agentic AI signals a move from augmentation to autonomy. Workforce models are becoming more fluid. Managed service providers are becoming more central. Technology is no longer a set of projects to be delivered, but a permanent condition to be designed around. CIOs are evolving into architects of environments where humans, machines and external partners must coexist without eroding responsibility or control.

Technology leadership is no longer defined by ownership of systems, but by stewardship of consequence as CIOs are being asked to balance speed with stability, ambition with restraint, and innovation with responsibility.

CHAPTER 1

Setting the AI Agenda

Artificial intelligence is advancing at a pace unlike previous waves of enterprise technology. What began as experimentation has become expectation. Boards are no longer debating whether AI belongs in the organisation, but how quickly it can be embedded, and what competitive advantages can be realised. For CIOs, that shift has moved the centre of gravity of their role. The challenge is no longer to introduce a new capability, but to hold the line between momentum and manageability.

The appetite for AI adoption has accelerated sharply over the past year with almost all (94%) reporting an increase. Innovation demands remain the strongest driver, cited by 48% of CIOs, but pressures around risk management and compliance are now almost as influential, being cited as a 'primary driver' in shaping adoption decisions for 38% of respondents. Early proof-of-concept success has also acted as a catalyst, with 37% accelerating AI initiatives based on initial results.

This combination of ambition and urgency places CIOs at the centre of a new balancing act. They are expected to move quickly enough to sustain competitive momentum, while ensuring that governance, resilience, and commercial discipline are not left behind. The AI agenda is no longer about identifying opportunities alone, but about regulating speed in an environment where technology is advancing faster than organisational structures can comfortably absorb.

94% of organisations say their appetite for AI has increased in the last 12 months

Yet **51%** believe AI adoption is already moving too fast

Yet strategic clarity has not kept pace with enthusiasm. Fewer than half of organisations (46%) say their AI strategy is fully aligned with their wider business plan or key performance indicators. In practice, this means CIOs are often operating in a grey zone where AI initiatives move forward without a fully mature framework for measuring value, prioritising investment or defining success.

This misalignment creates exposure. When AI activity advances ahead of business governance, the CIO inherits responsibility for reconciling ambition with accountability. The risk is not that organisations invest in AI, but that they do so without a clear line of sight between experimentation, enterprise value and long-term operating models.

Responsibility for AI decisions is increasingly concentrated within the technology function. When it comes to implementation, 59% of our respondents say they are the final decision maker. This reflects the expanding scope of the role: CIOs are being asked to take responsibility not only for delivery but also for the strategic integrity of AI across the organisation.

However, confidence in the structures that support these decisions remains uneven. Only around one in three CIOs (36%) are extremely confident that they have comprehensive guidance and best practices in place to lead AI initiatives effectively. CIOs are being positioned as the ultimate authority on AI deployment while simultaneously acknowledging that the governance models required to support that authority are still maturing.

Concerns about pace underline this tension. Just over half of respondents (51%) believe AI implementation within their organisation is moving too fast. This is not a signal of resistance or scepticism, but reflects an awareness that momentum is beginning to outstrip infrastructure.

More than half of CIOs (55%) lack strong confidence that their organisation has a coherent AI roadmap for the next two to three years, and 58% say business units and central IT leadership are not fully aligned on AI priorities and direction. For CIOs, this is a leadership challenge rather than a technical one. Unclear

priorities and lack of alignment make it harder to establish enterprise standards, govern risk consistently and scale successful initiatives beyond isolated teams. Without stronger alignment, AI adoption risks becoming uneven, reactive and increasingly difficult to control.

Environmental considerations add a further dimension to this responsibility. As AI usage expands, its energy demands and environmental footprint are becoming harder to ignore. Yet only 39% of CIOs are extremely confident that their organisation actively measures and manages the environmental impact of its AI initiatives, and just 41% say energy efficiency is prioritised in AI deployment. This marks a significant shift in the scope of AI leadership. CIOs are no longer just responsible for the financial and security costs of AI but are increasingly responsible for its sustainability implications. As regulatory expectations and board scrutiny grow, environmental accountability will become part of what it means to lead responsible enterprise AI.

