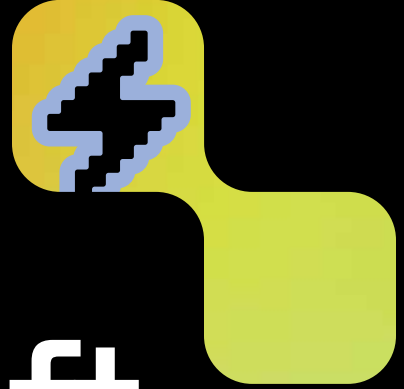


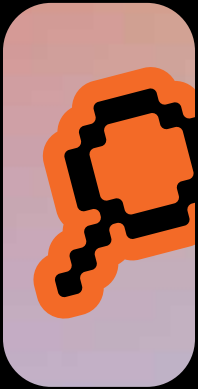
ShareGate



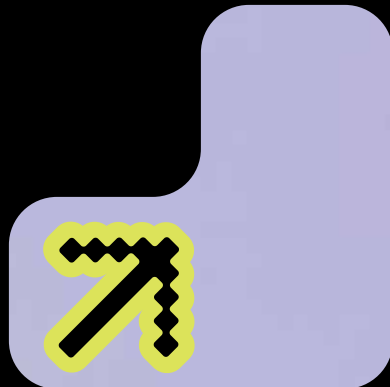
Microsoft

365

Decoded



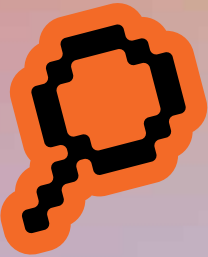
Get Total
Data Clarity



ShareGate



Microsoft 365 Decoded



Get Total
Data Clarity



What's in the book?

Foreword	2	Who's governing Microsoft 365? The 1% gap	62
The forces reshaping IT	4	Copilot readiness: Progress, pitfalls, and the opportunity for IT	84
Migration momentum	10	From pressure to payoff: An IT leader's mandate in 2026	98
M&A migrations by the numbers	28	Report contributors and research details	102
The security paradox: A data-driven look at Microsoft 365	44	Glossary	106

I've spent the last 15 years in and around the world of Microsoft 365. The truth is, it's never been harder to cut through the noise than it is today. New features, new acronyms, new AI assistants. Every week it feels like something shifts. Vendors talk. Microsoft talks. And the people who've had to make it all work? They're often left to sort hype from reality on their own.

That's why I'm excited to introduce this book. It's a grounded, honest look at what's really happening inside Microsoft 365 environments today, drawn from data, the hard-won experiences of MVPs, and Microsoft's own roadmap signals.

Here's what I hope this book gives you:

1 Perspective

Not just of where things are now, but where Microsoft is investing next, and how that shapes your window of opportunity.

2 Tools

In every chapter, you'll find checklists, scorecards, and frameworks, so you can move from reading to doing immediately.

3 Authenticity

You'll see hard data, including insights from people using Microsoft 365 with other vendors' tools. This book aims to give you a neutral, fact-based view of the ecosystem rather than a ShareGate echo chamber.

4 Confidence

As you dabble in AI, handle migrations, or clean governance debt, this is your guide, your roadmap, your ally.



The ecosystem is shifting fast. Some will talk louder. Some will promise more. Some will be drowned out by their own noise. My hope is that this book gives you some clarity.

We can't slow Microsoft's release cycle, and I wouldn't want to. But we can stay calm, confident, and in control.

This book won't do the work for you. It will, however, help you to see what matters so you can do the work that counts in 2026.



Benjamin Niaulin
VP of Product at **ShareGate**

01

The forces reshaping IT





From SharePoint end-of-support to an increase in mergers and acquisitions globally and the wave of organizations deploying AI, 2025 was a perfect storm for IT teams.

The forces reshaping IT

2025 was a cloud crunch year. Three forces collided at once: a looming end-of-support (EOS) for legacy SharePoint on-prem versions, an unprecedented wave of mergers and acquisitions, and the rapid-fire rollout of Copilot and AI-driven security features that depend on clean data and strong governance to work safely.

Microsoft isn't just shipping AI tools at a breakneck pace. It's also investing heavily in the data-protection and governance controls that make those tools safe to use. Clean, well-labelled content and strong permissions move from best practices to prerequisites for Copilot and next-wave AI agents to work responsibly.

In short, the clock is ticking, workloads are multiplying, and every migration decision now has a compliance-and-AI twist.

We wanted to cut through the noise by asking the people on the front lines how they're handling it all. We surveyed hundreds of IT decision makers from mid-market and enterprise organizations across North America and Western Europe.

Together, their responses provide a clear picture of the current state of the Microsoft 365 cloud in 2025. What's migrated, what's still stuck, and where the pressure points are. We didn't stop at describing the state of play.

We asked Microsoft MVPs for their insights and advice on the challenges IT teams are facing, and we examined Microsoft's roadmap to see what's coming next.

The result is this book: data couched in expert context, so you're not just reading about 2025—you're equipped to plan, prioritize, and succeed in 2026.

You'll discover how hard deadlines, consolidation pressures, and AI adoption intersect; why teams' trust in Microsoft 365 still collides with governance and compliance hurdles; and where the most significant opportunities and risks hide.

Whether you're planning an on-prem-to-cloud migration or orchestrating a complex merger, treat these findings as your strategic guide for a year when every cloud decision carries extra weight.

A time of non-negotiable change

The clock is officially ticking. Support for SharePoint 2016/2019 ends in July 2026, so IT teams need to move business-critical content before Microsoft stops offering patches and other support. Our survey shows 78% of organizations still run these legacy versions, and nearly a third admit they have no clear migration plan. That alone would make 2025 a frantic year, but the looming deadline is only the first squeeze.

Our survey shows **78% of organizations** still run SharePoint 2016/2019, and nearly a third admit they have no clear migration plan.

Mergers and acquisitions add another layer of urgency: **80% of respondents are in the middle of, or bracing for, an M&A event within the next 24 months.** Tenant-to-tenant consolidations don't wait politely for EOS calendars. They stack on top, compressing already-tight timelines and amplifying security and compliance risks.

A whopping 82% of IT teams have Copilot either deployed or in pilot, yet many admit they're still untangling data-security and governance questions. Clean, neatly labelled content is the price of admission for generative AI. Migrations that once felt optional now sit on the critical path to achieving productivity gains, meeting regulatory compliance requirements, and fulfilling executive expectations.

In the chapters that follow, we'll unpack what these forces mean for budgets, risk, and opportunity. Using the insights from our survey, subject matter experts, and Microsoft's roadmap, we'll show you how to prioritize in a high pressure environment with multiple factors to balance. And because knowing isn't enough on its own, each chapter includes built-in tools, including checklists, scorecards, and frameworks, to help you immediately apply what you're learning.

Roles, regions, and industries

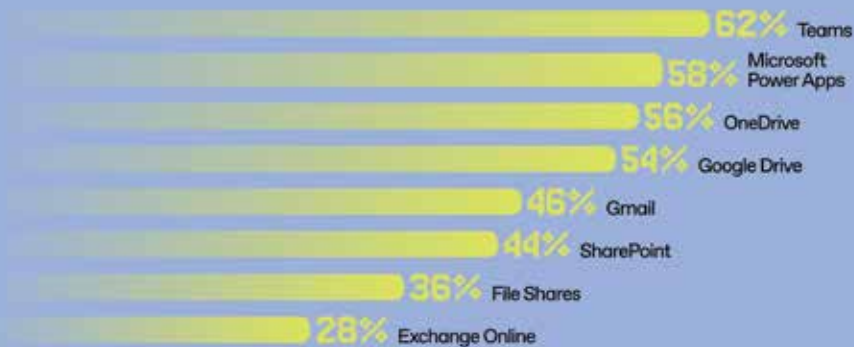
In March 2025, we surveyed 650 IT pros working in Microsoft 365. Every respondent has budget authority or hands-on responsibility for Microsoft 365. This means their answers reflect day-to-day realities rather than wish-list opinions.

Consider this section your “who’s who” primer before we dive into what these IT pros told us about upcoming deadlines, consolidation pressures, and AI ambitions.

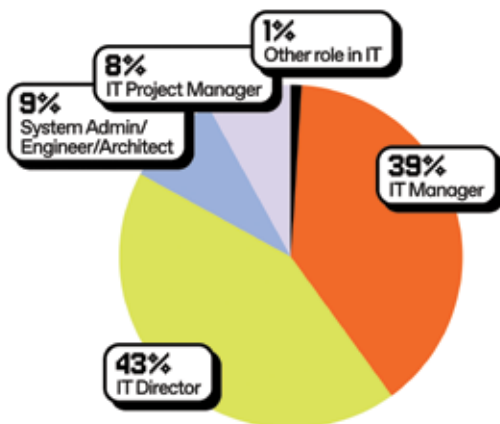
Our respondents span various IT roles, regions, and industries, yet their stories share a common thread: a limited runway and unlimited pressure to get cloud moves right the first time. This book picks up where their stories leave off, turning those realities into clear, actionable advice.

We translate raw numbers, expert perspectives, and Microsoft’s roadmap signals into practical guidance. So you get a 360-degree view of where things stand now and where they’re going next. You’ll come away with practical guidance to turn the major forces shaping IT in 2025 into a catalyst for a smarter, faster, and more secure transformation in 2026.

Types of workloads migrated



Role within the organization



Country of residence



Size of organization



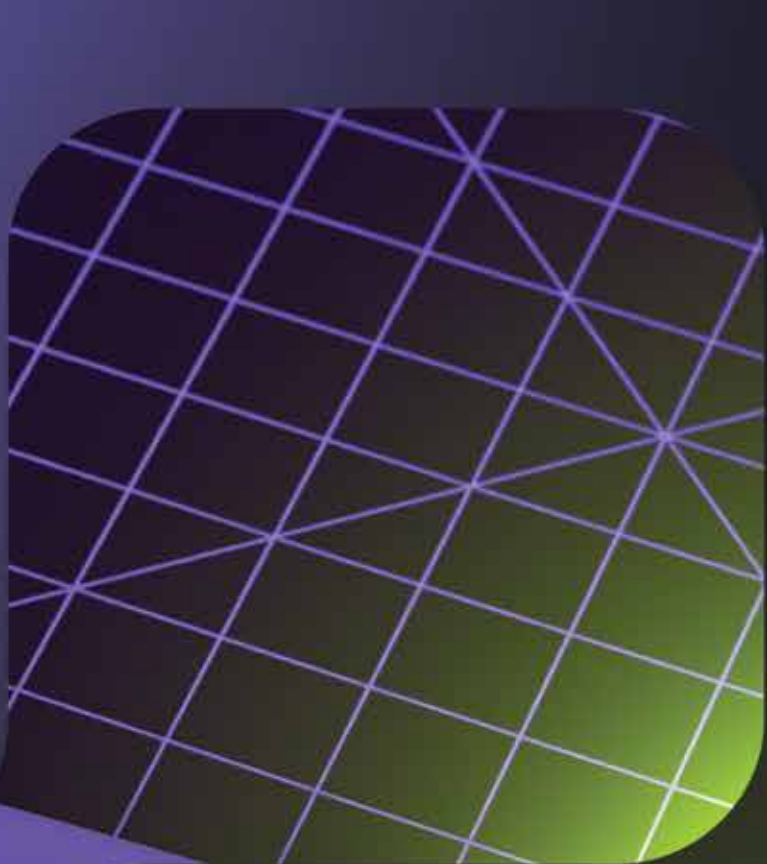
Industry



02

Migration momentum





Dig into fresh survey data on migration triggers, tooling gaps, and project timelines to build unstoppable momentum on your migration project. As you plan, remember the cloud you're landing in is evolving. Azure's next-gen infrastructure raises the ceiling on performance. Now migrations aren't just a move, they're an upgrade.

Migration momentum

The race to modern workspaces is uneven. While early adopters have embraced Microsoft 365, three-quarters of organizations remain anchored to on-prem versions of SharePoint despite end-of-support (EOS) now being in sight. The deadline isn't the only risk. Scalability, security, and cost pressures are piling up too.

Additionally, Microsoft is doubling down on AI-integrated productivity and tenant-aware agents, so your migration decision isn't just about the cloud versus on-prem debate anymore. Today, it's about whether your environment will support the next wave of Copilot and AI agents.

In this chapter, you'll see which triggers spark migrations, how native and third-party tools compare, and who actually signs off. These insights translate into benchmarks you can map to your own plan.

Think of your destination as a moving goalpost, in a good way. Azure's upgrades and Copilot's rise mean a well-planned migration does more than lift and shift. It future-proofs how your tenant performs and how people actually work.

Whether you're building an internal business case or fine-tuning a project already in flight, the insights here will equip you with a clear, evidence-based roadmap for moving forward.

Why are organizations migrating right now?

Three pressures top the agenda right now: EOS deadlines, budget and security scale needs, and M&A. However, because M&A migrations have such a unique set of challenges, we devoted the next chapter to them.

First, let's dive into SharePoint on-prem EOS.

Migrating from SharePoint 2016 or 2019 to SharePoint Online before support ends

In July, 2026 Microsoft is ending extended support for SharePoint 2016 and 2019. This means Microsoft will stop delivering security patches, bug fixes, and help-desk support.

From that day forward, every fresh vulnerability remains wide open, making on-prem farms a low-effort target for ransomware. Microsoft is putting AI-powered security and threat detection front and center, so we'll be hearing lots about defending the perimeter where attackers try to exploit exactly those gaps.

But breaches aren't the only price of inertia:

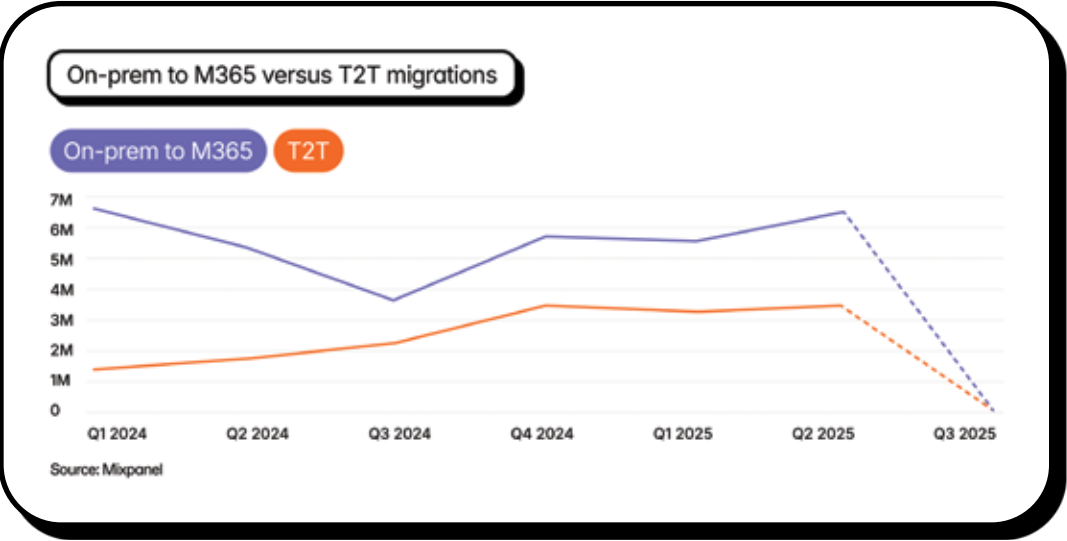
- **Cyber-insurance premiums spike**—or coverage is denied outright—when critical workloads outrun vendor support.
- **Compliance audits** flag unsupported environments under ISO, NIST, HIPAA, and others.

A move to the cloud hands patching, threat response, and certification maintenance back to Microsoft, giving your organization an evergreen security posture by default.

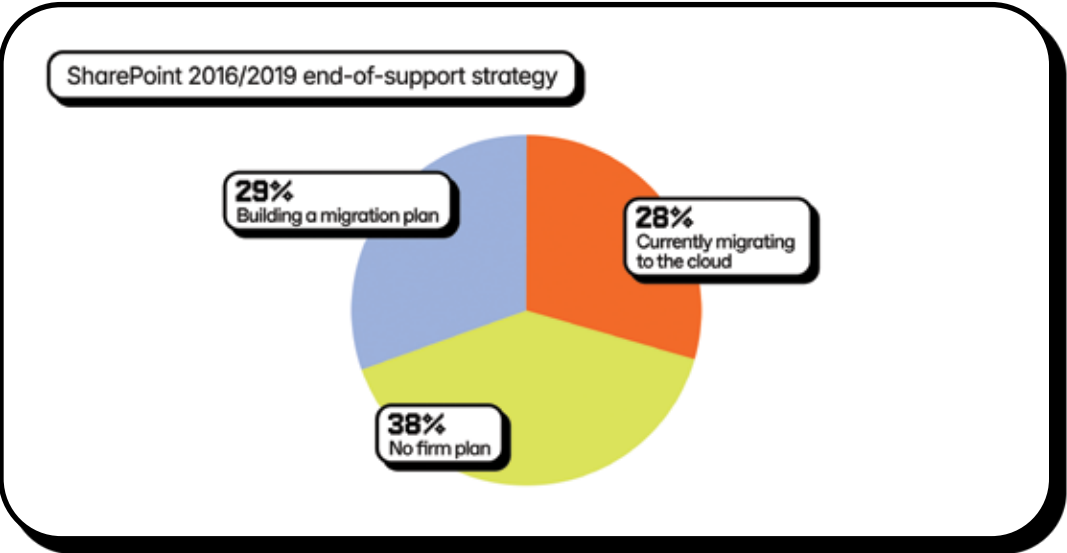
And with Azure's infrastructure upgrades coming online (better compute, new VM/network features), the target environment may soon outperform many on-prem setups.

Microsoft has been talking about SharePoint on-prem EOS since 2022, and **96% of our survey respondents said they knew about the quickly approaching date**. We've already seen on-prem migration activity climb in ShareGate usage data, matching the market's early moves away from SharePoint 2016/2019.

Among ShareGate customers, there had initially been a slow but steady decrease of on-prem-to-cloud migrations in the past few years. However, there was a steep uptick of on-prem-to-cloud migrations starting in Q3 of 2024, and it's continued to rise throughout 2025.



