rapidscale



AI AT SCALE:

What it takes to build an AI-ready enterprise

What the state of enterprise modernization reveals about the future of AI

Table of contents

Introduction 3

Key findings 4

Section 1
Modernization often introduces complexity instead of removing it 5

Section 2
Cloud maturity doesn't mean operational continuity 7

Section 3
How organizations adopt new technology matters for stability 9

Section 4
AI raises the stakes for infrastructure resilience 11

Special report
The human side of AI scale 13

Conclusion
Rising AI dependence, uneven operational readiness 14

Appendix + methodology
Additional data points 15

Introduction

AI may be becoming business-critical faster than the infrastructure around it can keep up.

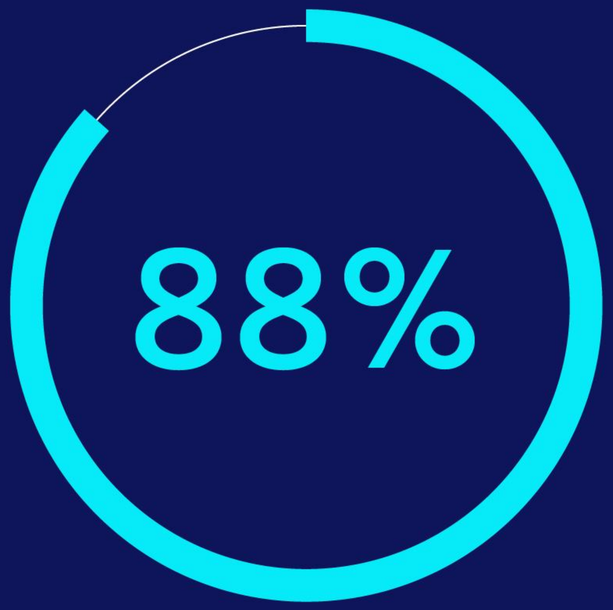
RapidScale surveyed 368 U.S. professionals involved in digital transformation to understand how organizations are managing AI's growing role in business operations and what their experience with cloud modernization can tell us about the road ahead.

The findings point to a potential readiness gap. Organizations are adding new capabilities to environments that are still evolving and not always stable. As AI becomes more critical to day-to-day work, the stakes of that instability rise with it.

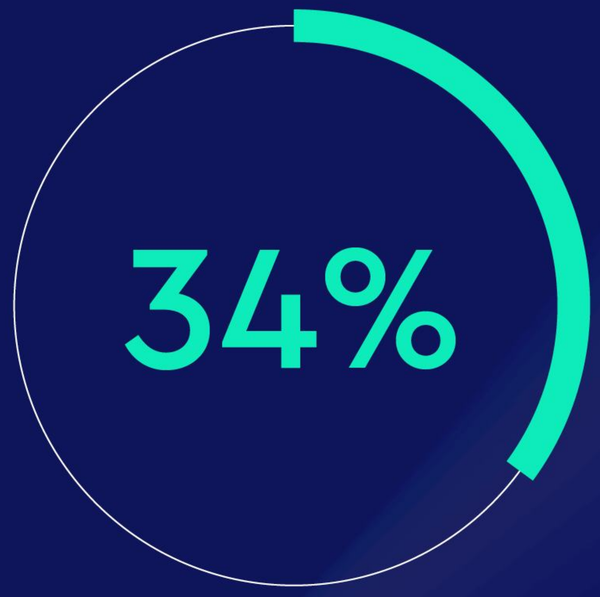
This report explores whether operational resilience is keeping pace and what the organizations furthest along in modernization can teach us about the risks ahead.



Key findings



use AI tools more than they did a year ago



anticipate significant or severe disruption if AI were unavailable for a day



experience unplanned cloud downtime or performance issues at least monthly

Organizations with advanced cloud maturity are **more than 4x as likely** to experience cloud downtime or performance issues multiple times per week.

Organizations where AI adoption is fragmented are more **than 2x as likely** to experience weekly cloud disruption.

Section 1

Modernization often introduces complexity instead of removing it

Each round of infrastructure modernization is meant to leave the environment simpler than it found it.