Taken together, these findings point to a redefinition of the CIO's role. Leadership in an AI era is becoming less about how fast organisations can move, and more about how deliberately they can move. The ability to slow certain decisions down to speed sustainable progress up is rapidly becoming one of the defining capabilities of the modern CIO.

CHAPTER 2

From Confidence to Capability

There is a strong sense of confidence in how CIOs view their organisation's position on AI. Compared to peers, many believe they are already ahead across generative, predictive and agentic capabilities, and that perception matters. It signals momentum, investment and seriousness of intent. But being further ahead than others does not necessarily mean being ready to operate AI at enterprise scale.

That distinction becomes clear when CIOs move from comparison to capability. AI is already delivering value in specific areas, particularly where data, ownership and processes are relatively well established. The strongest impact is being seen in predictive analytics and forecasting (56%), followed by improvements to customer experience and service delivery (both 45%), and in supporting innovation and idea generation (43%). These are meaningful gains, and they show that AI is firmly out of the experimental phase.

What they don't yet show is consistency. These successes tend to sit within defined functions or motivated teams, rather than forming part of a repeatable enterprise model. AI is working, but it is not yet embedded.

This is where confidence begins to soften. When CIOs consider their ability to move from early success to organisation-wide impact, almost two-thirds are not strongly confident they can scale AI beyond pilots and proof-of-concepts (65%). A similar proportion are not strongly confident that AI investments have yet delivered measurable business value (62%). This figure has barely changed since 2025, suggesting that a year on, not enough progress has been made in turning AI investment into business returns.

These figures point to a familiar pattern. AI has proven its potential, but it has not

yet proven its reliability. For CIOs, this is the moment where leadership shifts from encouraging experimentation to building a dependable business capability.

Part of the challenge lies in how AI has grown. Most organisations describe their approach as “learning as we go” (89%). That mindset has fuelled rapid progress, lowered barriers to entry and encouraged innovation. But it also means that many AI initiatives have developed without stable operating models behind them. What works in a learning environment does not always survive the demands of scale, auditability or regulatory scrutiny.

The barriers CIOs identify reinforce this. The most frequently cited constraint is not funding, but skills. A lack of internal technical capability is holding back AI ambitions in almost nine out of ten organisations (88%). Data challenges follow closely (87%), alongside

The biggest barriers to scaling AI

- Lack of internal technical skills - **88%**
- Regulatory and compliance concerns - **88%**
- Data challenges - **87%**

infrastructure limitations (84%). These are not minor operational issues, they shape whether AI can ever scale.

Without sufficient skills, AI remains dependent on a small number of specialists. Without robust data foundations, outputs remain difficult to trust. Without scalable infrastructure, success remains localised. Together, these weaknesses prevent AI from becoming an organisational foundation rather than a series of projects.