And yet, 66% of organizations still run **critical workloads** on at least one of these versions in production, and more than a third don't have a migration plan.



This lines up with what Ian Loman, Cloud Expert at the consultancy Adepteq has seen: “What we often see is that it's such a complex environment that people get scared of it. So, it gets pushed down the road because it's going to be a big project. And it's going to need buy-in from senior leadership, budget, and additional software or professional services to assist because the internal team won't have the skills to do it.”

It might also not just be the logistics that Ian mentioned. Microsoft MVP Sarah Haase pointed out it could also stem from compliance concerns:

“If they already have a lack of compliance where they are, migrating to the cloud requires a huge funding load. Not to mention subject matter expertise or even more funding to pay consultants to help them get there. A lot of companies can't even imagine a bridge path from where they are on-prem to being secure and compliant in the cloud.”



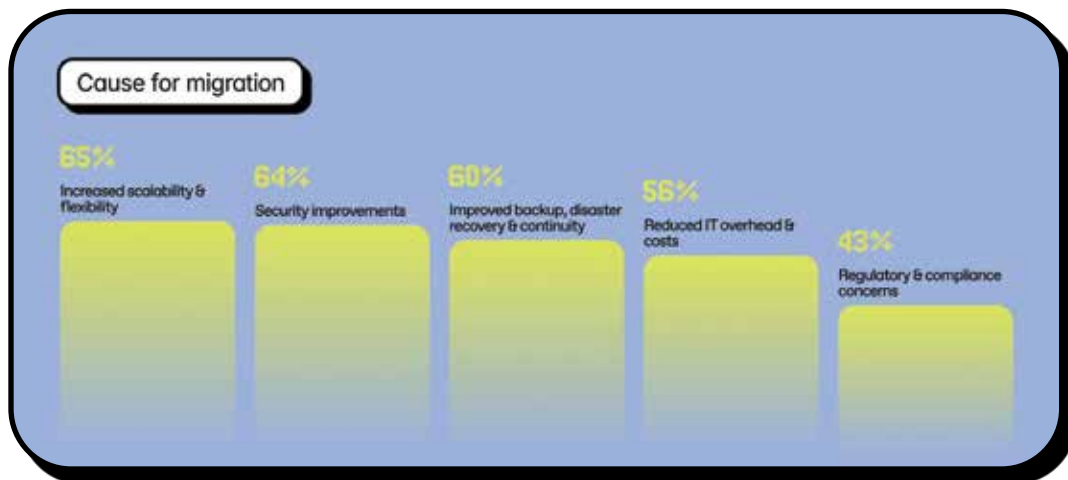
Sarah Haase
Microsoft MVP

If you're in that group of 38% without a plan, take a deep breath and tackle one thing at a time. The safest, most cost-effective migrations are the ones that start now.

- 1 **Run a system audit and risk assessment** – Inventory sites, custom integrations, and security gaps, so you can build a comprehensive migration strategy.
- 2 **Decide on your upgrade path** – We recommend migrating to SharePoint Online for collaboration and evergreen security. You may need to keep specific data on-prem, which you can move to SharePoint Server Subscription Edition. But even then, we still recommend using a hybrid model with most of your data in the cloud.
- 3 **Draft a detailed migration plan** – Map milestones, budgets, stakeholder comms, and, where needed, certified partners to keep the project on track.

Other migration triggers in 2025

Alongside the extended support deadline, our data shows day-to-day operational pressures build real momentum for change, too. A few business-critical factors formed the core of nearly every migration business case:



Each driver originates in a different corner of the org chart—growth from business leadership, security from risk teams, savings from finance—yet they converge on the same solution: a modern, cloud-first Microsoft 365 environment.

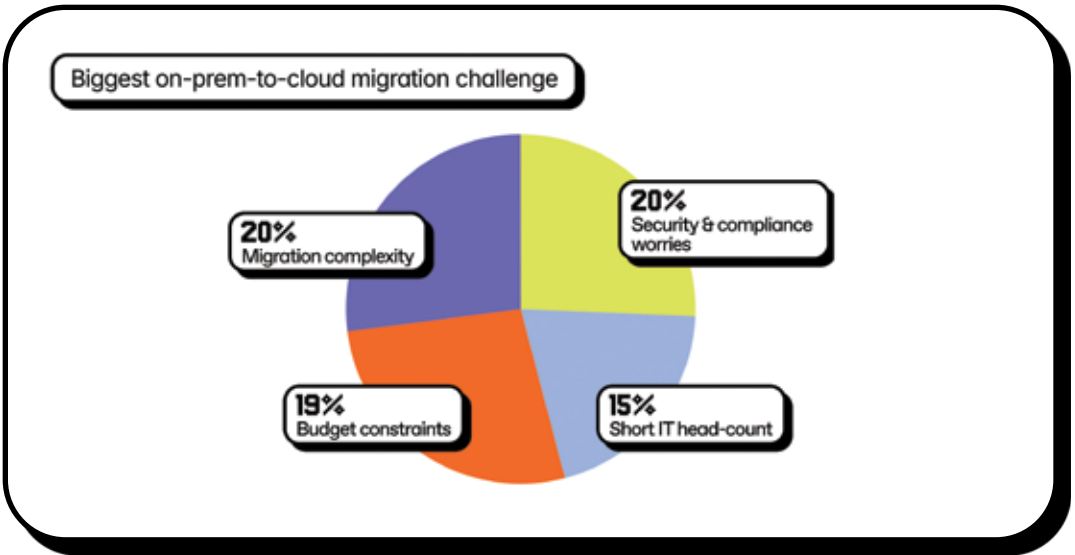
It's a good reminder that migration isn't always because of a big event. It's often a continuous process to keep up with how your organization and the cloud are evolving.

"Migration isn't a one-time thing, it's ongoing. It's a change management activity. Teams reorg, business changes, structure changes."



Christian Buckley
Microsoft MVP

Our survey also surfaced a predictable set of speed bumps that teams encounter once the project is underway. Factors that can quickly stretch a modest timeline into a costly slog.



While no single obstacle dominates, together they explain why even well-funded teams can lose momentum without a structured approach. The antidote is a program-level mindset:

- 1 **Secure executive sponsorship early.**
- 2 **Lock in budget.**
- 3 **Front-load discovery work.**
- 3 **Enlist proven tooling.**

With the deadline marked on the calendar, the next question is obvious: which tools will actually get the job done on time and be ready for tomorrow's Azure infrastructure?

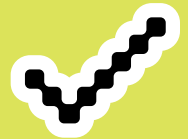
Azure infrastructure is leveling up. Microsoft has announced new performance-optimized VM SKUs, accelerated networking, and infrastructure designed to handle AI-scale workloads. This increased capacity means your migration target isn't static. Plan for growth, not just parity.

Your quick gut check on migration readiness

You've just seen the big migration triggers, from SharePoint EOS deadlines to the everyday grind of scalability, compliance, and cost pressures. The next step is figuring out how ready you are to migrate.

If you're mid-project, use this to find blind spots. If you're just starting, use it to see where to focus first.

Question	Not at all	In progress	Fully in place
1. Do you have a current, validated inventory of all customizations, integrators, apps, and site counts in your source?	0	1	2
2. Have you identified all security, compliance, or regulatory constraints that will affect your target tenant?	0	1	2
3. Have you estimated the bandwidth, network, throttling, and delta volumes for your migration window?	0	1	2
4. Is executive sponsorship and budget already secured?	0	1	2
5. Do you have a selected migration tool or partner stack?	0	1	2
6. Do you have a rollback, incremental copy, or delta-cutover strategy defined, along with contingency for downtime?	0	1	2



Scoring

0-4

High risk

5-8

Moderate risk,
needs validation
and tightening

9-12

Ready to accelerate
with confidence

Next steps

High risk

Pause and address gaps in discovery, security, and stakeholder alignment. Don't commit to tool purchases or migration scope until you close more than 50% of these to 1 or 2.

Moderate risk

You have some groundwork, but expose assumptions via pilots. Validate tool fit, get expert advice, and test blocker removals.

Ready to accelerate

You're in good shape. Refine your scale strategy, compare advanced tool capabilities, and secure partner commitments or add-ons.

Microsoft 365 migration tool usage trends: Power tools vs. hand tools

Before you can sprint toward the cloud, you need the right gear. We examine who's leaning on Microsoft's native utilities, where third-party platforms break through, and how satisfaction levels stack up.

The default first stop: Microsoft's own toolkit

Native tooling buys quick wins and executive approval because "it's the free option!" Plus, it's already whitelisted and backed by official documentation.

No wonder our survey found that **70% of IT pros have used Microsoft's native migration tools** on past Microsoft 365 migration projects.

But their limitations can introduce hidden costs from increased labor, project delays, and migration gaps. Understanding where the free tools stop scaling is the first step to choosing a stack that keeps momentum up instead of stalling it.

Native tools can handle small lift-and-shift scenarios, but they tend to come up short when projects grow or when teams lack migration experience and technical capacity for complex scripting. For large file volumes that trigger throttling or if metadata and permissions need to be preserved, teams need to re-evaluate.

With Microsoft's focus on multi-model Copilot support (e.g., Anthropic + OpenAI) and agent-based data flows, migration pipelines need to be architected for agility, not just brute-force lifts.

Yet IT pros running a SharePoint EOS migration still plan to use native tooling more than leveraging third-party tools or partners:

SharePoint 2016/2019 migration resource plan

48%

Microsoft native tools

22%

Third-party tools

21%

Partners

This is very different compared to M&A migrations, for which 87% of respondents said they were planning to involve partners. We'll dive into that more in the next chapter.

We asked Microsoft MVP Andy Huneycutt about the difference in IT teams' willingness to get external help for SharePoint EOS migrations. In his view, it's a common problem:

“Moving from on-prem to the cloud is a much bigger jump than people think it is. You're changing the way people access, store, and permission information.”



Andy Huneycutt
Microsoft MVP

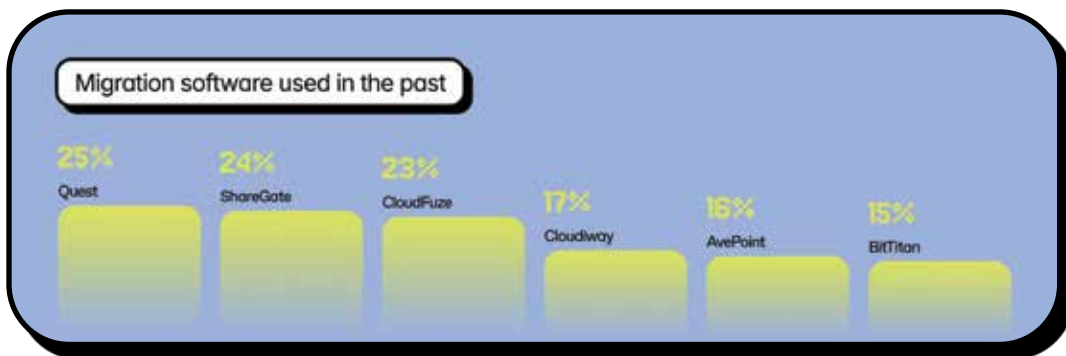
Even “plain” EOS migrations often involve more change than people anticipate:

- Retiring custom farm solutions and modernizing sites
- Re-mapping permissions and metadata for zero-trust policies
- Re-architecting information architecture for Teams and Copilot readiness

Keep in mind that native tools can move content, but they rarely control it after it lands. As soon as new workspaces appear—and Copilot crawls them—security, compliance, and lifecycle rules become the next bottleneck. In the chapter *Who's governing Microsoft 365?* we see how the same tool decisions surface again.

Third-party migration tools: Analyzing a fragmented landscape

Once teams outgrow Microsoft's free utilities, the field splinters.



Why the fragmentation? Feature depth and pricing models vary wildly. Some tools bundle certain workloads while others gate essential capabilities behind per-gigabyte fees. IT pros feel they have to use multiple platforms rather than converge on one universal standard.

User sentiment is good, but not great. Half of respondents said that they were very satisfied (50%) with their tooling experience, while another 42% were only somewhat satisfied. That leaves 8% neutral or dissatisfied—small but telling when migrations carry tight deadlines and high stakes.

Reliability—day-in, day-out performance that teams can trust—is often the difference between “good enough” and truly great. It’s this next-level ability that separates standout vendors from the pack.

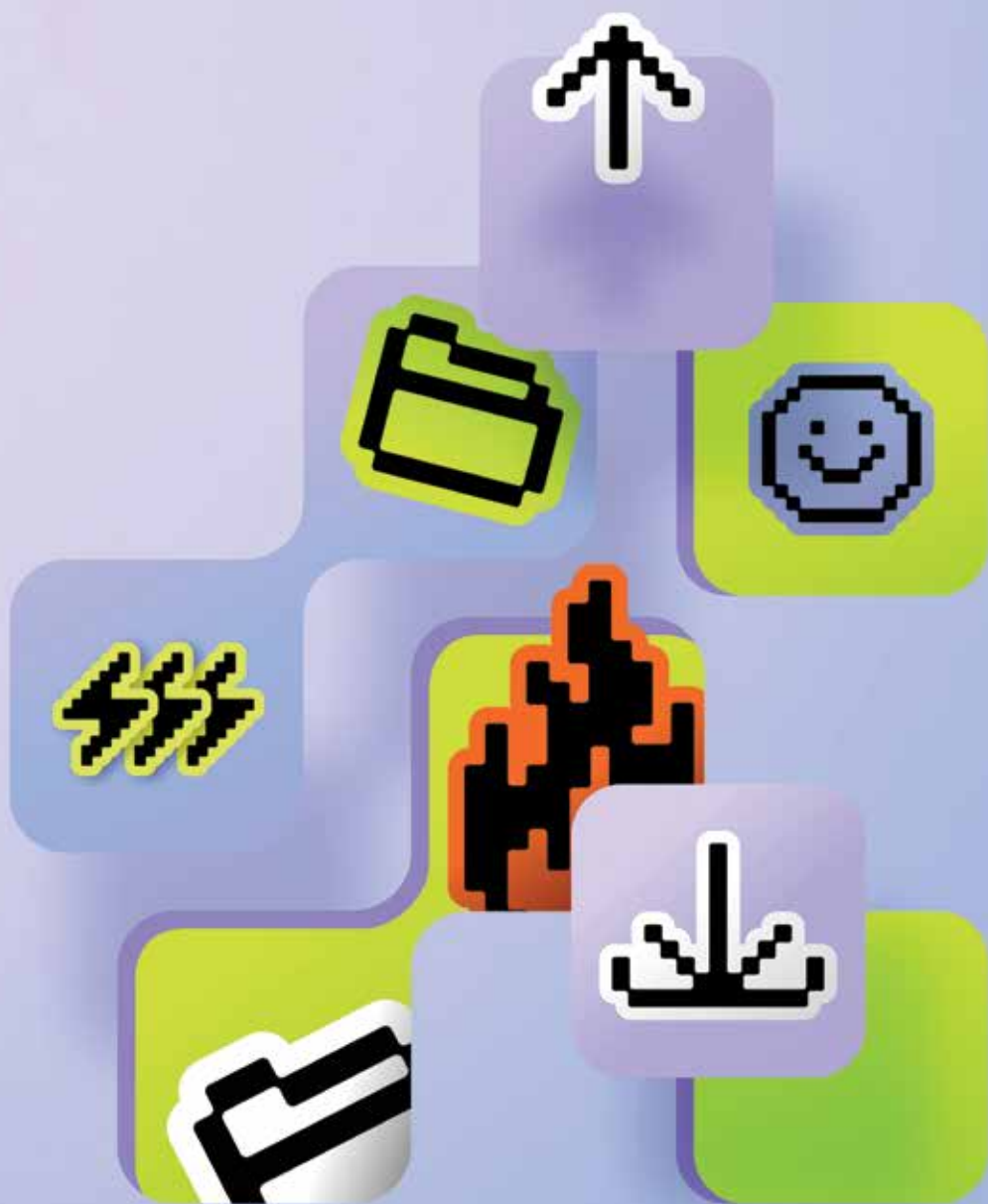
With the need to accelerate so many migration timelines we expect those seeking out third-party tools will lean towards solutions with:

- Transparent, all-in pricing
- Cross-workload coverage
- Accelerated and reliable migrations

“It’s always better to test with native and third-party tools early in the planning process. This helps avoid discovering complexity or scaling challenges later in an already stressful migration. It often makes it easier to see just how much another tool can accelerate the migration.”