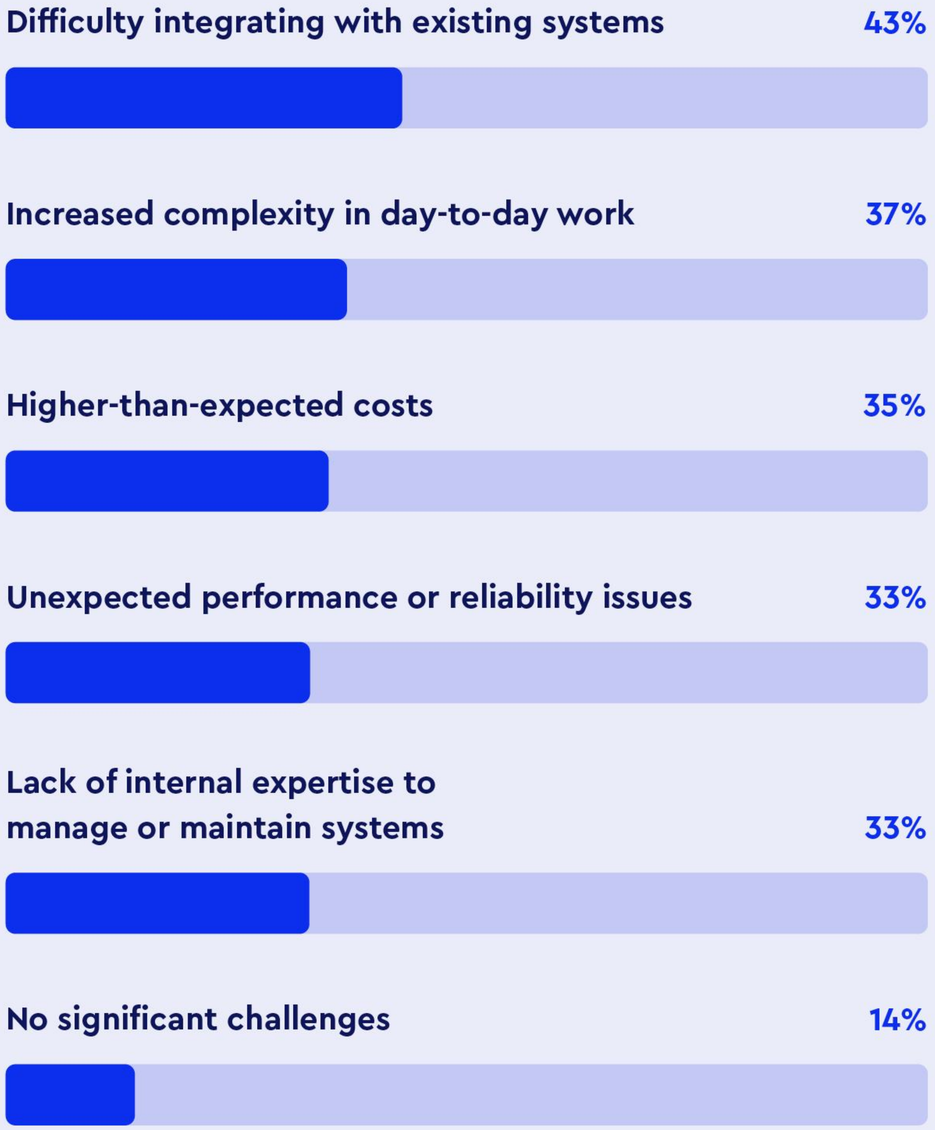
That's not what's happening at many respondents' organizations. As they modernize continuously, organizations add complexity *and* new points of instability.

About half of respondents (51%) say their organizations experience unplanned downtime or performance issues related to cloud infrastructure and applications at least monthly, including 16% that experience them at least weekly. Whether it's increased application latency or a total outage, these issues can interfere with day-to-day operations.

During cloud-based outages, 51% of respondents lose access to needed tools or systems, while 44% lose access to critical data. As AI becomes embedded in business workflows, reliable access to the systems and data around it becomes critical.

But reliability is only part of the challenge. Of respondents who had visibility into how their organization manages cloud-based systems and platforms, nearly nine out of 10 (86%) experienced at least one challenge following a new software, tool, or system implementation in the past year, led by difficulty integrating with existing systems (43%) **[Fig. 1]**.

Fig. 1: Post-implementation challenges organizations experienced in the past 12 months



Respondents rank security and compliance (57%) and performance and reliability (51%) as their most difficult cloud management challenges, pointing to gaps that can keep IT and operations focused on immediate needs rather than proactively optimizing systems for AI at scale **[Fig. 2]**.

Fig. 2: Top cloud management challenges





↗

Key takeaway

Modernization can solve yesterday's technology problems while simultaneously creating new integration and operational demands. The challenge is maintaining stability as the environment becomes more advanced.