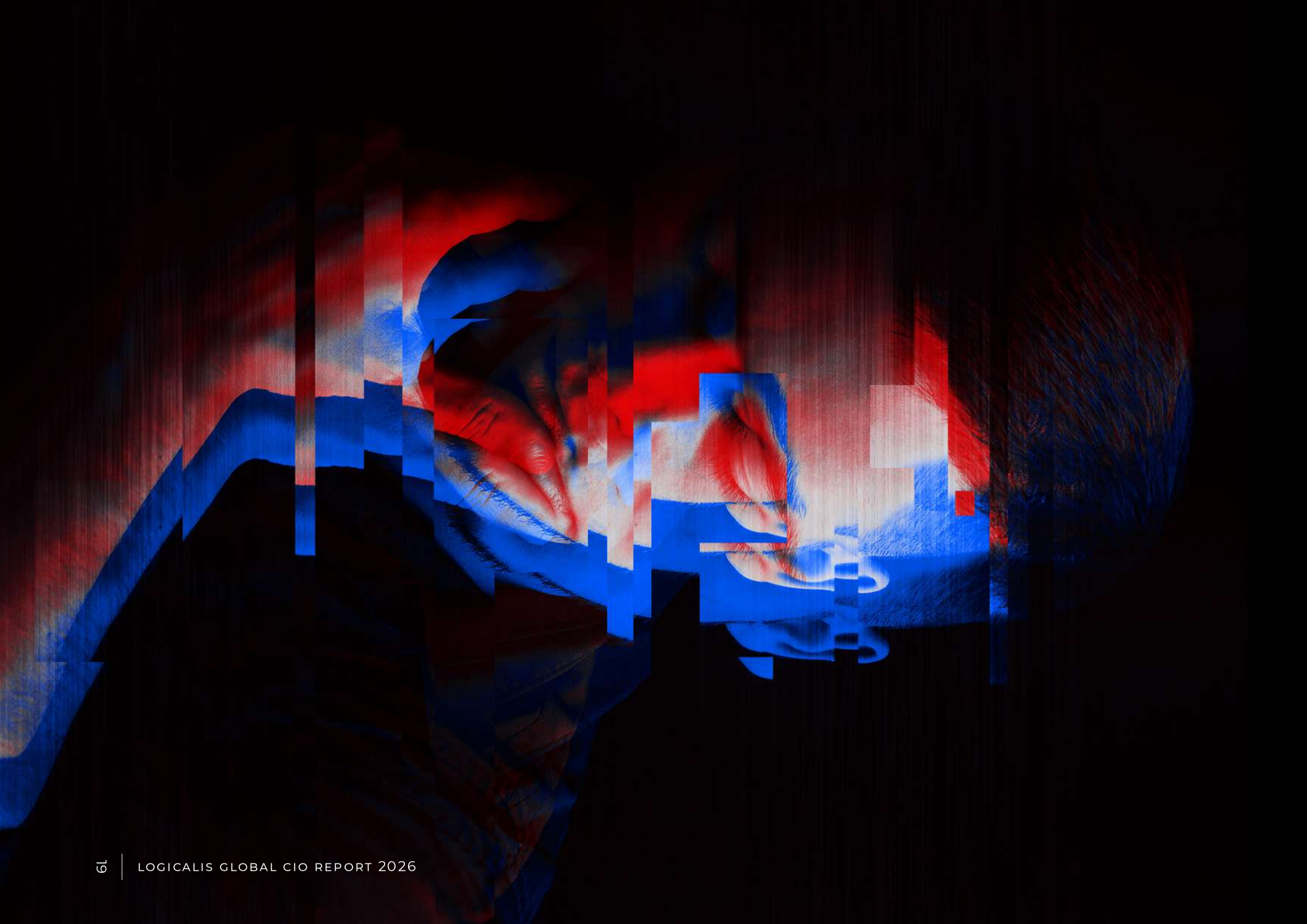
What the research suggests is that AI maturity is less about technology and more about organisational design. Scaling AI requires the same things that scale any enterprise capability: standardisation, governance, accountability and measurement. It requires clarity about who owns systems once they move into production, how performance is monitored, and how risk is absorbed.

This is why the gap between confidence and capability matters. Confidence reflects optimism and momentum. Capability reflects discipline and readiness.

For CIOs, the challenge is to turn early success into something more durable. The real work now is not proving what AI can do but making it reliable enough to be scaled with confidence to deliver a net business benefit.

CHAPTER 3

Managing Security in the AI Era



Cybersecurity was already operating under sustained pressure long before AI entered the mainstream. Spending has increased, tooling has multiplied, and threat volumes have continued to rise. Yet confidence has not grown at the same pace.