Richard Harbridge
Microsoft MVP



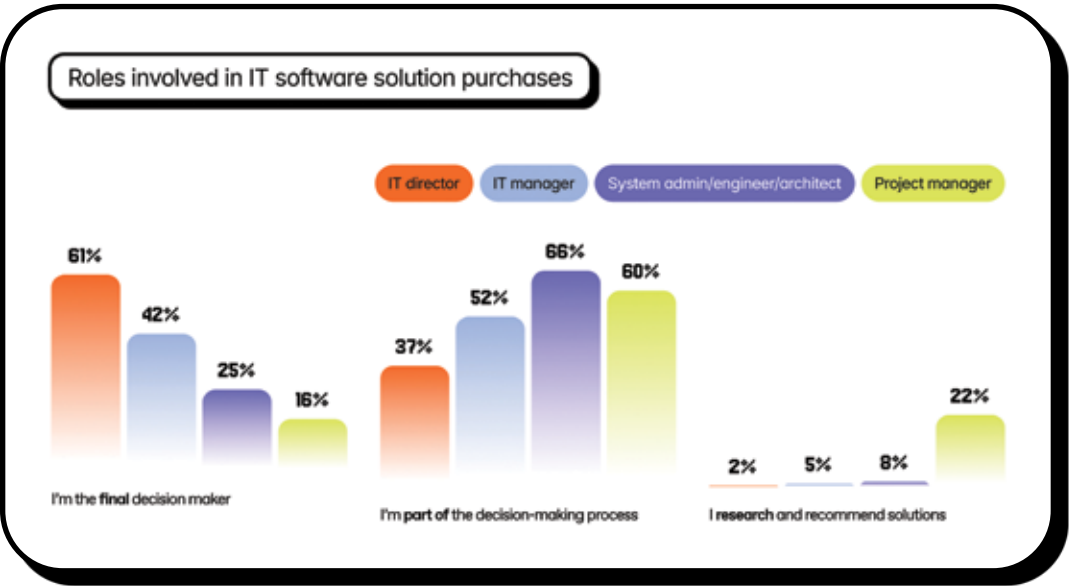
From approval to completion: Microsoft 365 migration benchmarks

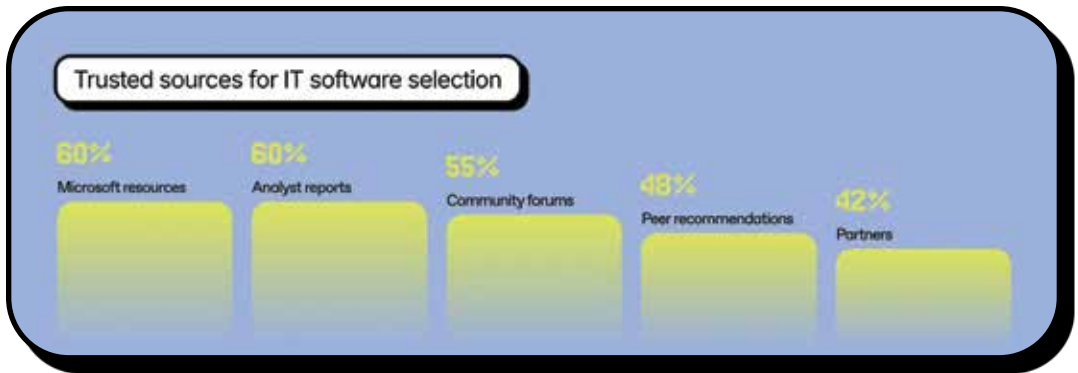
Powerful tools work best when paired with clear roles and processes. This section looks at who actually signs off and which recommendations hold the most sway.

Treat these insights as a checkpoint for your own stakeholder map and scheduling assumptions before you lock in budget and scope.

Decision desks: Managers, directors, and deadlines

Most projects are championed by the operational leaders who actually understand and work in Microsoft 365.





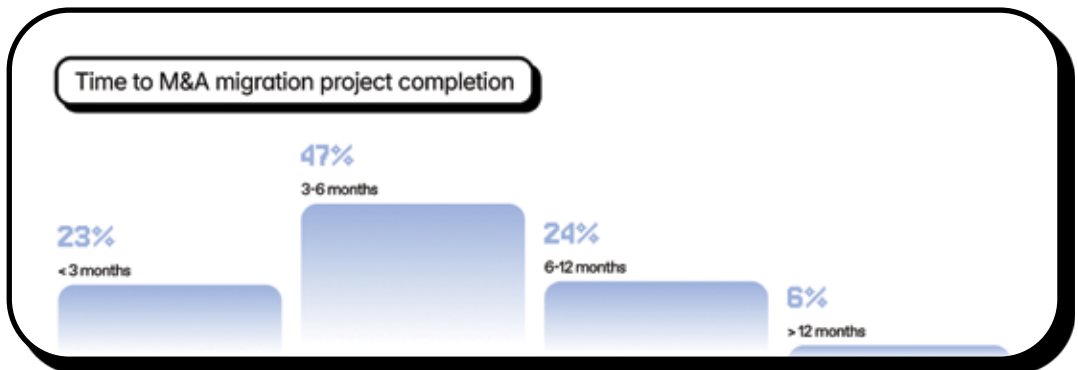
When you present tooling proposals, bring leadership clear discovery data—site counts, customizations, risk hotspots—so they can approve scope and budget with confidence.

Curate links to Microsoft white papers and Gartner or Forrester notes to back up your numbers. Then add peer forums to prove the pain points are real.

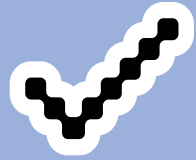
You can also leverage the sources leadership already trusts to make your case.

Timeline benchmarks to sanity-check your plan

All migrations are different, but you can use this data as a benchmark in your planning.



Something that isn't visible in the above chart? Projects that stretch **beyond a year** last an average of **21 months**. To stay on track, scope out your project thoroughly and set milestone-based funding gates. Vendor payments can even be tied to those checkpoints.



SharePoint migration checklist

Every successful SharePoint migration, whether a single site or an entire enterprise environment, starts with planning. This is the step that sets the tone for the whole migration. Here's the full planning section from our expert checklist to get you started.

Plan your migration

- ☐ **Decide on your approach**
Phased, single-event, sequenced, or concurrent.
- ☐ **Identify risks early**
Build a migration schedule with clear milestones and ownership.
- ☐ **Run a source analysis**
Understand environment size, sites, file shares, workflows, and potential issues.
- ☐ **Check your dependencies**
Customizations, workflows, authentication methods, and permissions.
- ☐ **Define success criteria**
Metrics for timing, accuracy, and user experience.
- ☐ **Assign owners**
Give someone responsibility for each stage of the plan.



Want all seven stages of our SharePoint migration checklist?
Scan this QR code.

Key lessons from the data

For a lot of people, migration is a race against the clock. But it's a race you can win with early discovery, the right mix of tools, and clear decision-maker alignment.

Three data-backed actions rise to the top:



Set your finish line now.

70% completed their moves inside six months. Map this onto your own scope and build a buffer into your roadmap now rather than later.



Match your tools to the project's complexity.

While nearly half (48%) of teams plan to rely on native tools, the reality is that most projects need more power. Bring in third-party software and partners to customize, re-map permissions, or modernize without derailing your timeline.



Give leaders evidence, not opinions.

Budget requests land better when grounded in the sources decision-makers already trust.

Leaders turn to partners far more readily for M&A migrations. It's a clear signal that playbooks shift when legal timelines and tenant consolidation collide. We'll dive into that next.

03

M&A migrations by the numbers





Tenant-to-tenant migrations are on the rise, and they bring a unique set of challenges and opportunities with them.

M&A migrations by the numbers

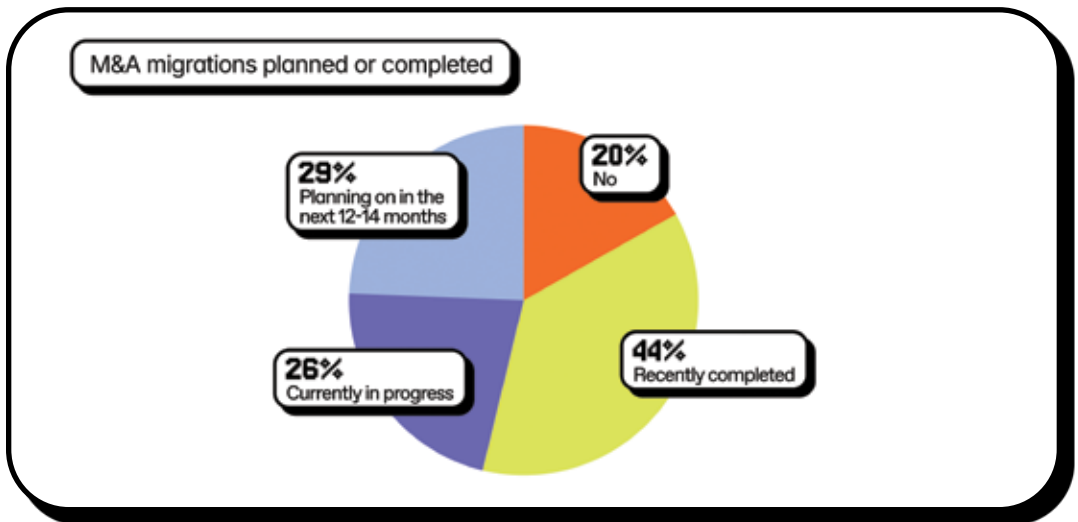
Every acquisition, merger, or divestiture sets off a high-stakes game of tenant-to-tenant Tetris where IT leaders must precisely align security, permissions, and strict timelines. For IT leaders, the pressure is real: keep the business running, keep the data locked down, and keep the CFO from fainting at unexpected costs.

In this chapter we'll analyze what makes M&A migrations uniquely difficult, spotlight the early decision points that can make or break the project, and map out how partners fit in.

The prevalence of M&A tenant moves

One of the most telling insights from our entire survey was around M&A migrations: **80% of organizations** have either completed one recently, are tackling one right now, or have one lined up within the next two years.

M&A migrations are now the rule, not the exception.



Why the surge?

- **Cash is back on the table.** Morgan Stanley reports that in 2025 \$3 trillion in unspent capital was waiting to be deployed and will drive a rebound in M&A activity.
- **IT delivers the quickest synergies.** Microsoft guidance notes that consolidating tenants after a deal reduces overhead and improves the collaboration experience.
- **Regulators are watching.** GDPR fines have passed €5.65 billion, and 43% of IT pros say compliance deadlines are a direct trigger to start a tenant-to-tenant move.

What it means for IT teams

Deal volume is rising. Now let's see what happens when those deals land on IT's desk.

- 1 **M&A readiness is no longer optional.** Even if you're in the 20% without an imminent deal, the data says odds are high you'll face one soon.
- 2 **Back-to-back projects are common.** The near-even distribution across past, present, and future buckets hints at a revolving door of consolidation activity.

Bottom line: This 80% figure is more than a statistic. It signals a fundamental shift where M&A migrations are now part of the day-to-day workload of IT teams rather than a rare, one-off event. Teams that have a repeatable playbook, automate the tedious bits, and pick their tooling early are the ones that come through each deal smoothly.

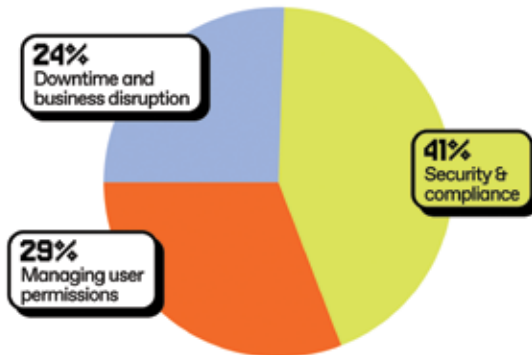
Amplified pain points in M&A migrations

While every migration has its own challenges, an M&A project acts as a magnifying glass, dramatically amplifying specific pain points. The concern for security, which we saw as a driver of migrations in the previous chapter, is a prime example. In an M&A context, it transforms into the undisputed number one challenge, cited by more than double the share of respondents compared to an on-prem-to-cloud migration.

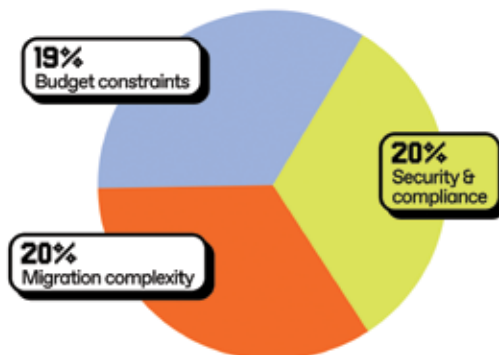
While security is the number one challenge for both types of migrations, the share of respondents who call it the biggest challenge doubles in an M&A context (41% vs. 20%). This underscores the heightened scrutiny when two security frameworks collide.

Permissions and downtime stand out as distinctly M&A-intensified worries. For example, in an M&A context, the challenge of managing user permissions increases substantially compared to on-prem-to-cloud migrations, where logistical hurdles like budget and complexity are more prominent.

Biggest M&A migration challenge



Biggest on-prem-to-cloud migration challenge



Two (or more) tenants, one security posture

Security drives every major decision in an M&A migration. More than a quarter of respondents (28%) rank security and compliance features as the single most important factor when picking a migration tool, ahead of accuracy, speed, or price.

Before any data moves, 62% insist on compliance validation, while another 20% say they'll delay or cancel the project if those risks aren't addressed. In other words, security isn't a checkbox at the end of the plan. It's the gate every other milestone has to pass through.

Security is also a springboard for whatever comes next.

“During mergers and acquisitions, many organizations need to rapidly develop a data integration plan. In the rush, it's easy to overlook that this migration represents a critical opportunity to securely handle data and build the basis of future readiness for Copilot. These key factors don't just happen in the background. They need a clear path, particularly when merging technical environments in M&A situations. The right strategy should turn migration into an opportunity.”



Richard Harbridge
Microsoft MVP

The permissions puzzle of M&A migrations

Managing permissions was rated as the top challenge in M&A migrations by **29% of respondents**. It makes sense: instead of one directory, you have two (sometimes more) Microsoft Entra ID tenants full of duplicate UPNs, nested groups, and conflicting retention holds. Any mismatch can leave users locked out of key workloads or, worse, over-privileged in a tenant they weren't meant to access.

As Microsoft MVP Andy Huneycutt warns:

“If you just do a lift-and-shift, there’s a world of technical debt pain waiting for you on the other end.”



Andy Huneycutt
Microsoft MVP

The fix starts with discovery. You need to map every user, group, and role early and watch for clashes, especially shared mailboxes, service accounts, and stale guests.

Next, decide how you’ll merge identities: consolidate into a single directory, maintain a long-term B2B setup, or adopt a hybrid model while legal integration finishes. Each path affects how permissions are migrated and how long coexistence tooling needs to stay in place.

Now, you also have to anticipate integration with Microsoft’s emerging identity services like Cross-Tenant Identity Mapping, currently in preview. That means your tooling should tie into Microsoft’s identity model while supporting the flexibility that exclusive tools bring.

As migrations scale, your map has to hold metadata, RBAC, and lifecycle context without breaking under new cloud demands.

Even as Microsoft simplifies identity mapping, Microsoft MVP Sarah Haase reminded us that the trust issue with imported data doesn’t go away:

“If you’re ingesting data from another company, it is inherently less trusted than data that had been in your SharePoint on-prem environment. How are you going to label and secure terabytes of data that you’re bulk moving into your tenant?”



Sarah Haase
Microsoft MVP

ShareGate’s Permissions matrix report¹ gives you a live snapshot of who can see what across both tenants, then lets you remediate gaps or overlaps. You can migrate permissions, sensitivity labels, metadata, and version history with ShareGate, so users land in the new tenant with the same access they had five minutes ago.

Whatever tool you use, test-drive the new access model. Validate MFA prompts, access policies, and external-sharing settings in a pilot, not just on a spreadsheet.

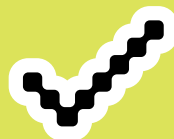
¹ sharegate.com/features/sharepoint-reporting-and-permissions-management

Are your permissions ready for an M&A shake-up?

The hardest part of permissions isn't moving them. It's knowing what you're moving in the first place. From UPN conflicts to service accounts, there are a dozen ways to get it wrong.

The scorecard will help you spot those cracks early and give you a clearer sense of where to focus.

Question	Not at all	In progress	Yes
1. Do you have a complete inventory of users, groups, and roles across both tenants?	0	1	2
2. Have you identified duplicate UPNs and put a resolution plan in place?	0	1	2
3. Do you know which retention policies or holds will collide once the tenants merge?	0	1	2
4. Do you have a way to see live permissions across both tenants so you can spot conflicts early?	0	1	2
5. Have you identified and planned for service accounts and automated jobs that rely on current tenant permissions?	0	1	2
6. Have you reviewed admin roles and RBAC assignments across both tenants?	0	1	2



Scoring

0-5

Permissions hangover incoming

Brace yourself. Without better prep and tooling, access chaos and user frustration are almost guaranteed.

6-9

Handle with care

You've got a lot covered, but there are weak spots. Shore them up before cutover to avoid ticket overload.

10-12

Permissions pro

You're in great shape. Your users should land in the new tenant with confidence and without drama.

Keeping the lights on during M&A

Unlike a migration triggered by SharePoint 2016/2019 end of support (EOS) or modernization, M&A migrations typically have hard deadlines. There's no wiggle room for a maintenance weekend when legal clauses, auditor sign-offs, and investor calls all hinge on a hard cutover.

The cost of failure scales fast. A few hours of outage during a tenant-to-tenant cutover can stall revenue-generating systems, delay integration milestones, and erode employee confidence at the very moment leadership is promising "business as usual." That's why 24% of IT pros listed downtime as their top M&A migration challenge.

One way to mitigate business disruption is to stage migrations in incremental waves: do a pilot migration, copy the bulk of your content, and then execute delta cutovers as needed. ShareGate's incremental copy² makes it simple by letting you rerun jobs for only what changed while preserving metadata and permissions. It's designed to align with evolving Azure throughput and delta-changes, so your waves can flex as Azure limits, batching, or transfer lanes shift.

Solutions and partners: Picking your M&A toolkit

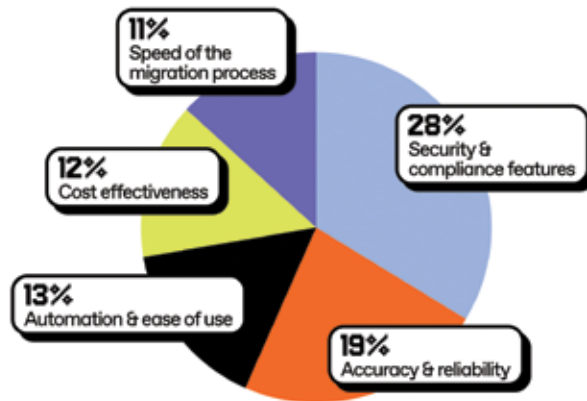
Most IT teams don't wait to pick their migration arsenal. In this section, we'll unpack when these decisions happen, which features tilt the scales, and how partners are involved—setting you up to benchmark (or rethink) your own approach.

Early birds and security nerds

The window for choosing a migration tool during an M&A closes fast. More than half of all IT teams (55%) make their selection before the merger even closes. Add to that the 37% who choose a tool within six months, and a staggering 92% of organizations have their migration solution locked in almost immediately after a deal is signed.

This front-loaded decision-making process leaves very little time for lengthy evaluations, often forcing a choice while due-diligence work is still unfolding. Considering security and compliance is noted as the top challenge for M&A migrations, it's no wonder that IT pros prioritize a migration solution with top-notch security features.

