

Building the resilient, agile, AI-enabled enterprise

AI is delivering real value, so teams are moving beyond pilots and into live business use. Turning that intent into production-grade AI is proving harder than many expected without sacrificing resilience, trust or security.

Azure leaders are under pressure to demonstrate resilience, accelerate transformation and prepare their platforms for enterprise AI. The insight in this report comes from working with some of the most complex Azure environments in the UK. We've built award-winning Accelerator Packs that deliver enterprise-grade platforms quickly and we use them in our own business every day. That's how we know what works, what doesn't and where the real returns are.

Executive summary

What follows links resilience, transformation and platform readiness directly to specific platform, architecture and operating model decisions that influence outcomes. You will gain a clear view of likely gaps in your current Azure estate and a focused set of priorities to guide investment in platform engineering, security by design and automation. BlakYaks starts by assessing the security posture and operational resilience of your current deployment, ahead of migrations and future service deployments, and how ready your Azure foundations are to host production workloads.

Talk to our team today or visit blakyaks.com to start with a complimentary Azure Vitals Assessment.

THE LANDSCAPE IN NUMBERS

70%

of digital transformations fail to meet objectives

15%

have achieved enterprise-scale AI deployment

The industry context: resilience and AI adoption.

RESILIENCE IS NOW A QUESTION OF SURVIVAL

We have watched operational resilience shift from something that sat with IT teams and business continuity planners to a standing agenda item in the boardroom. According to the BCI's Operational Resilience Report 2025, over 70% of organisations had established an operational resilience programme, with a further 10% in development.

DORA and the UK's FCA and PRA requirements are pushing the rest to follow. But regulation is only part of the picture. The increased frequency and cost of disruption is what has moved the conversation forward.

Research across 1,000 global enterprises highlights patterns that are widely seen across enterprise Azure environments: outages are escalating and recovery times are growing longer.^[3] For organisations running critical workloads on Azure, there is often an opportunity to tighten recovery time and data protection objectives, and to reduce the manual overhead that platform teams carry when proving resilience to the business.

If you are unsure where your Azure environment sits on this maturity curve, our Azure Vitals Assessment provides a fast, evidence-based snapshot of your current resilience posture and platform readiness.

Sources: resilience programme data^[3]

AI: THE GAP BETWEEN AMBITION AND PLATFORM READINESS

The enthusiasm around enterprise AI is well founded. We see it delivering real value in productivity, decision-making and operational efficiency. But we also see a pattern repeating across almost every organisation we work with: the ambition around AI is running well ahead of the platform's ability to support it.

The industry data confirms this. Only around one in four AI initiatives currently deliver their expected return on investment, and fewer than 20% have been fully scaled across the enterprise.^[4] For Azure platform leaders, this gap shows up as integration failures, governance blind spots and data privacy risks that were latent in the environment long before AI arrived. Integration complexity and data privacy risks are now the dominant barriers. A useful way to think about this is that privacy is mainly shaped by how data is governed and used, while infrastructure decisions mostly affect how easily data can be accessed and moved. These are infrastructure silos that become critical when AI is introduced. In most cases, they were already there, and tolerated, but today's pace of change makes them untenable.

Most organisations are still in the early stages. They are familiar with conversational tools that respond to prompts and return answers. Increasingly, though, we are seeing enterprises explore more advanced approaches where intelligent systems support planning, execution and decision-making across live platforms. Agentic AI systems go further than a simple chat interface.

That progression from conversational to agentic changes the stakes entirely. AI agents interact with your infrastructure. They pull from your documentation. They write code against your standards. The environment they operate in has to be governed, predictable and secure. The agent reflects the platform it runs on. AI performs reliably when the platform it runs on is built to the right standard: secure by design, consistently governed and ready for production workloads.

BlakYaks have built and deployed this ourselves. We run a fully private, secure Azure back end for AI services internally. We built the platform first and that is why it works.

Sources: AI ROI and scaling^[4]

blakyaks.com

The customer reality: transforming at speed.

WHY TRANSFORMATION KEEPS FAILING

The transformation failure rate should worry us all. Global business and technology transformation spending is headed for \$3.4 trillion.^[5] Most programmes still fall short. Only 12% of those that do succeed hold onto those gains beyond three years^[6]. In Azure estates, the pattern is consistent: cloud and data transformation stalls when platform engineering is treated as a layered on activity rather than the foundation of the entire programme.