Last year's report highlighted the 'security spending black hole' paradox of rising investment alongside persistent incidents. That tension has not disappeared. The majority of organisations still report experiencing a cybersecurity incident in the past 12 months (77%), and while that number peaked at 88% in 2025, the challenge is far from under control. Malware and ransomware remain the dominant threats (33%), closely followed by phishing (30%). The baseline risk environment remains unpredictable, resource-hungry and structurally demanding.

What has changed is the nature of the threat landscape itself. AI is no longer just a tool that security teams deploy to improve detection or automate response. It has become part of the attack surface. More than a quarter of CIOs now rank AI itself as a significant source of risk (28%), placing it on par with the more established modes of cyber-attack.

Security teams are no longer protecting only systems and data. They are increasingly being asked to govern behaviour, automation and decision-making processes that operate with a degree of autonomy.

At the same time, the foundations of security capability remain under strain. CIOs continue to point to shortages in specialist cybersecurity skills as a major weakness (30%), alongside a lack of staff awareness that exposes organisations to unnecessary risk (32%). These are not new problems, but AI magnifies their impact. As systems become more complex, the consequences of human error, misunderstanding and misuse grow more serious.

Training is struggling to keep pace. Nearly two-thirds of CIOs believe their organisation does not yet provide sufficient education on responsible AI use and AI-related risk (66%). More than half say employees are already putting data security at risk through how they use AI tools (57%).

Operationally, security teams are already feeling the impact. Over a third of CIOs say AI has created new security blind spots (34%), while a similar proportion

believe it has reduced their organisation's ability to detect breaches and cyberattacks effectively (35%). More concerning still, two in five report that incident response times have worsened (41%).

These are early warning signals. AI is increasing complexity inside security operations faster than processes, skills and tools are adapting. Systems are becoming harder to observe, harder to interpret and harder to control with confidence.

Just **37%** of CIOs say they have full visibility of the AI tools and services in use

Most organisations recognise the need for AI-specific governance, and almost all report having some form of it in place but only around a third of CIOs are extremely confident that their AI governance controls can keep pace with deployment (34%), and just over a third believe they have full visibility of all the AI tools and services in use across their organisation (37%).

Even more revealing is the degree of compromise. Nearly two-thirds (62%) admit relaxing governance standards due to limited understanding or capability.

62% admit they compromise on AI governance standards due to limited knowledge or capability

That is not a failure of intent. It is a sign that AI governance is running ahead of institutional capacity.

The data reveals a structural imbalance. Ownership of AI is distributed across the organisation, but accountability for its consequences is increasingly concentrated with the CIO.

This makes AI risk different from most previous technology risks. It is not just technical. It is organisational. It sits in the gaps between roles, teams, and decision rights.

Vendor dependence adds another layer of fragility. Many organisations acknowledge that they are increasingly reliant on a small number of AI providers for critical functions (59%). At the same time, concern about an "AI bubble" is widespread (67%), reflecting unease about the market's stability and maturity. Despite this, a significant proportion still lack continuity plans should a key provider become unavailable (16%).

For CIOs, this extends the idea of security beyond systems and data into supply chains, commercial resilience and strategic optionality.