Most important factors for M&A migration tools

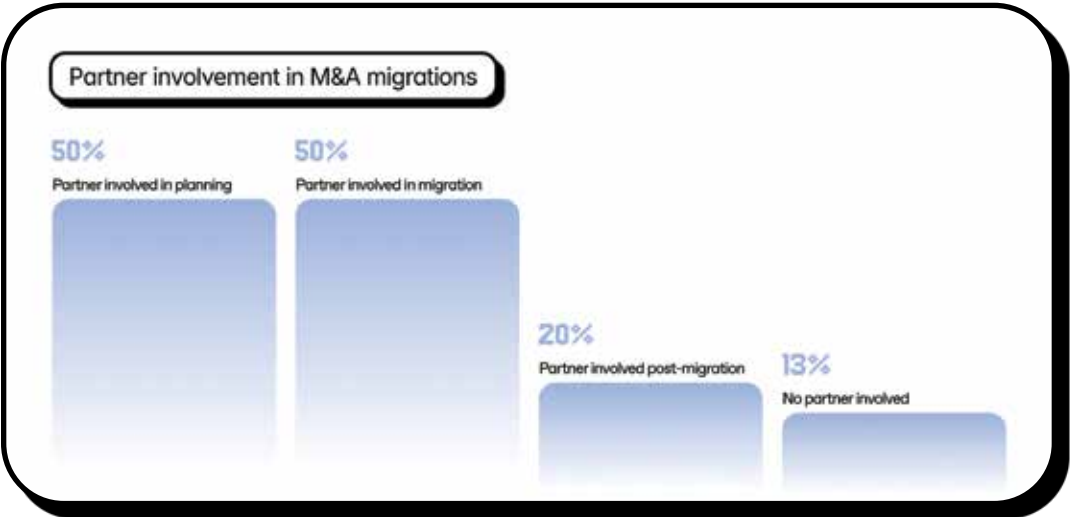


For IT pros scoping their own stack, that means front-loading a security review. Look for Microsoft Purview sensitivity label migration, granular permissions mapping, and audit-ready reporting. ShareGate, for example, ticks those boxes³ while offering flat licensing that's easy to approve. Make sure whichever tool you choose clears the security bar first.

Another factor to consider is how Microsoft's roadmap for Azure's infrastructure will evolve with transfer pipelines, Azure Blob queue usage, and throughput. Your choice of tool has to not only map permissions but also optimize alignment with Azure's evolving transfer architecture.

³ sharegate.com/blog/simplify-sensitivity-label-migration-in-microsoft-365
sharegate.com/blog/sharepoint-migration-tool-user-mapping-and-permissions-metadata
sharegate.com/reporting

Bringing in backup: The partner factor

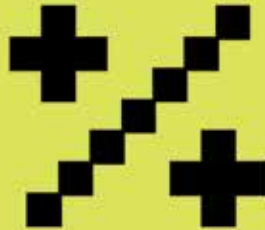


Navigating an M&A migration alone is almost unheard of: **87% leverage partners.**

Tenant-to-tenant projects pile on discovery workshops, after-hours cutovers, and governance cleanup. Work that’s easier with extra muscle and proven playbooks.



87



of respondents
**leverage
a partner**

before,
during
and/or
after
an M&A
migration.



Partner fit checklist

Is your migration partner the right one for your M&A project?

- ☐ Has your partner successfully handled tenant-to-tenant migrations tied to M&A in the past two years?
- ☐ Do they run a pre-migration discovery workshop (covering users, groups, permissions, and workloads)?
- ☐ Are they up to speed on Microsoft's latest building blocks, like cross-tenant OneDrive migration, SharePoint site migration (preview), and Entra cross-tenant sync?
- ☐ Can they support after-hours or weekend cutovers without leaving you short-staffed?
- ☐ Do they deliver audit-ready reporting to keep regulators, auditors, and your CFO calm?
- ☐ Will they stick around for post-migration cleanup (permissions, governance, and adoption), or do they disappear once the cutover is done?



If you need a short-list of expert partners with great migration knowledge, ShareGate can connect you with certified partners⁴.

Key lessons from the data

When a merger or acquisition enters the picture, the standard migration playbook gets a complete rewrite. The data shows these high-stakes projects are the new normal, demanding more speed, tighter security, and a different strategy from day one.

Three actions rise to the top:



Build a repeatable M&A playbook.

With 80% of organizations involved in an M&A migration, these projects are no longer one-off events. Having a process and a pre-vetted toolkit is the best way to avoid scrambling under pressure.



Make security your non-negotiable first step.

Risk multiplies in an M&A context, with security concerns doubling compared to on-prem moves (41% vs. 20%).



Don't go it alone.

Your peers overwhelmingly agree that outside help is crucial for these high-stakes projects. Follow their lead to get the expert capacity needed to handle discovery, cleanup, and business downtime mitigation.

In the following chapter, we'll delve into how organizations harden their Microsoft 365 environment post-migration, from threat protection to continuous compliance monitoring.

04

The security paradox: A data-driven look at Microsoft 365





Explore the paradox of high confidence versus high caution in Microsoft 365 security. Learn how to prioritize controls, justify budget, and streamline day-to-day security tasks.

The security paradox: A data-driven look at Microsoft 365

In previous chapters, we saw that security is a foundational pressure driving all modernization projects. Throw in the high-stakes environment of an M&A, and it gets elevated to the single most dominant challenge.

This raises a crucial question: if everyone agrees that security is paramount, why is there so much debate on how to achieve it? We'll dive into the data that reveals how the concern for security can lead teams to opposite conclusions. From there, we'll give guidance on how to navigate these conflicting views to build a security posture you can defend.

Compliance deadlines are now migration deadlines

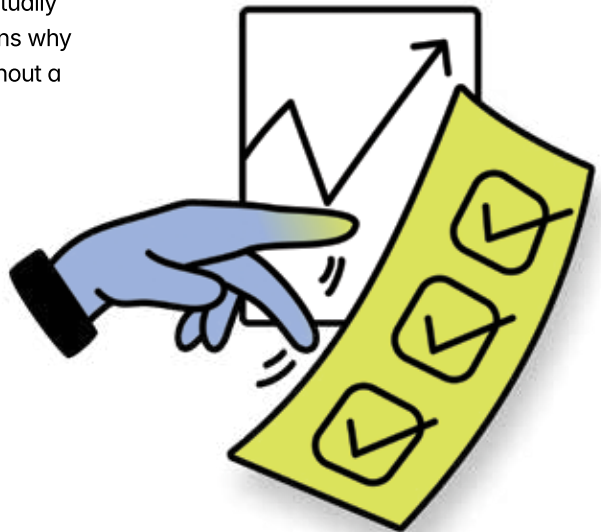
Compliance isn't waiting for anyone. Hard deadlines—from data-privacy updates to sector-specific rules—are forcing teams to lock budgets and prove controls fast.

Regulations write the roadmap

New or updated rules aren't just background noise. They set the schedule. Our survey shows that regulatory change is the single biggest trigger pushing security work forward.

Even vendor dates can act like law: the **July 2026 SharePoint 2016/2019 EOS** (discussed further in the *Migration momentum* chapter) effectively becomes a compliance deadline because unpatched software violates frameworks like HIPAA and ISO.

Security and compliance land on the same to-do list: auditors want proof that controls exist while security teams want proof they actually work. Same risk, two labels. That explains why pressure rises even in organizations without a formal regulatory trigger.



Regulation-to-action scaffold

This framework is built for partners.

Consultants, VARs, and SIs who step in when compliance pressure meets migration urgency. Use it to structure engagements around regulatory or vendor-driven deadlines, demonstrate value to clients, and deliver audit-ready outcomes that build trust.

Make this process scalable with repeatable templates and automation—like ShareGate's Governance risk assessment⁵—to shorten delivery.

Scope

- Provide structured, partner-led services that align Microsoft 365 migrations with regulatory and vendor deadlines.
- Focus on reducing client risk by validating compliance controls, documenting evidence, and executing migrations on schedule.

Inputs (from client + environment)

- List of applicable regulations/frameworks (GDPR, HIPAA, ISO, SOC 2, etc.)
- Vendor support deadlines (e.g., SharePoint 2016/2019 EOS in July 2026)
- Client's current audit reports and known compliance gaps
- Inventory of workloads (SharePoint, OneDrive, Teams, Exchange, on-prem systems)
- Approved migration tooling (permissions mapping, sensitivity label support, audit logging)



Outputs (delivered to client)

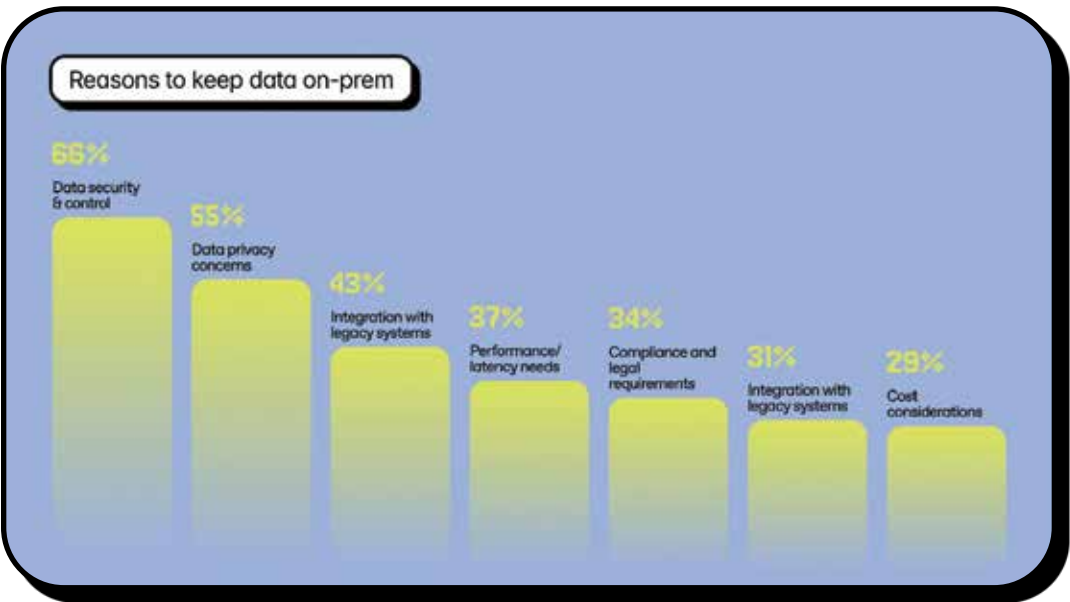
- Compliance gap analysis with prioritized remediation items
- Deadline-driven migration roadmap with clear milestones tied to regulatory dates
- Audit-ready validation package (before/after permissions reports, sensitivity label carryover, compliance sign-offs)
- Documented control map: how Microsoft 365 + partner services + migration tooling satisfy compliance requirements

Success criteria (partner + client)

- Client achieves compliance sign-off before migration cutover.
- Migration completes ahead of regulatory/vendor deadlines with no major audit gaps.
- Post-migration evidence package delivered to auditors and leadership.
- Partner engagement demonstrates measurable risk reduction, strengthening long-term client relationship.

High stakes, low cloud uptake

The pressure is sharpest in heavily regulated sectors where cloud adoption lags. Only 22% had fully moved to the cloud while 78% still had at least some data on-prem. The main reasons people cited staying on-prem was due to data security and data privacy concerns.



That caution has a price. Deadlines like the July 2026 SharePoint cutoff effectively force the hand of any organization that has to comply with regulatory standards. These teams are pushed to modernize under tighter timeframes than their hybrid or cloud-first peers.

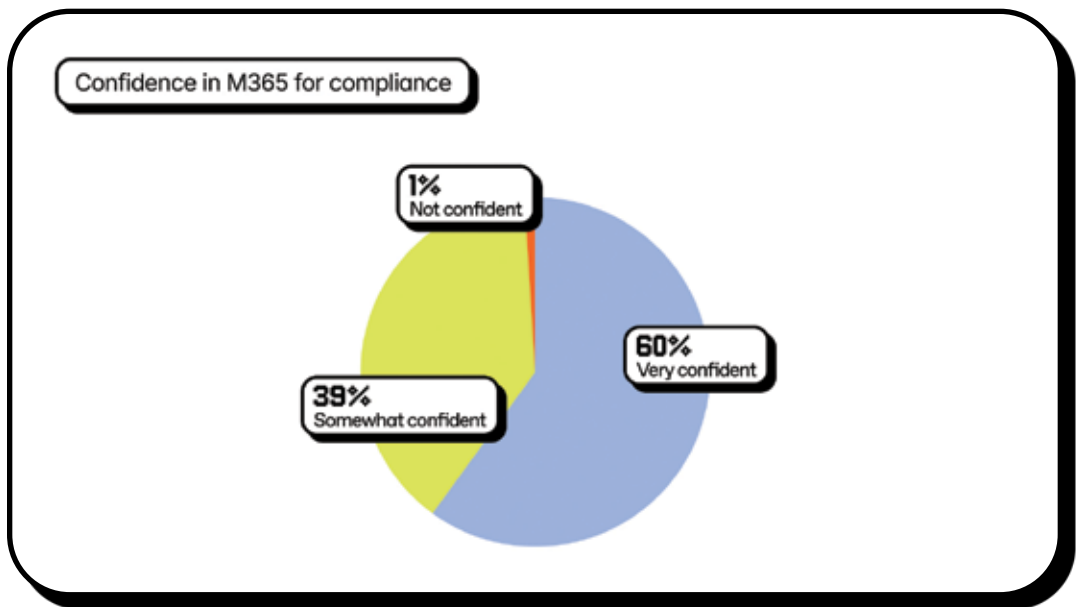
That same blend of caution and urgency also explains why teams say they trust Microsoft 365 yet still hesitate to act until every safeguard is proven.

Common concern, diverging plans

The same fear that pushes some toward the cloud drives others to maintain the control afforded by their server rooms. Let's look at how the worry for data safety splinters into two opposite strategies, and why both camps believe they're making the safest choice.

Trust Microsoft 365, verify everything

Most IT pros say Microsoft 365 ticks the compliance box.



But that confidence lasts only until someone asks for evidence. Then, most IT teams go about validating compliance on their own terms.

In other words, even teams that trust the platform won't move a single file until the paperwork is airtight.

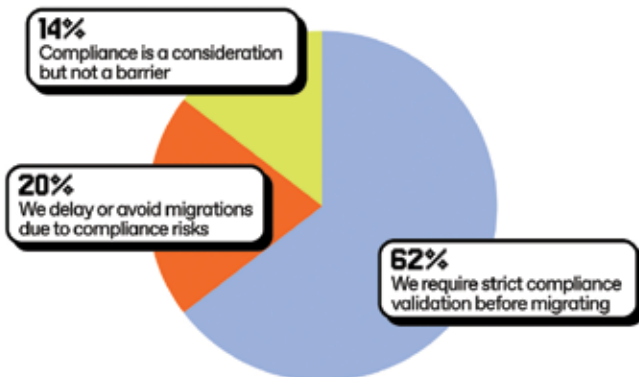
When we shared these results with Microsoft MVP Joanne Klein, she wasn't surprised.

“Teams often agonize over theoretical gaps while ignoring the fact that their current state isn't perfect—it's probably less secure.”



Joanne Klein
Microsoft MVP

Impact of compliance on migration decisions



This becomes truer with each passing month and quarter as Microsoft continues to announce and rollout new capabilities. Now, Microsoft Entra allows fine-grained conditional access policies tied to workload identities, not just users.

This extends zero trust deeper into hybrid estates. For teams balancing on-prem and cloud systems during phased migrations, it's an important feature.

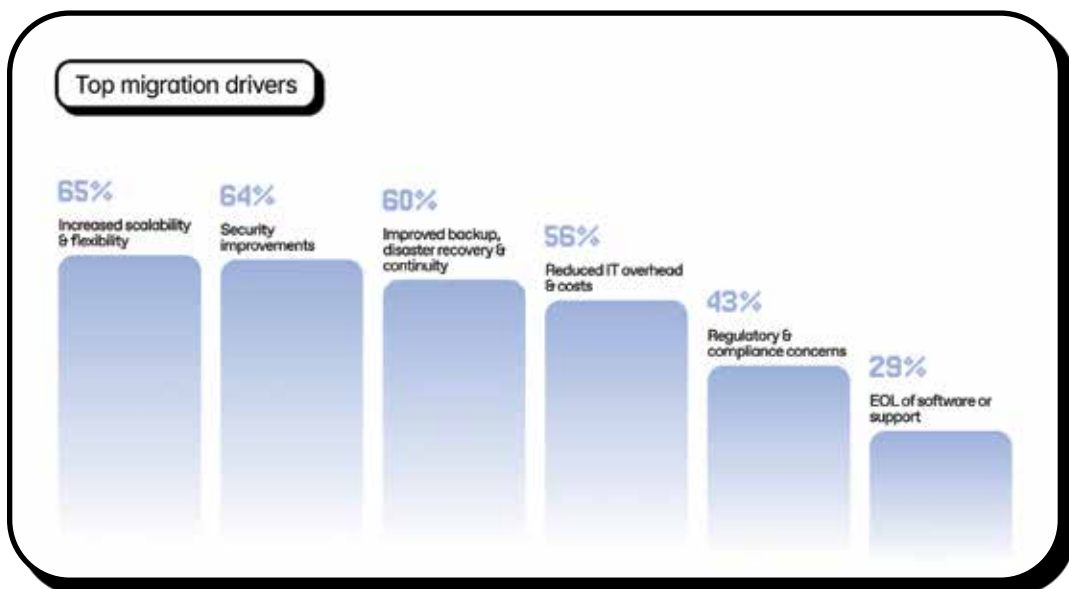
Additionally, Microsoft Purview's expanded data residency and compliance certifications give auditors more out-of-the-box proof, freeing teams to focus on real gaps.

Of course, those certifications only matter if your classifications survive the move. ShareGate's new Purview sensitivity-label migration⁶ carries your labels and metadata intact into the new tenant. The evidence you've built with Purview won't vanish during cutover. It'll land safely in the new environment, ready for audit.