We see the same root causes again and again:

- Change fatigue and competing priorities across teams and leadership
- Executive sponsorship is not secured beyond initial programme
- No clear strategic alignment between technology and the business
- Poor change management and teams launched into transformation without a plan

Organisations with a structured change management approach are seven times more likely to hit their transformation goals^[7]. Most programmes struggle do so because they move too slowly, fail to deliver visible impact, or are constrained by existing design and deployment issues in the legacy Azure environment.

Identifying what is really holding you back starts with understanding where the key risks and gaps sit in your Azure estate. An Azure Vitals Assessment analyses your landing zone architecture, security posture and policy alignment, benchmarks your environment against best practices, and highlights the most important risks, gaps and optimisation opportunities to address next.

Sources: transformation spending^[5]; sustained gains^[6]; change management success^[7]

TRANSFORMATION MUST FUND ITSELF

The days of open-ended transformation budgets are over. CTOs are expected to demonstrate ROI before the spend is approved. We see the successful programmes tying every initiative back to efficiency gains, revenue protection, or risk reduction. The evidence is consistent: resilient companies achieve 3% to 5% higher annual revenue growth than their peers. For Azure-based enterprises, those gains come from automation, policy-driven deployment and infrastructure as code, with licensing only opening the door.

Cloud-based solutions can drive efficiency improvements of up to 30%^[8], but only when automation and platform engineering are treated as strategic capabilities. The subscription gets you access. The engineering gets you the return.

Sources: cloud efficiency gains^[8]

The execution framework: engineering the agile enterprise.

SECURITY BUILT INTO EVERY LAYER

Despite significant investment in organisational resilience, including risk management, business continuity and technology resilience, most organisations remain unprepared for a major disruption. The gap between what they spend and what they can actually withstand is a growing cause of concern.^[9]

In practical terms, this means Azure environments with security and compliance layered on retrospectively, creating audit overhead, policy drift and blind spots that teams do not have the time or resources to govern properly.

If your security controls, identity governance and compliance automation are not where they need to be, the right move is to invest the time and engineering effort to fix that before the next migration or deployment. Every workload that lands on a well-engineered platform inherits those standards automatically, and the long-term returns are significant.

AUTOMATION AS THE GROWTH ENGINE

Automation is what breaks the trade-off between moving fast and staying resilient. Every manual step replaced or removed reduces human error, cuts through delays and eliminates inconsistency.

Over 40% of enterprises are planning to automate manual disaster recovery tasks within the next twelve months^[10]. For Azure platform teams, this translates to replacing manual runbooks with policy-driven pipelines, Infrastructure as Code, and automated testing before production deployment. The direction is right, but the pace has been slow.

The case for moving faster is straightforward: every manual step automated is one fewer source of error, drift or delay. Organisations that treat automation as a strategic discipline consistently outperform those that treat it as a tooling exercise.

We see this across every platform we build and operate:



INFRASTRUCTURE AS CODE

Every environment built the same way, every time



AUTOMATED TESTING

Quality assured before anything reaches production



POLICY-DRIVEN DEPLOYMENT PIPELINES

Speed and control working in concert

BUILDING THE SECURE BACK END FOR AI

89% of organisations are now piloting or deploying AI-augmented workflows.^[11]

That sounds impressive until you learn that only 15% have achieved enterprise-scale deployment.^[12] The gap between pilot and production-scale AI in Azure typically comes down to three things: integration complexity, data privacy risk and lack of a governed secure back end. These barriers are familiar to us. We see them in every environment where AI has been introduced before the platform foundations were ready:



DATA PRIVACY RISKS

Raised by 67% as a critical concern when deploying AI in enterprise environments^[11]



INTEGRATION COMPLEXITY

Cited by 64% of organisations as the primary blocker to AI at scale^[12]

These barriers are familiar to us. We see them in every environment where AI has been introduced before the platform foundations were ready. The practical reality is that if you want to run agentic AI systems that interact with your infrastructure, pull from internal documentation and write code against your standards, you need a fully private, secure back end built for that purpose.

Those AI services must be deployed properly in Azure, with the right security measures, network isolation and governance controls, or you lose the ability to trust and govern what the agents produce at scale.

Our award-winning **Accelerator Packs are pre-engineered**, pre-tested Azure solutions that deliver enterprise-grade platforms at speed. We apply the same approach to secure the AI layer, so it remains consistent, automated, governed and secure. The platform enforces those standards across every workload that runs on it. That consistency is what makes AI trustworthy at scale.