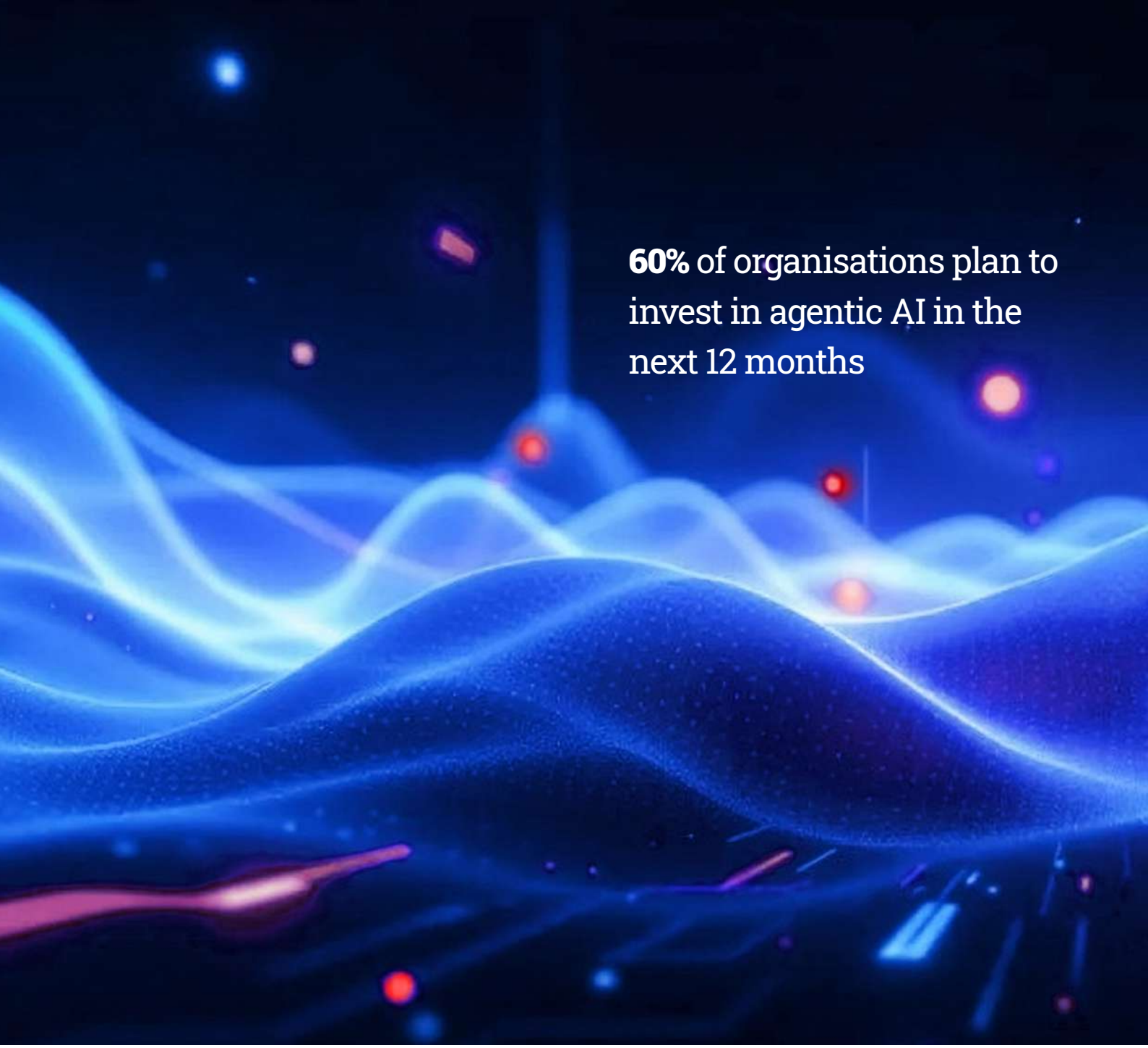
The response so far has been pragmatic. Many organisations are turning to external support, either by outsourcing cybersecurity elements (32%) or by bringing in contractors and interim specialists to close urgent gaps (31%). These measures provide capacity and expertise, but they also underscore a deeper truth: AI risk governance is becoming a permanent feature of leadership, not a temporary response to a new technology.

What is emerging is a quieter, more complex responsibility. CIOs are being asked to make AI safe enough to trust before it becomes powerful enough to be dangerous. They are operating in a space where visibility is imperfect, skills are scarce, and accountability is shared.

In that environment, governance is no longer a matter of policy, it is a matter of judgment. The CIO's role is increasingly defined by their ability to hold the organisation steady while its systems become more autonomous, more interconnected and harder to fully control.