To migrate or not to migrate

As we've highlighted, security is the number one reason why organizations choose to keep data on-prem. Let's pull up the data again: **66% listed data security and control as their top reason for staying on-prem.**

At the same time, when asked why they migrated to the cloud, **64%—a nearly identical share—selected “security improvements” as their top driver.**



So, how do we make sense of this? We asked Microsoft MVP and security specialist Jasper Oosterveld about the seeming contradiction here.

“Security means different things to different teams. In the cloud, you get security services like conditional access and multi-factor authentication. But some people feel like they’re more in control of their data when they can touch the servers. I do get where those people are coming from, especially for people in Europe who are concerned about where their data is being stored.”



Jasper Oosterveld
Microsoft MVP

Neither is wrong. They’re simply weighing different priorities, regulations, and worst-case scenarios.

The bottom line: the same fear drives both strategies. The deciding factor is which part of the risk equation your leadership prioritizes:

- **Control vs. coverage**

On-prem advocates equate safety with physical custody. They can track every patch and firewall rule. Cloud advocates view Microsoft’s 24/7 threat response and constant patching as a stronger shield.

- **Risk tolerance**

Some sectors fear data residency and third-party access more than missed patches. Others fear the opposite.

In practice, many organizations land somewhere in the middle. Hybrid setups keep certain data on-prem while shifting collaboration and archive data to Microsoft 365.

Microsoft’s investments in Azure Arc and hybrid key management show it’s not just pushing all-in cloud. It’s meeting organizations where they are.

However, Microsoft is primarily highlighting a new wave of Azure-native security services. Some of these are automated threat containment and AI-driven anomaly detection, designed to reduce the window between detection and remediation.

For regulated sectors still cautious about the cloud, these advances tilt the balance with proof of constant monitoring and instant containment that would be nearly impossible to replicate on-prem.

The next piece of the puzzle is tooling—what actually turns proof into a button click.

Building a security stack you can defend

Secure data is usable data. That's why Microsoft is positioning security as the foundation for Copilot adoption. Microsoft MVP Antonio Maio says that's clear based on Microsoft's roadmap:

“The two areas Microsoft is investing in are AI and data protection, with an emphasis on supporting the AI and Copilot workloads.”



Antonio Maio
Microsoft MVP

Without strong access controls and clean permissions, AI outputs can expose sensitive information. That's why both Microsoft and ShareGate frame security checks as step one, not an add-on.

A strong security posture starts with trust, but it's finished by evidence. The right mix of software and expert help turns that proof into a routine deliverable rather than a last-minute scramble.

Must haves for audit-friendly software

When you size up software to help you secure your tenant—whether for one-time moves or everyday management—prioritize a few essentials:

- **Permission visibility and mapping**
See who has access, adjust in bulk, and migrate permissions intact.
- **Label and metadata support**
Carry over sensitivity labels and custom metadata so classification sticks.
- **Audit-ready reporting**
Exportable logs that show what moved, who changed it, and when.
- **Automated policy enforcement**
Schedule checks for stale sites, overshared links, or risk flags.
- **Point-in-time backup and restore**
Quick rollbacks for accidental deletions or ransomware events.

Stacking these capabilities cuts review cycles and closes the confidence gap.

Microsoft 365 vs. on-prem security⁷

This framework helps you gauge whether your Microsoft 365 environment is ready for a cloud-first approach or still needs to address on-prem security blockers. It turns the “security paradox” into a practical self-assessment so you can see your true readiness and plan your next steps.

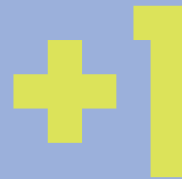
Step 1

Hard blockers

If your organization has any of these, keep it on-prem for now and assign an owner and target date to unblock it.

- Contract or regulatory prohibition on cloud processing or storage is still in force.
- Residency isn't finalized and Multi-Geo/ADR aren't approved for the required regions.
- Full-trust farm solutions (WSPs), server-side code, or timer jobs are in active use with no re-platform plan to SPFx, Graph, or Power Platform.
- Bespoke integration depends on direct SQL, content DB access, or unsupported APIs, and components in SharePoint Online.
- Network and latency SLOs can't yet be met over WAN to Microsoft 365 (e.g., CAD/PLM/video libraries, plant floor apps).
- Keys must remain entirely on-prem (e.g., HSM mandate) and Customer Key isn't accepted as equivalent.

*Quick residency note: The EU Data Boundary plus Multi-Geo/ADR may satisfy many EU/EFTA cases. If so, treat “Residency not finalized” as a temporary gate and set the approval step as your burndown item. If you need even tighter control, Microsoft now offers Data Guardian and External Key Management to add sovereignty safeguards while staying in the public cloud. There's also Microsoft 365 Local for organizations that must run Microsoft 365 in their own datacenter. (Availability varies by region.)

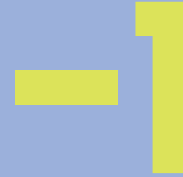


Step 2

Strong indicators (+1 each)

These aren't full-on blockers, but they make immediate cutover harder. Add a point for each that applies.

- Legacy or bespoke integrations (LoB, event receivers, BDC, scanner imports, in-house add-ins) that need refactoring
- Data gravity and complexity (multi-TB libraries, extreme file counts, deeply nested permissions)
- RBS or cheap storage (Remote Share Provider/SMB offload) you're not ready to replace
- Hybrid search required (align farm to SPSE 25H1+ going forward)
- Auth mid-transition (apps still rely on non-modern auth)
- RMS/IRM dependencies not yet redesigned for sensitivity label encryption
- Tight change-control windows or seasonal freezes right now
- IR/backups still centered on on-prem; not ready for Microsoft 365 Backup or SaaS backup
- Classic customizations (classic publishing, JSLink, InfoPath) that need redesign
- Local or isolated operations (regulated labs, defense, disconnected plants)
- Missing governance baseline (sharing defaults, lifecycle, provisioning, naming, labels)
- Role clarity and/or owner readiness (labels, retention, sharing, training) not in place
- Incident and eDiscovery not transitioned to Microsoft Purview workflows



Step 3

Cloud advantages you need

(-1 each)

If stakeholders expect these in the next 12 months, subtract a point per item. They tilt you toward the cloud.

- **Information protection and governance**
Purview sensitivity labels (with encryption or usage rights), retention (auto-apply or event-based records), unified DLP, site, or container labels, and default doc labels
- **Threat protection**
Built-in anti-malware at rest; Defender for Office 365 Safe Attachments for SharePoint Online, OneDrive, and Teams
- **Access control**
Unmanaged device controls (Conditional Access app enforced restrictions), Defender for Cloud Apps session controls, SharePoint Advanced Management (e.g., Restricted Access Control), Information Barriers v2
- **Audit and discovery**
Purview Audit (Standard) or Audit (Premium) retention and events; Purview eDiscovery (Standard or Premium)
- **Encryption and keys**
Per-file service-side encryption; Customer Key (BYOK)
- **Resiliency and recovery**
Self-service Restore this library, deleted site recovery, Microsoft-assisted backups; Microsoft 365 Backup at scale
- **Data residency choices**
Multi-Geo/ADR for at-rest placement across regions

Step 4

Decide the path (Add up your points)

If any gate in Step 1 is checked, keep on SPSE/hybrid for now and create a plan for addressing it. Otherwise, total Step 2 points and subtract Step 3 credits.

≥ 6

Stay SPSE/
hybrid for now.

Publish your
burndown and
re-score next quarter.

3-5

Hybrid with
aggressive
blocker
burndown.

Pilot in Microsoft 365,
close top gaps,
re-score quarterly.

≤ 2

Cloud-first
migration to
SharePoint
Online.

Plan your waves and
go (with Conditional
Access, MFA, and
Microsoft Purview
controls as table
stakes).

Why most teams phone a friend

When the project stakes climb—new regulations, sensitive data, unfamiliar jurisdictions—teams call in help. In our survey, **42% list partners among their most-trusted sources when evaluating IT software**. That trust shows up later in project timelines, too: 87% of respondents involve a partner during complex moves like tenant consolidations. Why lean on outside help?

- **Regional nuance**
A local partner already speaks the auditor's language, saving cycles on data-residency fine print.
- **Staffed for off-hours**
Cutovers and remediation often happen overnight. Partners supply the after-hours crew.
- **Tool know-how**
Seasoned migration firms arrive with proven platforms, so they don't lose any time learning new tooling.
- **Acceleration and predictability**
Repeatable runbooks and pre-built scripts compress schedules, firm up timelines and shift risks away from your IT budget.

Why product-embedded expertise matters, too

A good tool should feel like a miniature consulting firm hiding behind the UI. ShareGate bakes the following in, so you don't have to hire out:

- **Smart pre-check diagnostics**
Before the first byte moves, ShareGate runs a pre-check that flags unsupported risks, conflicts, missing templates, and dozens of other blockers. Then it suggests fixes.
- **Contextual error coaching**
When a task fails, the UI links straight to the exact help center article or PowerShell snippet required to remediate it.
- **Auto-retry and incremental copy**
If Microsoft 365 throttles or the network hiccups, ShareGate queues only the delta on the next pass—no full reruns needed. And Insane mode and Copy if newer make cutover time even faster.
- **Audit-ready reporting**
Migration reports can be exported to Excel/CSV or piped to Power BI, capturing who moved what, when and flagging compliance violations.
- **Governance automation out of the box**
Assessments and actionable reports keep the tenant lean long after the migration is over.

Key lessons from the data

Security is the one topic everyone agrees is paramount, but some rush to the cloud for its protections while others prefer on-prem servers for control. How can you build a posture you can truly defend?

Three actions rise to the top:



Turn confidence into concrete proof.

While 60% of IT pros feel "very confident" Microsoft 365 meets their compliance needs, a nearly identical 62% require strict compliance validation before moving a single file. Help bridge this gap by using tools that support hard evidence—like audit-ready reports, Purview label migration, and permissions mapping. Proof that will get leadership to act.



Reframe the security debate from location to capability.

Security is both a top reason to migrate (64%) and to stay on-prem (66%). Shift the focus from where the data lives to what protects it. Highlight modern controls like MFA and automated threat response to make the case for the cloud. Third-party tools give you greater control on how you get there.



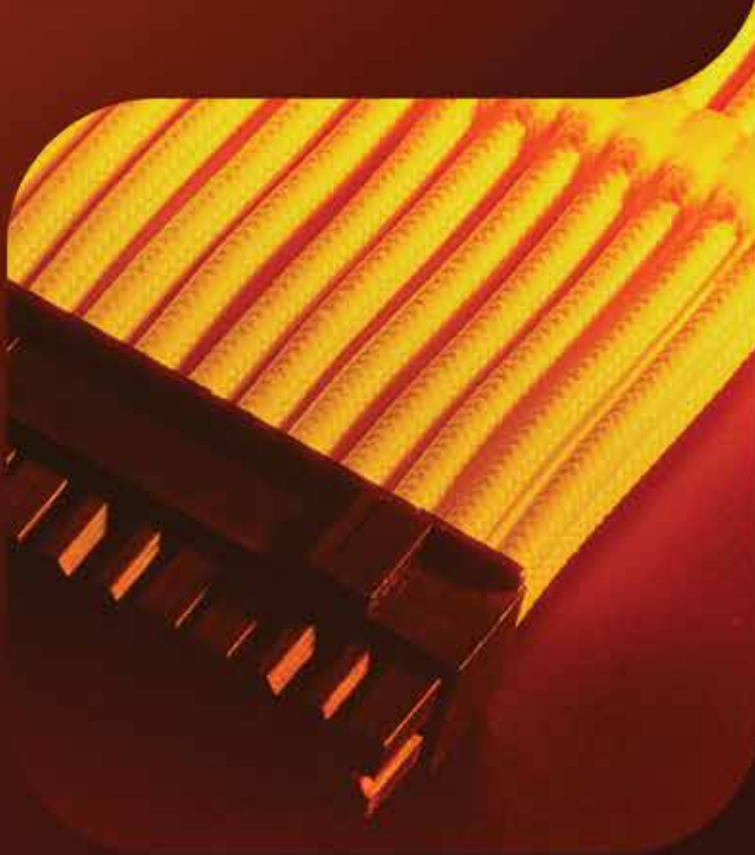
Use expert validation to break the stalemate.

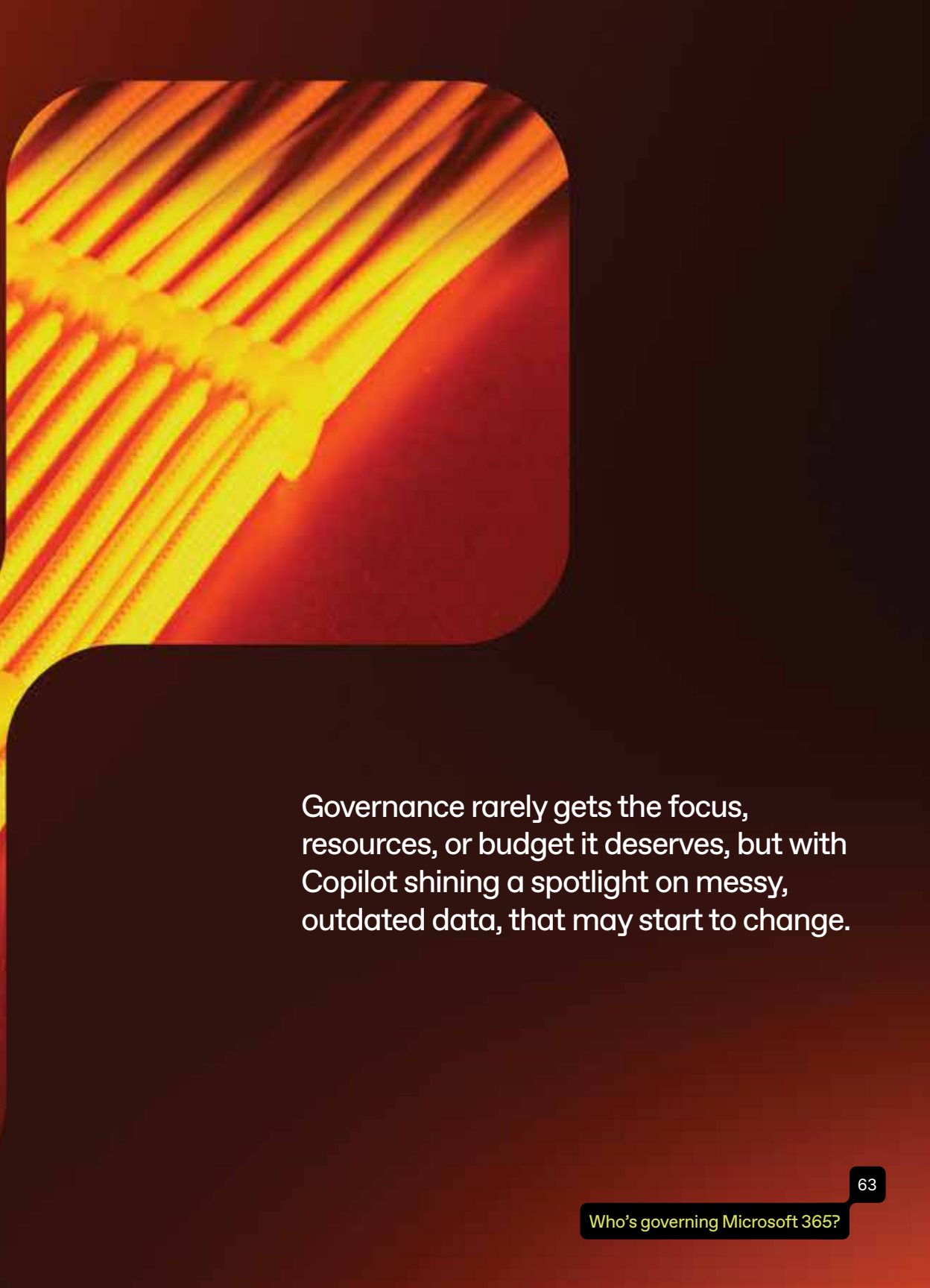
For the 82% of teams that either require strict validation or delay projects due to compliance fears, an outside voice can make all the difference. Involve a trusted partner to provide an objective assessment that builds confidence and gets the project moving again.

A strong security posture isn't just a one-time project, it's a daily practice. That brings us to the focus of our next chapter: governance. The ongoing rules and routines that keep your Microsoft 365 tenant secure and efficient long after the migration is over.

05

Who's governing Microsoft 365? The 1% gap





Governance rarely gets the focus, resources, or budget it deserves, but with Copilot shining a spotlight on messy, outdated data, that may start to change.

Who's governing Microsoft 365?

The 1% gap

You finally crossed the migration finish line and slammed the laptop shut. High fives all around! Until the first “why can't I access that site?” ticket hits.

Your tenant will always be changing. Sites multiply, links get shared, departments are restructured, employees are hired and replaced. In order to optimize and secure your environment, you need governance.

Our survey showed what most of us already know: governance isn't the top priority for most IT teams.

Governance may not be flashy like an M&A cutover or ransomware drill. But every expert we spoke with told us how critical governance is.

In this chapter, we'll discuss why governance slips down priority lists, how that blind spot balloons risk and cost, and—good news—why that may be starting to change.

Your migration's over, but your governance is ongoing

All the challenges IT pros face when managing their tenants are symptoms of the same diagnosis: loose or non-existent governance.