Section 2

Cloud maturity doesn't mean operational continuity

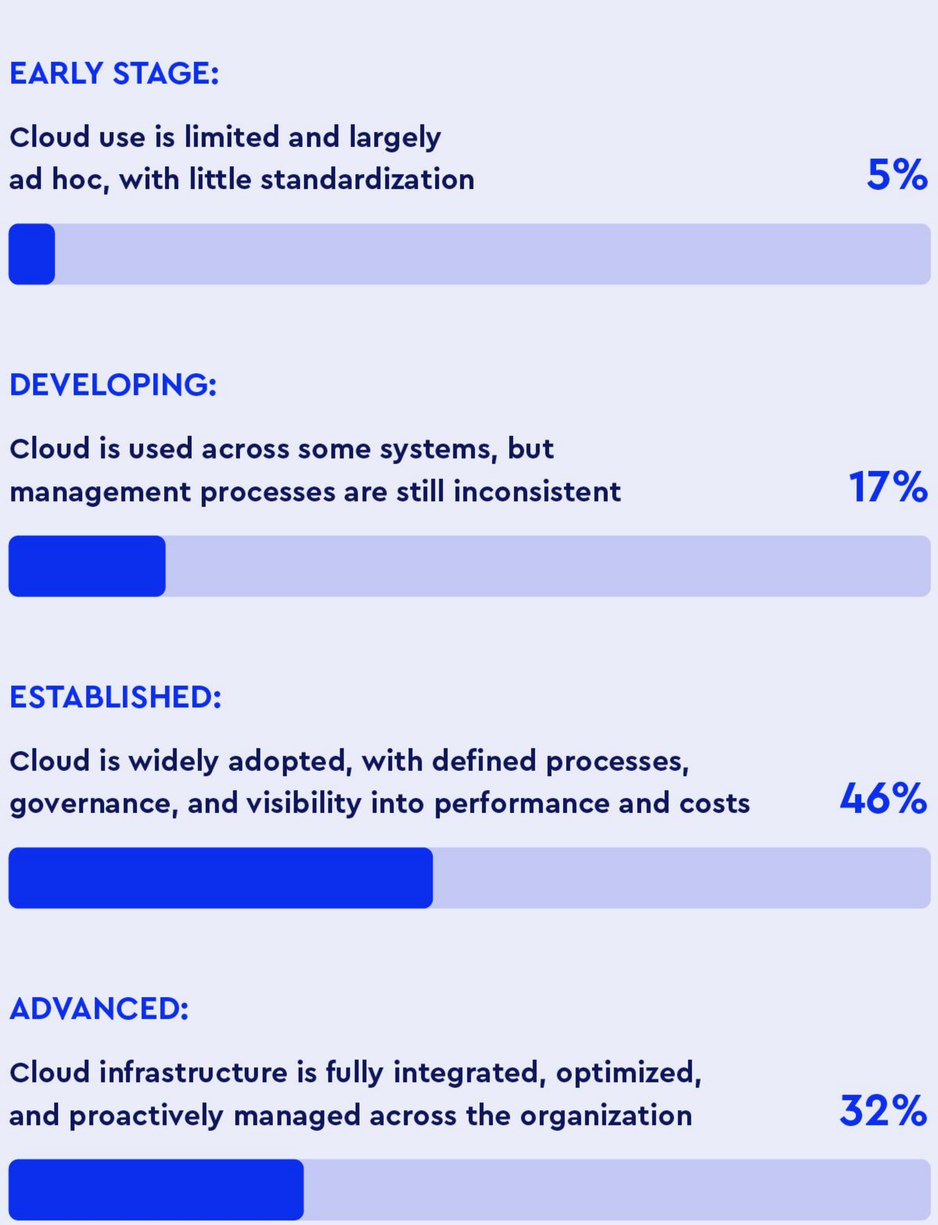
The reasonable assumption is that operational problems decline as cloud environments mature. Across several measures, they do.

Because established and advanced organizations make up the majority of respondents, they offer the clearest view into what specifically changes as cloud environments mature. For example, advanced organizations are less likely to report challenges from implementing new software, particularly around skills gaps or integration difficulties **[Fig. 3]**.

Fig. 3: Challenges encountered after implementing new software, established vs. advanced

Challenges	Established	Advanced
Difficulty integrating with existing systems	33%	26%
Lack of internal expertise to manage or maintain systems	48%	32%
No significant challenges	14%	22%

Fig. 4: How respondents rated their organizations' cloud maturity



But that pattern doesn't extend to operational stability.