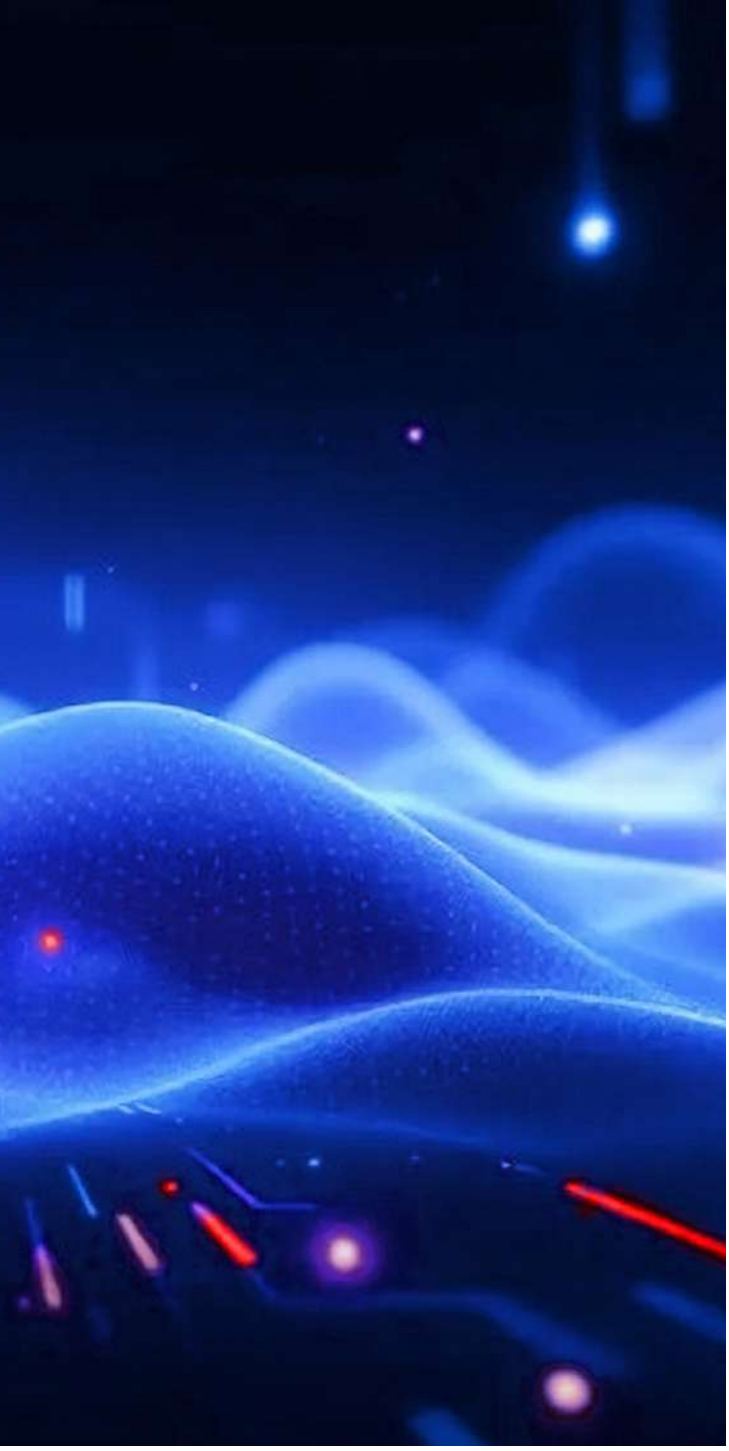
CHAPTER 4

The Next Frontier



As AI moves from supporting work to actively shaping it, the nature of enterprise technology begins to change again. Generative AI has captured attention because it is visible and immediate, but it is only the first step in a longer shift towards systems that act with increasing independence. For CIOs, this is where the conversation stops being about tools and starts becoming about behaviour. What happens when technology is no longer just something the organisation uses, but something that participates in how it operates?