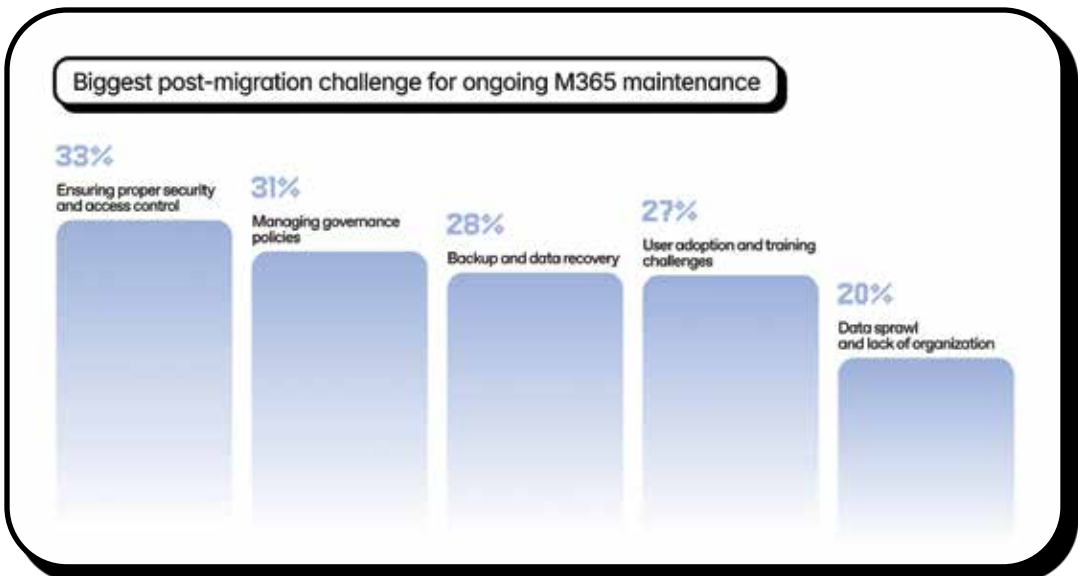
Think of governance as a living framework, not a one-time checklist. It's the set of rules, roles, and automated routines that keep sites tidy, data protected, and users productive long after the migration ends.

Yet, it's often overlooked.

We asked 650 IT pros about their Microsoft 365 management challenges, and we weren't particularly surprised by the results.

Security is at the top, governance policies come in second, closely followed by backup and adoption, and then sprawl trails behind. But all of these issues share one root cause: unmanaged governance.

As Microsoft MVP Marc Anderson puts it: "If you care about security, you care about governance. Those two things aren't separate."



If you care about security, you care
about governance. Those two things
aren't separate.

— Marc Anderson

That's evident in the way Microsoft is positioning some of its new releases. Microsoft's Secure Future Initiative (SFI) is pushing governance and risk oversight into the core of product design. Governance isn't a back-office checkbox but a core part of how Microsoft is reworking identity, audit, and compliance across its stack.

Let's look at how the top post-migration challenges in our survey all relate back to governance:

■ **Access-control gaps**

Ownership ambiguity lets permissions sprawl. Governance steps in with role-based policies, scheduled audits, and delegated approvals that keep the right people in and everyone else out.

■ **Policy enforcement**

Having policies in place allows your end users to work productively and collaboratively within the guardrails you've set up for them.

■ **Backup and recovery gaps**

Native retention limits and scattered scripts leave restore gaps. Unclear RPO/RTO make every accidental delete unnecessarily risky.

■ **User adoption stalls**

Governed templates and self-service guardrails cut red tape and get employees actually using the tools.

■ **Data sprawl**

Orphaned sites and duplicate OneDrives drown search (both in SharePoint and Copilot). Governance manages the chaos with clear information architecture, content classification, and automated lifecycle rules.

Treat governance like an always-on service—complete with owners, metrics, and tooling—and these pain points become routine maintenance.

Triggers that turn neglect into necessity

Marc Anderson is CEO of Sympraxis, a consulting firm that helps companies migrate to and manage Microsoft 365. He explains how organizations come to care about governance:

“There has to be a trigger for people to understand that governance matters. That trigger may be that they’re mature enough to know that governance matters, or it might be a governance emergency.”

We found there are four main triggers for IT teams to start caring about governance:

- 1 **An emergency**
- 2 **Copilot and AI**
- 3 **Compliance**
- 4 **A complex migration**

What is a governance emergency?

We all know what a security emergency might look like. Governance emergencies are less common and rarely make the news, but they do happen. Marc told us about one example:

“We had one client that had been using a single document library for everything. They had 16 terabytes in that one library, and they came to us when they ran out of sharing links for it, since Microsoft has a maximum of 50,000 external sharing links per library. That is a governance emergency.”

Unfortunately, most organizations that seek out help specifically for governance tend to do so because they’re responding to a major issue rather than to *prevent* major issues from happening in the first place.

“Governance is something where no one wants to pay for preventative health, they just want to pay for the emergency lifeline when it all goes wrong.”



Christian Buckley
Microsoft MVP

Garbage in, garbage out: A recipe for Copilot waste

Copilot's answers and efficiency are grounded in data, which primes another major trigger that gets people caring about governance.

"It's a garbage in, garbage out kind of thing. If you have old data and lots of versions, Copilot will struggle to figure out the right answer to your prompt."



Eric Overfield
Microsoft MVP

It can go beyond risking inefficiency into risking security. If you have broad permissions on sensitive data, Copilot can accidentally risk a critical security breach. Richard Harbridge, Microsoft MVP and Strategic Alliances and Ecosystem Manager at ShareGate, explains the importance of governance to Copilot efficiency:

"Without governance, Copilot becomes a high-speed engine for surfacing chaos. Good governance is key to transforming Copilot from a potential liability into a reliable productivity tool."

That's why **58% of IT leaders say sloppy data quality and retention rules** are their top Copilot worry.

Recognizing that gap, Microsoft is rolling out new Purview features—priority cleanup, Copilot-related retention policies, and AI support for data-security investigations—to help address it. These updates make governance readiness for AI interactions less optional and more urgent.

And if you've been championing governance without getting the green light, that urgency is finally working in your favor.

"Things like sensitivity labels and better security posture, that's always been an easy conversation to have with leadership. Better records management or retention? That's been a hard sell."



Joanne Klein
Microsoft MVP

Yet retention emphasizes the very same needs that power AI: understanding what's valuable, relevant, and worth keeping.

We'll talk more about this in our next chapter all about Copilot.

Compliance and complexity

There are a few other situations that create a governance pressure cooker:

1

Ever-tightening compliance deadlines

43% of teams launch governance projects specifically to satisfy new regulations. The previous chapter gives more details on this.

3

Significant modernization

Migrating from on-prem to the cloud means new apps, tools, and architecture. The *Migration momentum* chapter delves into modernization migrations.

2

Tenant-to-tenant migrations

41% rank security and compliance as the hardest hurdle. The *M&A migrations by the numbers* chapter breaks down that high-stakes playbook.

The drive for governance is finally here. So why do 99% of teams still stick with the “free” toolkit?

Without governance, Copilot becomes a high-speed engine for **surfacing chaos**.

— Richard Harbridge



Gove
sm



ern
arter

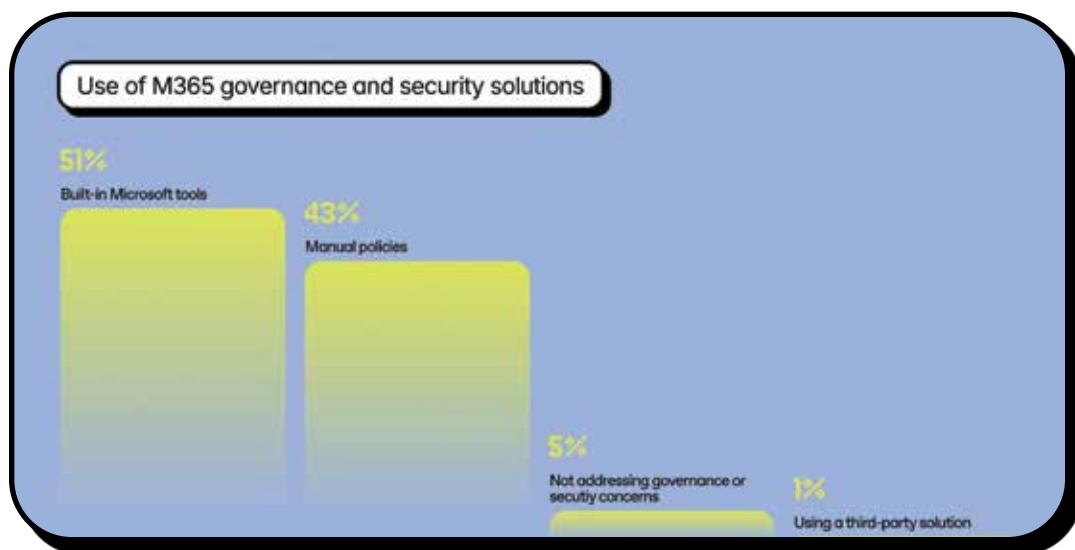
Why 99% settle for “good enough” governance tools

If urgency is rising, why do so few IT teams use purpose-built tools for governance? The answer starts with convenience and cost. Native tools are already licensed, already whitelisted, and feel “safe” in front of the C-suite.

But as governance demands multiply, reliance on built-ins drives hidden labor costs, slows remediation, and leaves audit trails paper-thin.

When “free” governance isn’t actually free

We weren’t surprised that governance didn’t top the list of post-migration priorities. But one stat we were shocked by? **Only 1% of IT pros use a purpose-built governance solution.**



Back in the chapter *Migration momentum*, we noted that 70% of teams begin migrations with Microsoft's free utilities. Of those same respondents, 51% now rely on the matching "free" dashboards for governance—revealing the same convenience instinct at play.

We asked Microsoft MVPs Jasper Oosterveld and Marc Anderson about this stat. They weren't as surprised as we were. As Jasper shares, "I've definitely seen a lot of customers working with native, and it's always interesting because it's very limiting in my eyes. A lot of that stuff hasn't been developed for years, like Teams templates and expiration policies."

Jasper attributes some of the hesitance to use third-party solutions to red tape. "You have to go through a compliance process. Plus some organizations are worried about where their data might be stored, especially for customers in Europe who might not want their data stored in the US."

Marc has seen it as well, and he thinks that IT pros probably see cost as a roadblock. That would be a misconception:

"The cost of ShareGate is irrelevant compared to the amount of time you spend trying to use Microsoft's half-baked tools."



Marc Anderson
Microsoft MVP

When we showed Microsoft MVP Christian Buckley the previous graph, his reaction was telling.

"I'd be interested in knowing what percentage of those people think they're doing a good job of governance."



Christian Buckley
Microsoft MVP

Some probably know that the native tools and manual scripts aren't cutting it, but they don't have the time, resources, or executive buy-in to get a purpose-built tool. Others may not understand the significance of governance and think that what they have is good enough.

Microsoft MVP Ragnar Heil viewed this data from a different perspective—collaboration and shadow IT. He told us that relying on Microsoft's built-in dashboards isn't enough to preserve good habits or protect collaboration:

"We need to use professional tools to make sure people are still using SharePoint as a place to share content."



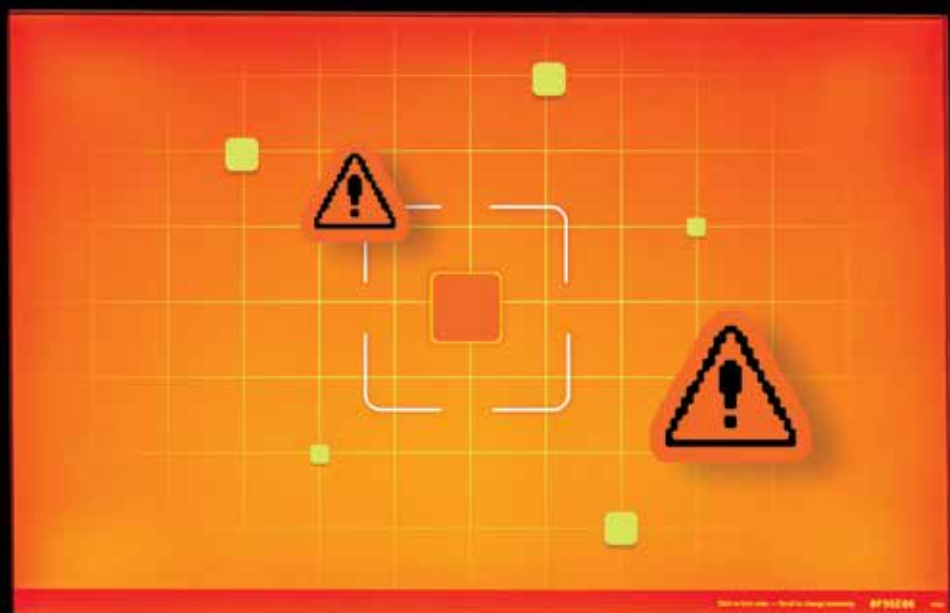
Ragnar Heil
Microsoft MVP

Let's look at some of the hidden costs of native tools and manual scripting:

- **Labor drain**
Admins hop between scattered dashboards and PowerShell windows, burning hours that could fund a modern tool.
- **Slow remediation**
Manual reviews and CSV exports delay fixes, letting risk linger.
- **Weak reporting**
Native reports don't capture every change, forcing last-minute evidence hunts.
- **Opportunity loss**
When Copilot launches or M&A projects need airtight controls, teams have to clean up past oversights instead of moving forward.

In short, the "free" option isn't free at all. It just defers the bill until an audit, breach, or board-level project makes the true cost impossible to ignore.

Just as tenant-to-tenant moves forced admins to abandon native migration tools, growing workloads and Copilot pilots force them to abandon built-in governance options.



How much are you spending on “free” tools?

Native Microsoft 365 governance tools and manual scripting may not come with a price tag, but the labor, delays, and risks can dwarf the price of a modern solution.

If you're not using a purpose-built solution for governance, take a moment to get a rough estimate of how much your “free” strategy is actually costing your team. It may be time to invest in a better way.

Question

0

1

2

1. How many admin hours per month are spent on manual governance tasks (CSV exports, PowerShell scripts, cross-dashboard checks)?
2. When an auditor or exec asks for a permissions report, how long does it take to deliver it?
3. How many separate dashboards or scripts does your team juggle for governance tasks?
4. How many duplicate or ownerless Teams/SharePoint sites exist in your environment?
5. How do you apply or adjust lifecycle policies (naming, retention, expiration) across workspaces?
6. How fast can you rollback a permission change or restore a deleted workspace?
7. How much time does your team spend preparing reports for leadership or audits each quarter?
8. How many governance tasks still require senior admins or PowerShell expertise?

≥ 40 hours per month

10-39 hours per month

≤ 9 hours per month

A week or more

2-6 days

< 48 hours

≥ 4

2-3

1

≥ 100

Dozens, tracked manually

Tracked automatically and remediated regularly

Manually one by one

With scripts / templates

Bulk or automated

Days with manual restore

Hours with scripting

Minutes with one-click restore

A week or more

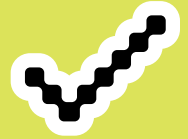
1-6 days

Hours

Most / all

Mixed

Very few / none



Scoring

13–16 pts

Governance efficiency champ

You've got things pretty well figured out. Keep monitoring, but you're in good shape.

7–12 pts

The hidden-cost zone

You're burning more admin time and risk than you realize. Track hours and delays. You probably have a business case for a purpose-built tool.

0–6 pts

"Free" is expensive

The cost of manual work and fragmented dashboards is likely costing you more than the price of a modern governance solution. Time to quantify the drain and make your pitch.

Automating proof and protection with the right allies

Purpose-built tools aren't just more user friendly, they do the grunt work that keeps governance alive long after the migration ends.

Microsoft's roadmap shows alert triage agents in Purview (powered by Security Copilot), which will help automate data-security investigations and highlight governance anomalies. Those capabilities are powerful, but they're still scattered. ShareGate Protect consolidates them and turns them into prioritized, actionable fixes.

This signals a shift in both the governance and security narratives. The first is that governance must be more proactive, not passively reactive. The second is that governance has to be the foundation for AI and Copilot security.

If Copilot is going to surface data, governance has to prove that it's safe to expose.

A modern tool should:

- **Surface risk in plain language**—who has access, what's overshared?
- **Export audit-ready reports on demand.**
- **Let you remediate in bulk** rather than script by script.
- **Capture granular, point-in-time snapshots** so you can roll back accidental deletions or ransomware hits in minutes.

Organizations that moved fast during migration now need to move just as fast on governance. With ShareGate Migrate and ShareGate Protect, teams carry the same advantages they unlocked on day 1 into day 1,000.



ShareGate Protect⁸ gives you an at-a-glance dashboard—total sites, inactive workspaces, guest access, overshared links—plus one-click fixes to act on the data.



With **ShareGate Migrate⁹**, you can preview, map, and clean up permissions before, during, and after your migrations to ensure groups and roles always have the right access.



You can also **bulk-copy and transform the details that matter**—metadata, version history, and even Microsoft Purview sensitivity labels¹⁰—so content keeps its context, compliance tags, and searchability.

Astrid Gibbon is a Communications Systems Manager at Oxford Instruments¹¹, and like so many other IT pros, she realized she had little control over her tenant—and no clear picture of what even needed to be governed: “It wasn’t until I opened ShareGate that I discovered there were 107 teams that didn’t have owners. And then on the dashboard I could see who they were, where they were. Even better is the automation. Now I feel completely in control. Every team has two owners, every team has been checked for external users and links in the last six weeks, and we don’t have any inactive teams.”

As Microsoft layers in richer governance and AI agents, ShareGate Protect’s unified console and built-in risk assessment become the active layer that helps you interpret and act on those signals, rather than chasing them in multiple systems.

It can also help to lean on a certified Microsoft partner for the heavy lifts, like policy design or regional compliance nuance. This can help the in-house team to stay focused on the day-to-day checks.

⁸ sharegate.com/microsoft-governance

⁹ sharegate.com/microsoft-migration

¹⁰ sharegate.com/blog/simplify-sensitivity-label-migration-in-microsoft-365

¹¹ sharegate.com/user-story/how-oxford-instruments-regained-control-of-their-microsoft-365-environment

A governance conversation starter

If you're a partner, you know the value of good governance and you probably have the expertise to make it a simple, repeatable task. But as we've seen, many IT teams aren't interested in spending time and resources on governance.

So, we put together some targeted questions and data points to help your prospects see the hidden costs of "free" tools, position yourself as the trusted advisor, and tee up ShareGate Protect as the next logical step.

How to use it today

Choose one or more of the questions to open the conversation and listen to their answers. Jot down any pain points they mention.