Among advanced organizations, more than half (57%) experience unplanned cloud downtime or performance issues at least a few times a month, 1.3 times the 45% reported by established organizations.

However, that comparison only tells part of the story. As downtime grows more frequent, the gap between established and advanced organizations widens.

Advanced organizations are 1.7 times as likely to experience disruption a few times a month, 2.8 times as likely to experience it weekly and **more than four times as likely to experience it multiple times per week [Fig. 5].**

In other words, while both established and advanced organizations break, the advanced ones experience more frequent disruptions.

That distinction matters. Occasional disruption is common across complex technology environments. Chronic disruption points to a different operational challenge: maintaining reliability as scale, interconnectedness, and technology demands increase.

Key takeaway

Cloud maturity and operational continuity are different capabilities. Organizations can become more sophisticated without becoming more stable.

Fig. 5: Frequency of cloud downtime or performance issues, established vs. advanced

Frequency	Est.	Adv.	Multiplier
Rarely or never	16%	19%	1.2
At least a few times a year	83%	82%	1
At least once a month	45%	57%	1.3
At least a few times a month	29%	48%	1.7
At least weekly	10%	28%	2.8
Multiple times per week	4%	18%	4.5

Section 3

How organizations adopt new technology matters for stability

If maturity alone does not guarantee stability, what distinguishes organizations experiencing fewer chronic disruptions? The clearest difference is how technology enters the environment.

New technologies are evaluated and introduced through multiple, often overlapping paths. While 59% use structured evaluation processes and 45% have a formal internal team or function, 36% say individual teams or leaders independently explore and adopt new technologies **[Fig. 6]**.

Fig. 6: How organizations evaluate and stay informed about new technologies



That decentralized pattern is associated with substantially more frequent disruption. Organizations where teams or leaders independently explore and adopt new technologies are more than twice as likely to experience cloud downtime or performance issues at least weekly—26% compared with 11% among organizations without this approach.

The pattern is even more pronounced in advanced cloud environments, where 42% experience these issues at least weekly, compared with 18% of their peers.

↗

Key takeaway

Not every technology decision needs to be centralized. Business teams need room to experiment, and organizations need to move quickly as new capabilities emerge. However, organizations need a coordinated process for introducing change into an increasingly interconnected environment, even when individual teams retain ownership of their decisions.



Section 4

AI raises the stakes for infrastructure resilience

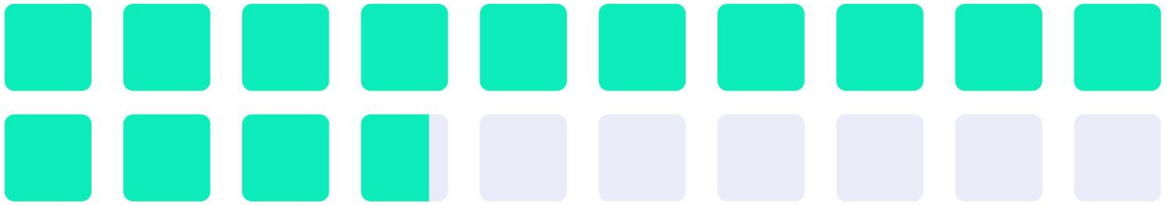
Organizations have been evolving their cloud infrastructure for years. Now, they're introducing AI, a newer and faster-moving layer, into those same enterprise environments.

Already, 88% of respondents use AI tools more than they did a year ago. For many, that adoption was not a deliberate bet. In fact, 86% say their organization's AI usage came through features embedded in software they already owned or through a mix of embedded capabilities and internally built tools.

AI is also becoming operationally important. Nearly nine in 10 respondents (89%) said they expect at least some level of disruption if their primary AI tools were unavailable for a full business day, including 34% who anticipate significant or severe disruption.