Investment patterns already reflect this transition. Generative AI remains firmly on the agenda, with nearly three-quarters of organisations (72%) planning further investment in the next 12 months. But interest is moving quickly beyond it. Six in ten expect to invest in agentic AI (60%), signalling a growing appetite for systems that can execute tasks, make decisions



and coordinate activity with minimal human intervention.

AI is shifting from augmentation to agency. For CIOs, the implications are less about performance and more about accountability. Systems that advise can be challenged. Systems that act must be governed.

The practical consequences of this are only just beginning to surface. As AI becomes more autonomous, questions of identity, authority and traceability become more complex. Who is responsible when an AI-driven process makes a flawed decision? How are actions audited? How is intent distinguished from error? These are not abstract governance problems. They shape how much responsibility organisations are willing to give to machines in critical workflows.

The workforce implications are similarly unsettled. Some organisations expect AI to reduce headcount (40%), others expect it to increase (31%). The gap between those positions suggests that AI's impact will not follow a single pattern. More likely, it will reshape roles rather than simply remove or create them.

For CIOs, this makes workforce design part of AI strategy. The question becomes how to structure environments where humans and AI systems work together, how authority is shared, and how accountability is maintained when work is distributed across people and machines.

Beyond AI, CIOs are also being asked to think across multiple horizons at once. More than half believe generative and agentic AI will disrupt existing business models within the next two years (53%). At the same time, quantum computing is already appearing on strategic roadmaps, with almost a third expecting it to have a similar impact (30%).

This has consequences for operating models. The growing reliance on Managed Service Providers reflects a recognition that few organisations can sustain the pace of change alone. Nearly all expect to use MSPs in the coming years (94%), and almost half anticipate that external partners will deliver core IT services (47%).

This changes the CIO's role again. Technology leadership becomes less about ownership and more about orchestration. The enterprise increasingly depends on a web of vendors, platforms and specialists and managing that ecosystem becomes as important as managing internal teams.

For CIOs, this demands a different kind of leadership. Less about transformation projects, more about institutional design. Less about deploying new tools, more about shaping environments in which autonomous systems, external partners and human teams can coexist without eroding accountability.

If earlier chapters revealed how AI is accelerating pressure, complexity and risk, this one points to something longer term. The CIO is becoming the architect of an organisation that must remain in control even as intelligence becomes distributed, autonomy becomes normal, and control becomes harder to centralise.

More than half of CIOs believe AI will disrupt their business models within the next two years