If they're struggling with governance, reassure them with one or two of the data points so they know they're not alone.

Then offer one of the next steps as a free or low-friction way to continue the discussion.

Governance service offering conversation starters

Use any or all to open the door:



- How long would it take you today to produce an audit-ready permissions report for leadership or an auditor?
- Do you have any outdated workspaces or overshared links that Copilot might surface to the wrong audience?
- How many different admin centers or scripts does your team juggle to keep governance in check?

Core data points to share

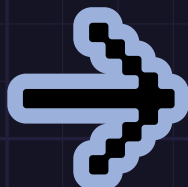
Anchor the discussion with credible stats:



- 58% of IT leaders say sloppy data quality and retention rules are their top Copilot worry.
- 43% of teams launch governance projects specifically to satisfy new regulations.
- 31% of IT pros cite “managing governance policies” as a top post-migration challenge.

Next steps to offer on the spot

Give the prospect an easy path forward:



- Run a no-cost Governance risk assessment in minutes to show live results.
- Book a 30-minute “governance health” briefing where you present their top risks in plain language.

ONLY

1~~2~~4

**of IT
pros**

use a purpose-built
governance solution.



Key lessons from the data

The migration is done, but the real work is just beginning. The data reveals a massive gap: while teams battle the daily fires caused by poor governance, a shocking 99% lack the purpose-built tools to fix the root cause. We need to make the case for investing in control.

Three actions rise to the top:



Connect governance to your team's daily fires.

Stop talking about governance as an abstract concept. Frame it as the strategic solution to the issues your team already faces: **security (33%)**, **governance policies (31%)**, and **data sprawl (20%)**.



Use Copilot as your catalyst for change.

Leverage the fact that **poor data quality is the top Copilot concern (58%)** to finally secure the investment in governance that 99% of organizations are currently missing.



Expose the high cost of "free" tools.

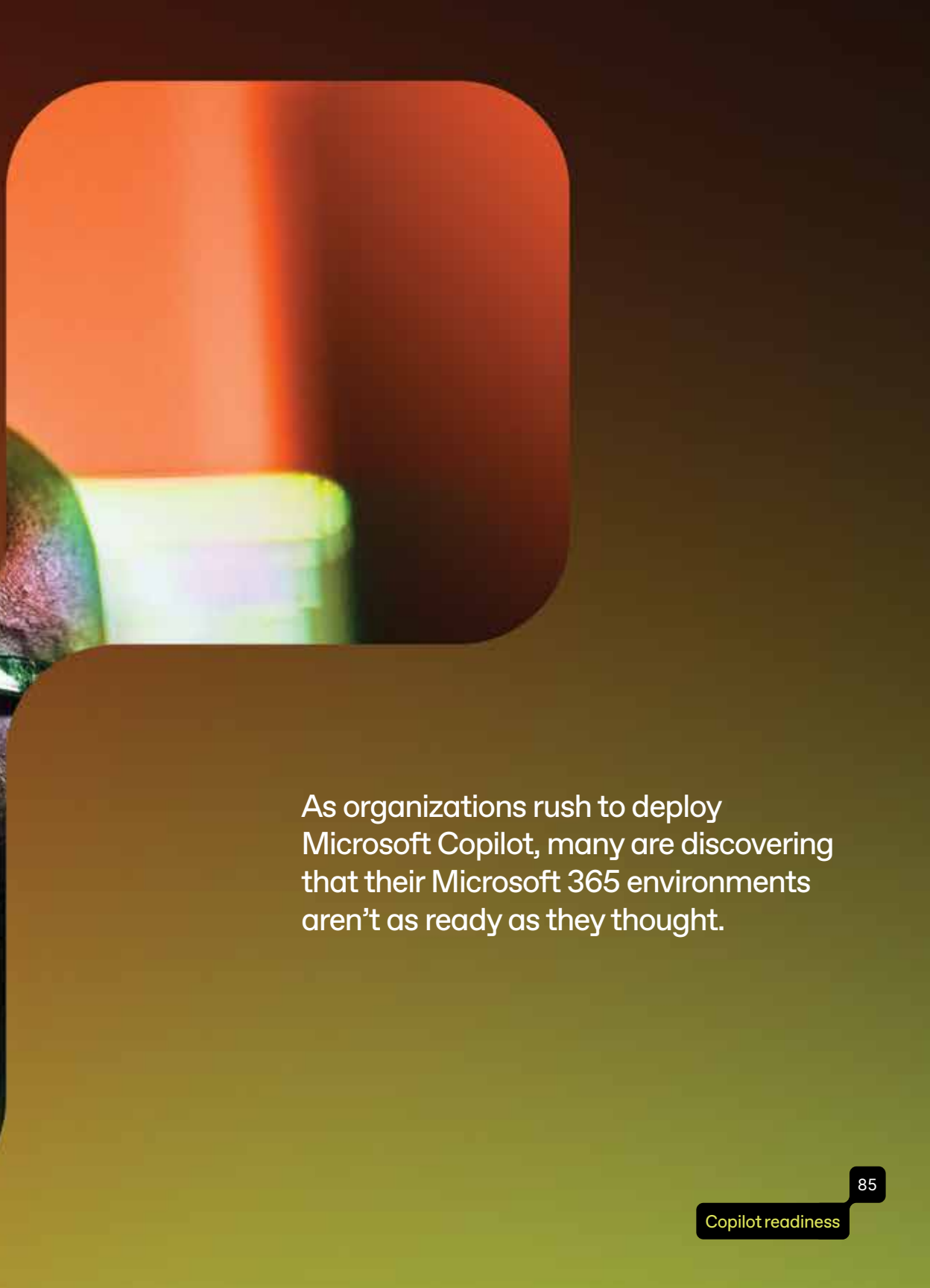
Track the hours your team spends on scripting and manual clean-up to **prove that the price of a dedicated tool is a fraction of the cost** of the inefficiency and risk of relying on native tools.

This newfound urgency around governance sets the stage perfectly for the biggest IT initiative of the year and the focus of our next chapter: turning AI risk into AI reward.

06

Copilot readiness: Progress, pitfalls, and the opportunity for IT





As organizations rush to deploy Microsoft Copilot, many are discovering that their Microsoft 365 environments aren't as ready as they thought.

Copilot readiness: Progress, pitfalls, and the opportunity for IT

In 2025, many organizations are discovering a foundational truth: AI is only as good as the data it runs on.

Copilot acts as a powerful magnifying glass, bringing into sharp focus the pre-existing state of your Microsoft 365 environment. For many, that means it illuminates years of messy permissions, content sprawl, and unclear data ownership.

IT teams are moving quickly to deploy Copilot and unlock its promised benefits, but that speed comes with risk.

In this chapter, we'll explore how organizations are approaching Copilot deployment, where they're running into roadblocks, and what IT teams can do to lead secure, sustainable rollouts that maximize value. You'll get a clearer picture of how your readiness compares to the market and where to focus to maximize your AI investment.

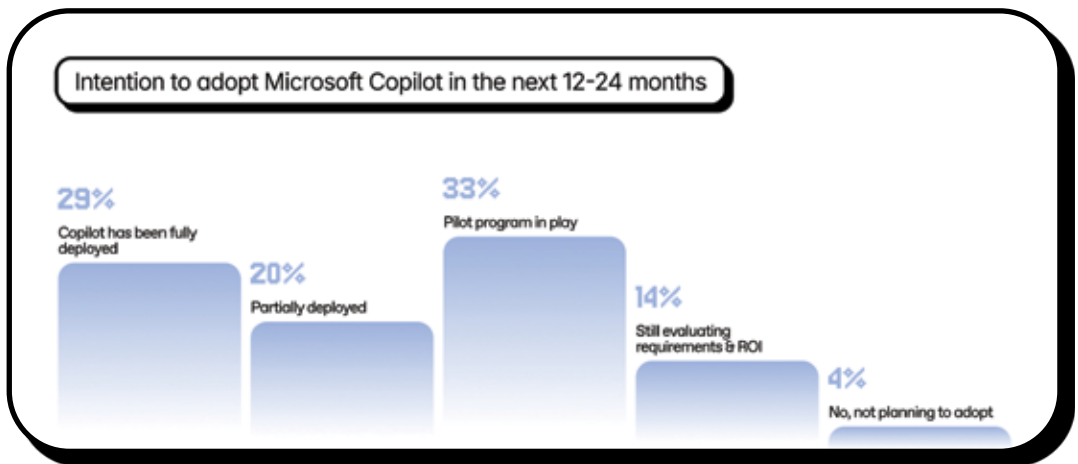
Copilot adoption benchmarks and rollout patterns

Organizations are investing time, budget, and talent into Copilot with the expectation that it will streamline operations, boost productivity, and unlock the full potential of their Microsoft 365 environments.

In this section, we'll walk through how Copilot is being adopted, who's leading the rollout, and what goals are shaping the journey.

AI in action: Deployment is already happening

More than four-fifths of organizations have moved past planning for Copilot and into deployment:

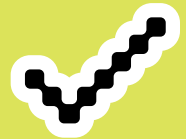


The numbers speak for themselves. Copilot is not a side experiment. Now, most organizations are looking for what to do post-deployment, or at least post-pilot.

Are you ready to expand your Copilot pilot?

You've piloted Copilot, wahoo! Now what? This scorecard will help you decide if you're ready to expand or if you should refine your pilot first.

Question	No	In progress	Yes
1. Have you validated permissions, sensitivity labels, and external sharing policies for the pilot group's data?	0	1	2
2. Do you have an easy way to identify and remediate oversharing or stale workspaces at scale?	0	1	2
3. Is the content Copilot indexes current, deduplicated, and properly labelled?	0	1	2
4. Do you have retention/lifecycle rules for inactive content?	0	1	2
5. Have you defined measurable success metrics for your pilot (time saved, productivity gains, license utilization)?	0	1	2
6. Do you have a training/communications plan to support adoption at scale?	0	1	2
7. Do you have clear evidence that your Copilot deployment meets your sector's regulatory or residency requirements?	0	1	2
8. Have you validated that retention, eDiscovery, and data classification policies carry through to Copilot?	0	1	2



Scoring

Add up your points. Your total will fall into one of these ranges:

0–7 pts

Keep refining your pilot

You're still building your foundation. Focus on closing the biggest gaps first—permissions and oversharing controls, content cleanup, and baseline success metrics. The more you shore up now, the smoother and safer your scale-out will be.

8–11 pts

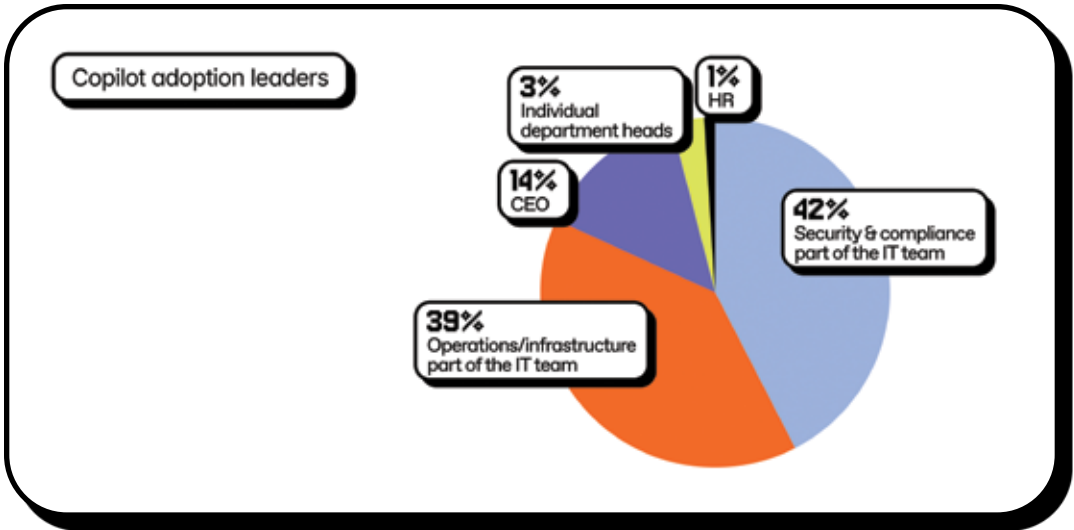
Tighten the screws

You've got many of the essentials in place, but a few weak spots remain. Prioritize finishing those items, for example, lifecycle rules, adoption training, or evidence for compliance. Once you've filled those gaps, you can scale confidently.

12–16 pts

Green light for expansion

You've built a solid foundation for Copilot. With permissions, content, adoption, and compliance all addressed, you're ready to roll out by waves and monitor usage and ROI at scale.

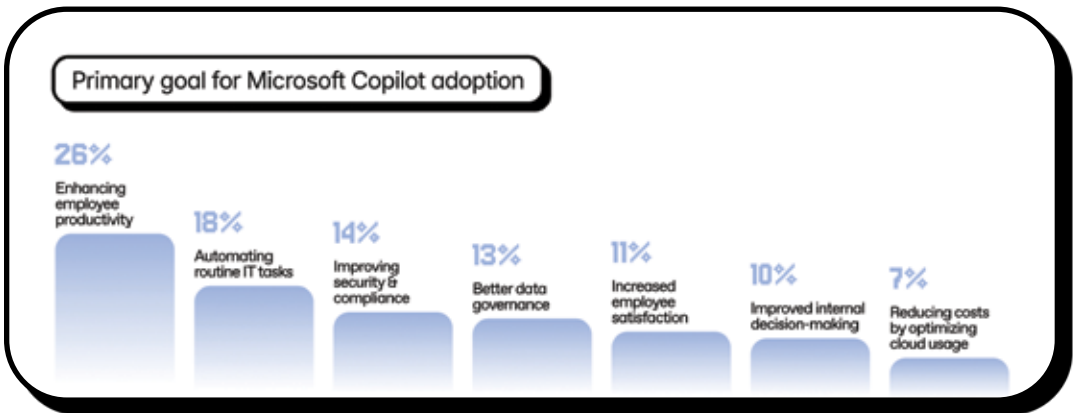


Our survey also showed that the momentum behind Copilot rollout is being steered from the engine room—the teams running Microsoft 365, not the boardroom.

The onus is on IT to ensure the environment—and the data that fuels Copilot—is truly ready before flipping the switch. Technical readiness, especially governance, is the deciding factor between a quick win and a messy rollout.

The business case for Copilot: A double-edged sword

Copilot isn't being adopted for novelty. It's being funded for impact.



IT leaders first point to productivity (26%), highlighting how it enables employees to work faster and create content more efficiently, followed by the automation of routine tasks (18%). While these gains map neatly to everyday pain points, they're directly threatened by the "garbage in, garbage out" principle. If Copilot surfaces irrelevant, outdated, or incorrect information, it hinders productivity instead of helping it.

But it's not only the quality of content at stake; your AI agents themselves need guardrails. Without clear policies, even well-trained Copilot agents can bypass your existing controls.

Microsoft's Copilot Studio roadmap reflects this. The new preview features allow admins to quarantine or block potentially unsecured agents via PowerShell and apply the same classification, permissions, and lifecycle rules you set for content and identity.

With both data hygiene and agent governance in place, organizations begin to see time savings that make Copilot's ROI story so powerful.

For many teams, that kind of time savings is the simplest ROI story they've ever had to tell.

Another 14% cite stronger compliance workflows, viewing Copilot as a catalyst for surfacing the right data at the right time:

"Executive interest in Copilot finally gives compliance teams board-level airtime and funding."



Joanne Klein
Microsoft MVP

Taken together, these adoption benchmarks show that Copilot is moving fast—and IT teams are behind the wheel because they see clear wins in productivity, automation, and even compliance. That speed, however, creates its own risks and roadblocks.

"Every time I use Copilot—and I use it daily—it saves my company more than the license costs, just by giving me a solid first draft or a quick meeting recap."



Eric Overfield
Microsoft MVP

From promise to pitfalls: Copilot's risk landscape

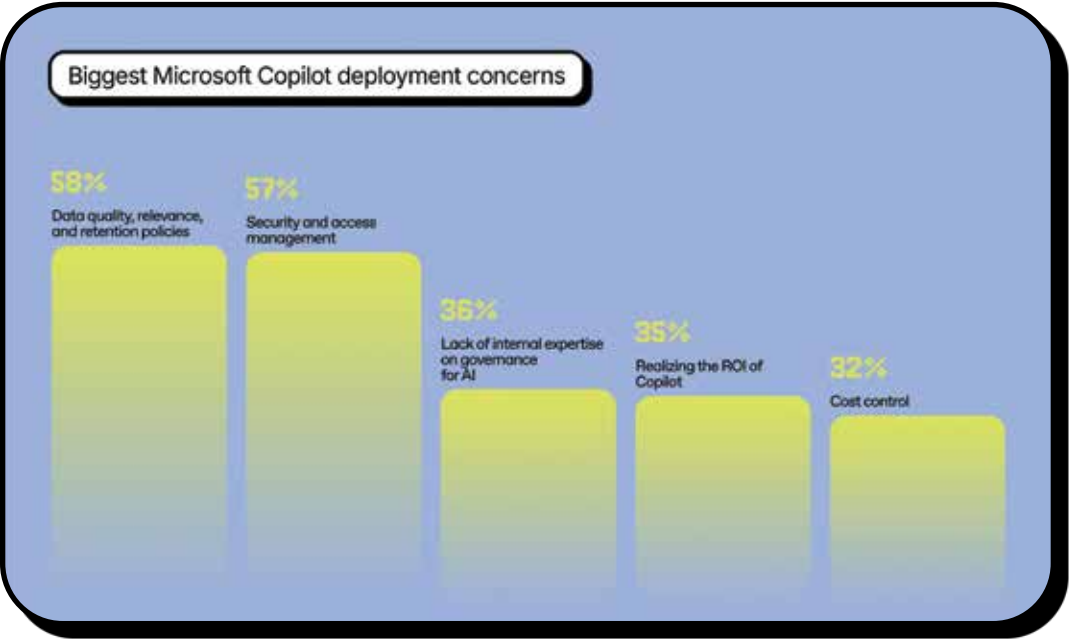
Copilot's business case is compelling, but no rollout happens in a vacuum. The same IT teams driving adoption are also grappling with security, data quality, and skills gaps that Copilot can exacerbate if left unaddressed.