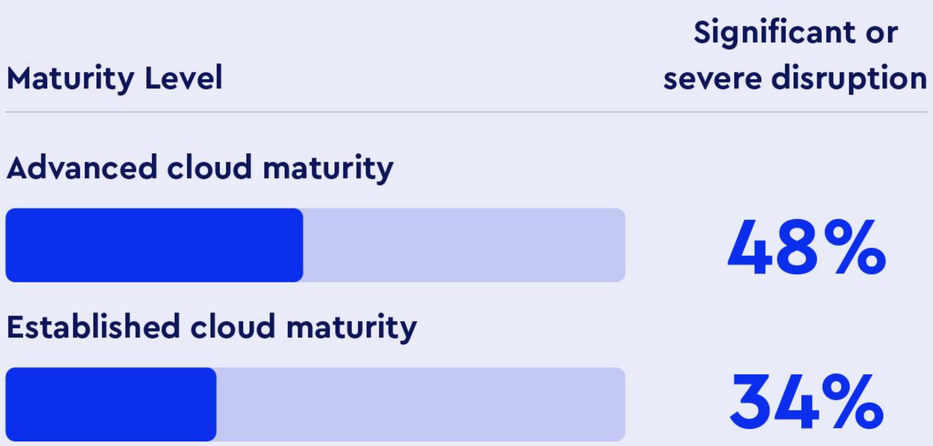
The organizations furthest along in cloud maturity are moving even faster. Two-thirds of advanced organizations (67%) report significantly greater AI use than a year ago, compared with 49% at established organizations.

Their expected exposure is also greater. Nearly half (48%) of advanced organizations anticipate significant or severe disruption if their primary AI tools were unavailable for a full business day, compared with 34% of established organizations **[Fig. 7]**.



68% **of respondents are concerned about their organization's ability to maintain operations during an AI outage.**

Fig. 7: Anticipated impact of a one-day AI outage



The financial stakes follow a similar pattern, with 58% of advanced organizations anticipating at least $100,000 in costs from a one-day AI outage, compared with 49% of established organizations.

None of these findings demonstrate that cloud instability will cause AI disruption. Instead, they illustrate something simpler: The organizations reporting the most chronic instability in their cloud environments are also increasing their dependence on AI the fastest.



↗

Key takeaway

AI is rapidly becoming part of the operational load technology environments must carry. That load is growing faster than the evidence that organizations can carry it.

Special report

The human side of AI scale

As AI becomes embedded in everyday work, organizations are still working out the guardrails around it—from who is accountable for AI decisions to how much employees should rely on the technology and where sensitive data can be used.

1 AI oversight is still taking shape.

Just 43% of respondents say their organization has clearly defined and consistently enforced AI oversight. Among these respondents, only 15% are concerned about unclear responsibility when AI-related issues occur, compared with 24% of other organizations. The difference underscores the role governance can play in establishing accountability as AI becomes embedded across the business.

2 Sensitive data remains a governance fault line.

Policies around sensitive data also vary, with **64% of respondents** saying their organization limits or prohibits the use of AI with sensitive data. Another 18% allow it with clear controls and safeguards, while smaller shares report inconsistent controls or regular use without strict safeguards.

3 AI reliance is testing workforce judgment.

Growing AI use is also raising questions about how employees work and develop expertise.

62% are concerned about over-reliance on AI tools in day-to-day work.

63% worry employees may rely on AI outputs without verifying their accuracy.

70% agree that employees early in their careers may be less likely to develop foundational skills because of their reliance on AI.

Yet respondents express considerable confidence in their own abilities: **93% say they are confident they can identify incorrect or misleading AI outputs in their work**. That contrast suggests respondents may have more confidence in their own AI judgment than in the broader organization's ability to use AI critically and responsibly.

Conclusion

Rising AI dependence, uneven operational readiness

Taken together, the findings reveal a tension at the center of enterprise AI adoption. AI raises the stakes for a challenge organizations already face: how to continually introduce new technology without sacrificing operational continuity.

For many organizations, external expertise can help connect these priorities across cloud, data, applications, AI, and security. But the larger lesson extends beyond any individual technology decision.

Maturity and continuity are separate capabilities. As AI becomes more critical to business operations, organizations need to build both.



Appendix: Additional data points

74% of respondents anticipate losses of $50,000 or more if their organization's primary AI tools were unavailable for a full business day, with 49% expecting losses of $100,000 or more.

47% of respondents say they have full visibility into factors like performance, cost, and risk when making decisions about systems or tools.

When decisions about systems or tools are made without full visibility, 37% of respondents say decisions need to be revisited or adjusted after implementation, while 33% report higher-than-expected costs, 33% longer implementation timelines, and 32% rework.

26% of respondents say integration challenges are the biggest factor limiting value from AI and cloud investments, followed by security, compliance, or governance requirements limiting use (20%).

Half of respondents say AI oversight and accountability at their organization are still evolving (25%) or defined, but not consistently applied (25%).

Methodology

RapidScale surveyed 368 U.S. professionals at the manager level and above at organizations with more than $50 million in annual revenue. Respondents are involved in digital transformation across IT, operations, finance, marketing, and digital strategy. Data was collected in April 2026.