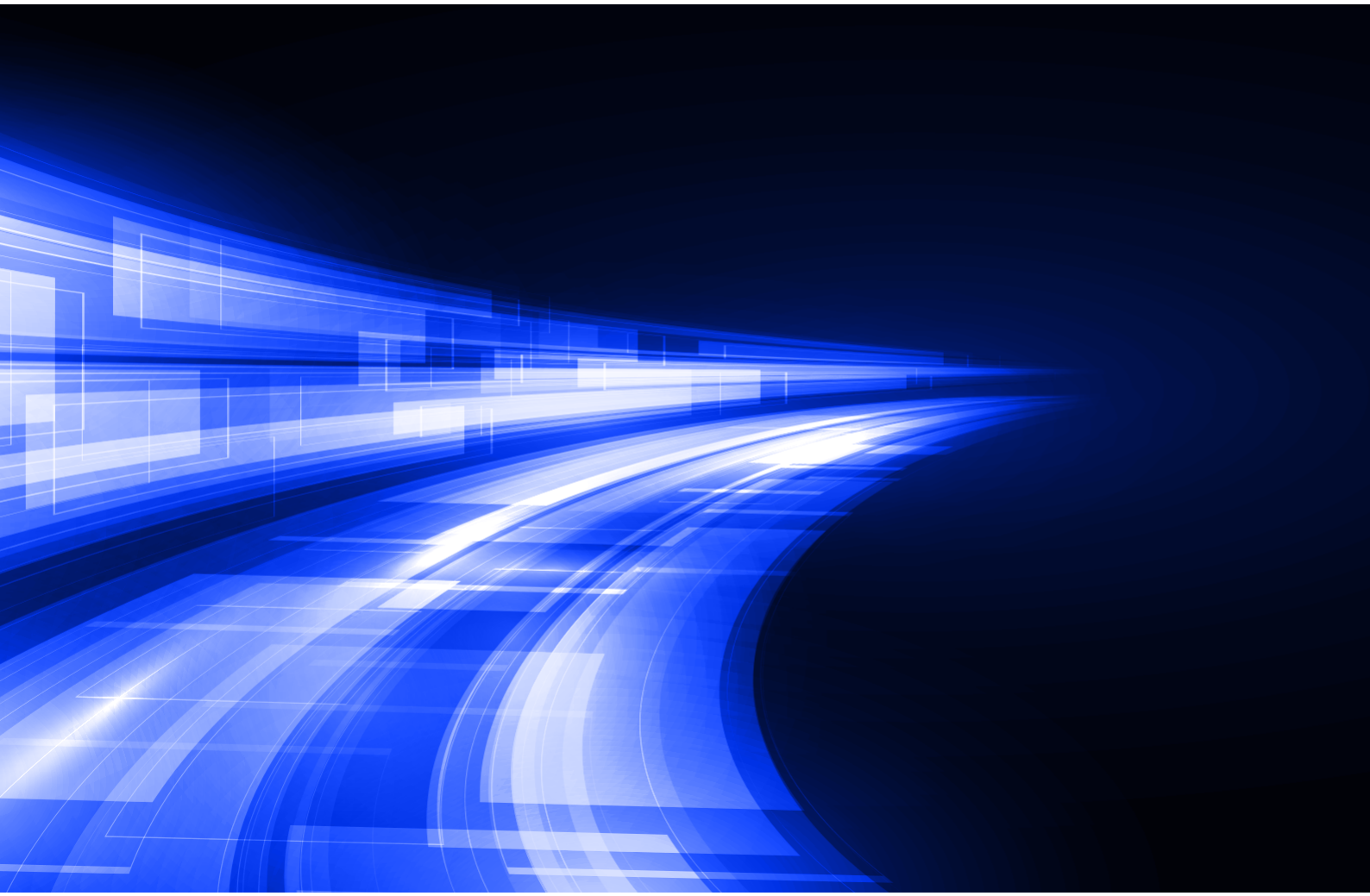
Nearly all organisations plan to rely on Managed Service Providers in the next 2–3 years

Conclusion

The perspectives shared by CIOs in this year's report point to a far-reaching shift. AI is no longer something organisations are preparing for, it's shaping decisions, expanding risk and redefining what responsibility looks like inside the enterprise.

For CIOs, their role is becoming less about introducing new capability and more about shaping the conditions under which that capability can thrive sustainably.

Across all four chapters, a consistent tension runs through the data. Ambition is high, momentum is strong and belief in AI's potential is widespread. At the same time, confidence in governance, scalability and long-term control is shaky. CIOs are operating in a space where progress is accelerating faster than the structures designed to support it. They are expected to move decisively while also absorbing the consequences of decisions whose implications are not yet fully visible.



What the research reveals isn't hesitation, but realism. CIOs understand that AI can't simply be deployed and left to evolve, it has to be guided and made dependable before it can be truly beneficial.

In earlier technology cycles, success was often measured by how quickly new capabilities could be deployed. In the AI era, success will be measured by how effectively those capabilities can be harnessed and managed, how well they can be governed, how independently they can be allowed to act, and how confidently organisations can rely on them without losing sight of human judgement and institutional accountability.

That is a bigger responsibility than any single technology project, but it is also what makes this moment one of the most significant in the history of the CIO role.

LOGICALIS
Architects of Change

We are Architects of Change. We help organisations succeed in a digital-first world.

At Logicalis, we harness our collective technology expertise to help our clients build a blueprint for success, so they can deliver sustainable outcomes that matter.

www.logicalis.com/cio-report