In practice, the rush to deploy AI often outpaces the foundational work required to secure content, verify access, and prevent sensitive information from being disclosed in unintended prompts.

This section explores the issues most likely to hinder progress. By understanding where the pressure points lie and how to prioritize fixes, you can allocate resources to stay on track.

Top worries: Data, access, and expertise

Ask IT leaders what could derail their Copilot rollout, and three themes emerge immediately: messy data, leaky permissions, and a shortage of governance know-how.



Data hygiene, access, and lack of governance expertise consistently ranked in the top three concerns across every industry we surveyed—technology, financial services, healthcare, education, and more. This makes sense since Copilot shines a spotlight on these issues.

“Copilot is the trigger that finally makes messy permissions and site sprawl impossible to ignore,” explains Marc Anderson, Microsoft MVP.

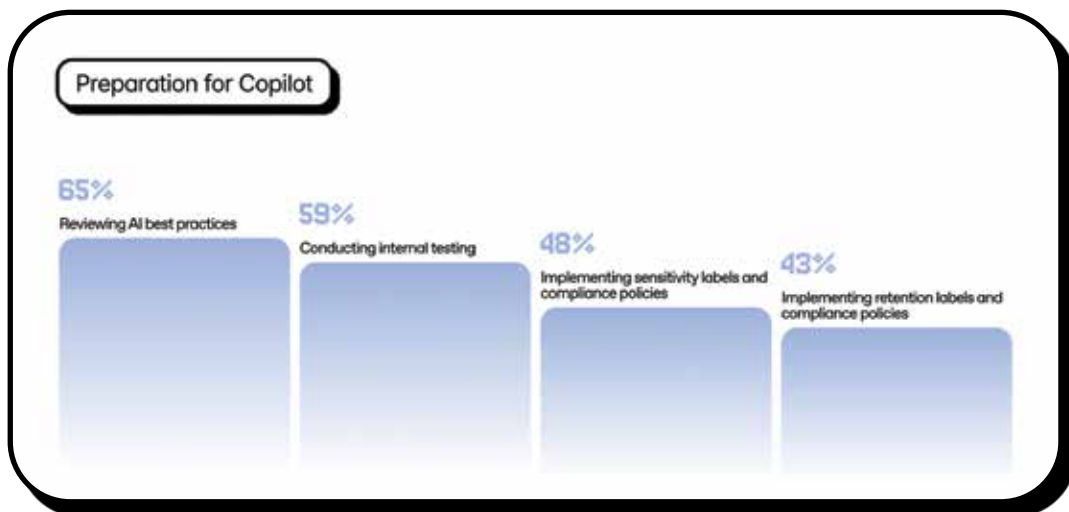
When AI can instantly surface any piece of data a user has access to, even routine governance work—like archiving stale sites or tightening guest access—becomes urgent.

These concerns aren’t lost on Microsoft. In fact, the latest roadmap shows governance being baked directly into Copilot. The Copilot Control System enables IT teams to set fine-grained policies—such as Allow web search in Copilot—separately from other connected experiences. This granular tuning gives you more control over how AI behaves.

Meanwhile, Copilot now includes built-in content governance reports and controls via SharePoint Advanced Management, helping teams accelerate adoption securely.

Readiness in practice: Policies, people, and platforms

These new governance controls in Copilot are promising, but they only pay off if your own tenant is already clean and classified. That’s why most teams begin their Copilot prep with tasks they can control right away:



These steps are low-friction, budget-friendly, and show visible progress to stakeholders. To help you pull these threads together, here’s a quick Copilot readiness checklist. Use it as your preflight before flipping the switch.

Copilot prep

This checklist is built for IT teams rolling out Copilot to help you secure your environment, clean up data, and get quick wins before flipping the switch.

Use it to gauge your progress and what to tackle next.



Confirm licensing and prerequisites

Make sure every user who'll have Copilot also has a Microsoft Entra ID account, the right Microsoft 365 Apps channel, and a Copilot license.



Enable key Microsoft 365 features

Turn on the apps and services Copilot relies on (OneDrive, new Outlook, Teams transcription or Copilot without transcription, Loop, and Whiteboard).



Bring content into Microsoft 365

Migrate or connect the files Copilot needs so it can surface the right information from day one.



Review and tighten permissions

Audit SharePoint and Teams access, remediate oversharing, and establish a framework for ongoing permissions governance.



Classify and protect data

Use Microsoft Purview sensitivity and retention labels so Copilot only works with data that's properly governed.



Pilot with a small group

Run a limited rollout to test policies, permissions, and user behavior before expanding.

If you're staring at hundreds of overshared sites or inconsistent labels, you don't have to fix them one by one. ShareGate Protect's built-in Governance risk assessment and bulk actions make it easy to audit, prioritize, and clean up at scale. This automated power puts your Copilot rollout on solid ground.

However, readiness momentum slows when the work shifts from setting policies to cleaning up the environment at scale. As we discussed in the chapter *Who's governing Microsoft 365?*, only 1% of respondents have adopted a purpose-built governance platform. Another 94% default to Microsoft's built-in tools or manual scripts to audit access, retire stale sites, and bulk-fix permissions. The last 5% said they don't do governance at all.

This over reliance on manual effort creates an unsustainable governance or technical debt. It requires deep expertise and countless hours that IT teams simply don't have.

"Proactive investment in automation and governance accelerates AI adoption and maximizes ROI while reducing risk."



Richard Harbridge
Microsoft MVP

This is where a tool like ShareGate can change the equation. ShareGate's Governance risk assessment consolidates data hygiene insights, allowing IT to fix permissions or retire stale sites in bulk without the need for months of custom scripting. By automating the heavy lifting, teams shorten the runway to a secure, organization-wide Copilot rollout.

The IT team at Arkin used to spend hours every month managing their tenant. Vera Van Es, Arkin's Function Microsoft 365 Administrator, told us about how time-consuming the process was:

"Before ShareGate, it cost us so much time to manage inactive teams. Now, we have an instant view, and we can quickly delete or archive them. Because we don't have to spend as much time keeping the environment tidy, we can do more to help the business."

As you absorb all these signals from Microsoft and the data from your peers, one trend stands clear: data governance and security are no longer optional.

Microsoft is making it evident that AI, security, and data protection are co-equal pillars, not separate tracks. As pilots expand to production and data volumes grow, the gap between governance needs and manual capacity will only widen.

Teams that invest in scalable governance automation today will build the secure foundation Copilot and other AI workloads need to succeed. Those that postpone risk watching complexity outpace their capacity just as AI adoption accelerates.

Yet until budget cycles align or compliance pressure peaks, most organizations continue to manually chip away, reviewing sites one by one, exporting CSVs, and scripting fixes, as Arkin used to do. Marc Anderson feels this is shortsighted:

“The hours you spend hopping between half-baked dashboards easily outweigh the price of a real tool.”



Marc Anderson
Microsoft MVP

That’s why Microsoft is layering more native signals into Copilot. It’s also the reason why tools like ShareGate Protect are becoming indispensable for translating those raw signals into prioritized, actionable fixes before you scale AI across your tenant.

Key lessons from the data

The race to deploy Copilot is on, with over 80% of organizations already in the game. But this rush to unlock AI's promise is shining a harsh light on years of messy data and leaky permissions. The data shows how IT can lead a rollout that delivers rewards, not risks.

Three actions rise to the top:



Lead with a governance-first mindset.

IT teams—not executives—are driving Copilot adoption (81%). Use this position to be the strategic leader who builds in security and data hygiene from the start.



Tackle the top two fears head-on: data and oversharing.

Your peers' most significant concerns about Copilot are poor data quality (58%) and insecure access management (57%). Make automated permissions auditing and data cleanup a non-negotiable first step to prevent Copilot from exposing sensitive information.



Bridge the expertise gap with automation.

More than a third (36%) of IT teams admit they lack the expertise for AI governance. The scalable solution is to invest in a tool that automates best practices and builds the secure foundation AI needs to succeed.

Copilot's business value is within reach, but without automated, scalable governance, most IT teams will struggle to keep pace as adoption accelerates.

07

From pressure to payoff: An IT leader's mandate for 2026





From pressure to payoff: An IT leader's mandate for 2026

This book began with a single, undeniable reality: we are in a cloud crunch. It's a period defined by the relentless pressure of looming deadlines, the dizzying complexity of mergers, and the disruptive promise of AI.

At the same time, Microsoft's own roadmap makes clear that AI, security, and data protection will rise together as co-equal pillars. The journey through these pages has navigated this storm, moving from the chaos of colliding forces to the clarity of a strategic roadmap.

We confronted the SharePoint EOS deadline, a challenge pulling three-quarters of organizations from the sidelines. We uncovered how the 80% prevalence of M&A makes tenant-to-tenant integration the new standard, turning security and permissions into the ultimate test. We stared down the security paradox and saw that the path forward is built on capability, not location. Finally, we saw how Copilot turns governance from a perennial backlog item into an urgent, top-priority opportunity.

And throughout, we highlighted Microsoft's own investments, like Purview's expanded certifications, Entra's workload identity controls, and Copilot's built-in governance guardrails. These advancements demonstrate how Microsoft is aligning its roadmap to the same pressures you face.

The journey leads to one conclusion: the organizations that thrive will be those that see these challenges not as separate fires to be extinguished, but as interconnected pillars of a single modernization mandate. In this linked setup, governance is not a box-checking exercise but the connective tissue across migrations, M&A, and AI adoption.

This understanding provides a decisive advantage: a data-backed playbook while others are still reacting to the pressure.

The path from crunch to catalyst can be distilled into three immediate actions:

Turn deadlines into drivers

Treat the SharePoint EOS deadline not as a defensive scramble, but as the budget-backed mandate to modernize. Your peers have proven that, with early discovery and the right tools, this is a race that you can win in under six months, setting you up to tackle 2026 on offense.

Weaponize your M&A playbook

With 80% of teams in the M&A cycle, integration is no longer a rare event but a core competency. Build a repeatable process with a pre-vetted toolkit, making security your non-negotiable first principle. Use Microsoft's new cross-tenant migration features and ShareGate's permissions and sensitivity-label migration to reduce friction and risk.

Frame governance as your AI foundation

The "garbage in, garbage out" principle of AI underscores the importance of governance as the foundation of Copilot's success. Pair Microsoft's latest controls—like the Copilot Control System and Purview's automated retention—with ShareGate Protect's continuous risk and sprawl detection to automate cleanup, rein in oversharing, and create the trustworthy data foundation AI needs to deliver value.

As Microsoft MVP Richard Harbridge notes, this is a "critical opportunity to build the foundation for Copilot and stronger security."

Microsoft is rolling out the building blocks, and ShareGate Protect provides the operational muscle to make them a reality in your tenant. The pressure we're feeling isn't something to be survived. It's a force to be harnessed.

The insights are here. The roadmap is clear. The opportunity is now.

08

Acknowledgments and methodology





Research foundations

This book was developed by ShareGate. Findings are grounded in an independent survey of mid-market and enterprise IT professionals conducted in March 2025. The data was supplemented by expert interviews and secondary analysis.

Expert contributors

We're grateful to these subject-matter experts for sharing their insights and for their ongoing partnership and guidance:



Antonio Maio
Microsoft MVP and Managing Director
Protiviti



Joanne Klein
Microsoft MVP and Advanced Compliance Consultant
NexNovus



Andy Huneycutt
Microsoft MVP and Senior Technical Specialist
Atrium Health



Marc Anderson
Microsoft MVP and Co-Founder and CEO
Sympraxis Consulting



Christian Buckley
Microsoft MVP and Fractional CMO
Smarter Consulting



Ragnar Heil
Microsoft MVP and Business Development Manager
Microsoft



Eric Overfield
Microsoft MVP and CIO
Creospark



Richard Harbridge
Microsoft MVP and Technology & Ecosystems Strategist
ShareGate



Ian Loman
Cloud expert
Adepteq



Sarah Haase
Microsoft MVP and Principal Product Manager
U.S. Bank



Jasper Oosterveld
Microsoft MVP and Data Security Consultant
Rubicon Cloud Advisor

Survey partner

To ensure methodological rigor, we partnered with Dig Insights, an award-winning insights firm with more than 250 research professionals across North America and Europe.

Dig Insights designed and executed the study—recruiting, weighting, and analyzing responses from 650 mid-market and enterprise IT professionals in the US, Canada, the UK, Germany, and France—to deliver vendor-neutral, statistically sound findings.

About this book

This publication is part of ShareGate's ongoing research into Microsoft 365 migration, governance, operations, and administration. Our objective is to help technology leaders:

- **Understand the forces shaping IT practices**
- **Identify high-impact opportunity areas**
- **Prepare for the next wave of organizational growth**

All survey responses are vendor-neutral and were neither commissioned nor sponsored by any external entity.

Join the conversation

Feedback and dialogue strengthen our work. Connect with us on LinkedIn, visit sharegate.com/blog to access additional resources, or subscribe to our newsletter for future research.

Glossary

The following terms in this book are defined specifically for its context.

AI readiness

An organization's state of preparation for implementing and leveraging artificial intelligence technologies like Microsoft Copilot. This includes having clean, well-organized, and properly permissioned data, as well as established governance policies.

Cloud-first strategy

An organizational approach where new initiatives and solutions are designed to use cloud-based services by default over on-prem solutions.

Compliance

Adherence to regulations, standards, and policies relevant to an organization's industry and location. In the context of this book, it often refers to data privacy and security frameworks like GDPR, HIPAA, and ISO.

Copilot

Microsoft's AI-powered assistant integrated into Microsoft 365 applications. It uses large language models to provide generative AI capabilities, such as creating content, summarizing documents, and automating tasks based on the user's organizational data.

Data governance

The overall management of the availability, usability, integrity, and security of an organization's data. It involves establishing policies and procedures to ensure data is handled consistently and correctly.

Data hygiene

The process of ensuring that data is clean, accurate, and free of errors or duplications. Good data hygiene is crucial for the effective functioning of AI tools like Copilot.

Data sprawl

The uncontrolled proliferation of data across an organization's IT systems, often leading to disorganization, duplication, and difficulty in finding and managing information.

Delta cutover

The final stage of a migration process where only the changes (the "delta") that have occurred since the last major data copy are moved to the new environment. This minimizes downtime.

Divestiture

The process of a company selling off a subsidiary business unit or assets. In an IT context, this often requires a tenant-to-tenant migration to separate the divested entity's data.

End-of-support (EOS)

The point at which a software vendor, like Microsoft, ceases to provide security patches, bug fixes, and technical assistance for a product. Continuing to use software after its EOS date poses significant security risks.

Evergreen security

A security posture that is continuously updated and maintained, typically by a cloud provider like Microsoft, ensuring that systems are always protected against the latest threats.

External sharing

The practice of granting access to internal files, folders, or sites to individuals outside of the organization. If not properly managed, this can be a significant security risk.

File shares

A traditional method of storing and sharing files on a central server within an organization's local network. Many organizations are migrating from file shares to cloud-based solutions like SharePoint Online and OneDrive.

Governance emergency

A critical issue arising from a lack of proper data governance, such as running out of external sharing links in a single document library, which can halt business operations.

Hybrid model

An IT environment that combines on-premise infrastructure with cloud-based services. For example, an organization might keep some sensitive data on-premise while using Microsoft 365 for collaboration.

Incremental copy

A migration technique where, after an initial full copy of data, subsequent copies only transfer new or modified data. This is a key feature of delta cutovers.

Information architecture

The structural design of shared information environments. In the context of SharePoint and Microsoft 365, it involves organizing content in a way that is intuitive and easy to navigate.

Lift-and-shift migration

A migration approach where an application or workload is moved from an on-premise environment to the cloud with minimal or no changes to its architecture.

M&A (mergers and acquisitions)

The consolidation of companies or assets through various financial transactions. M&A events are a major driver of complex tenant-to-tenant migrations.

Microsoft 365

An integrated suite of cloud-based productivity and collaboration applications, including SharePoint Online, Teams, Exchange Online, and OneDrive, along with security and management tools.

Microsoft Entra ID

Formerly known as Azure Active Directory, this is Microsoft's cloud-based identity and access management service. It is central to securing access to Microsoft 365 resources.

Microsoft Purview

A family of data governance, risk, and compliance solutions from Microsoft. This includes capabilities for sensitivity labeling to classify and protect data.

Native tooling

Migration and management utilities that are provided by the primary software vendor, in this case, Microsoft. While often included in existing licensing options from Microsoft, they may incur a cost and many lack the advanced features of third-party solutions.

On-premise (on-prem)

IT infrastructure, such as servers and software, that is located and managed within an organization's own physical facilities, as opposed to in the cloud.

Permissions Matrix

A detailed report or view that shows which users have what level of access to specific files, sites, and other resources. This is a crucial tool for security and compliance audits.

SharePoint

A web-based collaborative platform from Microsoft that is primarily used for document management and storage. The book focuses on the migration from on-premise versions (SharePoint 2016/2019) to SharePoint Online.

SharePoint Server Subscription Edition

The on-premise version of SharePoint that organizations can run in their own data centers, which receives continuous updates and support from Microsoft.

Technical debt

The implied cost of rework caused by choosing an easy (limited) solution now instead of using a better approach that would take longer. In the context of migrations, a "lift-and-shift" approach can create significant technical debt.

Tenant-to-tenant migration

The process of moving data, users, and workloads from one Microsoft 365 environment (tenant) to another. This is a common and complex requirement during mergers, acquisitions, and divestitures.

Third-party tools

Specialized software solutions developed by vendors other than Microsoft to provide more advanced capabilities for migration, governance, and management of Microsoft 365.



Ready to ShareGate?

Microsoft 365. **We got this.**

We still live and breathe migration, but we've grown into so much more. Built from real conversations with IT pros and partners, ShareGate makes it simple to assess, migrate, and govern Microsoft 365 clearly and confidently. Our out-of-the-box solution gives you the visibility and control you need to keep your environment secure and your users empowered, without the complexity.