Talk to our team today or visit blakyaks.com to start with a complimentary Azure Vitals Assessment.

Looking ahead: what we think enterprise leaders should prioritise.

Elevate resilience to board-level strategy. The most competitive organisations treat resilience as a board-level discipline, with unified accountability spanning business continuity, risk management and cybersecurity. Those that do recover faster, protect revenue more effectively and retain customer trust under pressure. Every client that has made this shift tells us the same thing: the conversation about platform investment changes entirely. It becomes one of the most important strategic decisions on the agenda.

Close the gap between ambition and execution. Successful transformation is as much about people as it is about platforms. The programmes that deliver have strong executive sponsorship, a structured change plan and leadership that stays present throughout. We have seen this make the difference repeatedly, on both sides. Leaner programmes often outperform well-funded ones when the people side is taken as seriously as the technical delivery.

Embed security by design. Redesigning security after the fact is one of the most common challenges across Azure estates, and one of the most important things we fix. DevSecOps is built into every landing zone we deliver, with policy enforced in code and embedded in the platform itself. The result is a platform where security is verifiable, auditable and consistent from the first deployment.^[13]

Build AI on platform foundations. AI readiness is a direct consequence of getting your cloud environment right. Consistent, automated, governed, secure. Enterprise AI only delivers when the platform underneath it is ready. The organisations seeing real returns built that foundation deliberately, prioritising security, governance and consistency before rolling out AI across the business.

Overall.

The themes running through this report converge on one point. Resilience, transformation and AI readiness all depend on the same thing: a platform built with the right foundations. The organisations that understand this are the ones moving with confidence. BlakYaks has delivered exactly this for some of the most complex Azure environments in the UK, and we use it ourselves every day.

Talk to our team today or visit blakyaks.com to start with a complimentary Azure Vitals Assessment.

Sources and references.

Full source URLs are provided in the footnotes throughout this document.

- [1] Mavim, Why 70% of Digital Transformations Fail: Insights and Solutions.
<https://blog.mavim.com/why-70-of-digital-transformations-fail-insights-and-solutions>
- [2] Microsoft Ignite, Building Secure AI-Ready Infrastructure (BRK217).
<https://ignite.microsoft.com/en-US/sessions/BRK217>
- [3] Fusion RM, The Intersection of AI and Operational Resilience.
<https://www.fusionrm.com/whitepapers/its-all-about-data-intersection-of-ai-and-operational-resilience/>
- [4] Stack AI, AI Statistics and Enterprise Benchmarks.
<https://www.stack-ai.com/blog/ai-statistics>
- [5] MeltingSpot, Why Digital Transformation Projects Fail.
<https://blog.meltingspot.io/why-digital-transformation-projects-fail/>
- [6] McKinsey & Company, Perspectives on Transformation.
<https://www.mckinsey.com/capabilities/transformation/our-insights/perspectives-on-transformation>
- [7] Prosci, Change Management and Transformation Research.
<https://www.prosci.com/change-management/thought-leadership/11-stats-transformations>
- [8] Rocket.chat, Business Resilience and Cloud Efficiency.
<https://www.rocket.chat/blog/business-resilience>
- [9] Forbes, Without the Right Culture Your Digital Transformation Efforts Will Fail.
<https://www.forbes.com/sites/larryenglish/2023/03/21/without-the-right-culture-your-digital-transformation-efforts-will-fail/>
- [10] Cutover, Annual IT Disaster & Cyber Recovery Trends and Insights Report 2025.
<https://www.cutover.com/content-hub/annual-it-disaster-cyber-recovery-trends-insights-report-2025>
- [11] Capgemini, World Quality Report 2025: AI Adoption in Quality Engineering.
<https://www.capgemini.com/news/press-releases/world-quality-report-2025-ai-adoption-surges-in-quality-engineering-but-enterprise-level-scaling-remains-elusive/>
- [12] IBM, Operational Resilience and AI.
<https://www.ibm.com/think/insights/operational-resilience-ai>
- [13] Microsoft Learn, Secure AI-Ready Infrastructure Training Path.
<https://learn.microsoft.com/training/paths/secure-ai-ready-infrastructure/>



BlakYaks.
a **PROACT** company

GET IN TOUCH

020 4551 9237
solutions@blakyaks.com
blakyaks.com
