The Confidence Gap:

State of M365 Governance Report

Syskit

Gradually, then suddenly

There is a line in Hemingway's The Sun Also Rises where a character is asked how he went bankrupt. "Two ways," he says. "Gradually, then suddenly."

That is how Microsoft 365 governance fails.

Gradually: **a site shared with the whole company because it was faster that way.** A guest account from a project that ended two years ago. A workspace whose owner left, whose files stayed. None of it looks like a decision. All of it is one.

Then suddenly: **an auditor asks who can access what, and the honest answer takes three days.** An AI assistant, doing exactly what it was told, surfaces a document nobody remembered was open to everyone. The gradual becomes the sudden in a single search result.

This report measures the distance between those two moments. We asked 327 IT and security leaders in the US and UK, the people who actually hold the keys, **how their organizations govern the platform where their most sensitive work lives.** They were remarkably candid. More than eight in ten are confident they know who has access to their data. Nine in ten have also had a confirmed or suspected incident say otherwise.

We commissioned this research because the industry is racing to deploy AI on foundations nobody has inspected, and we would rather everyone see the inspection report. The gap between what we believe about our environments and what is true of them is the **defining security question of the AI era**. AI does not break your permissions. It believes them.

Read this report the way the best leaders read anything: not to confirm what you already think, but to find the number that makes you uncomfortable. It is in here. It is probably in your tenant, too.

Toni Frankola
CEO, Syskit

ABOUT THIS REPORT

What this is

The State of M365 Governance Report is based on original research commissioned by Syskit and conducted by Censuswide among 327 IT and cybersecurity decision-makers responsible for Microsoft 365 governance. All respondents work in organizations of 500 or more employees across the United States and the United Kingdom. Fieldwork ran from 18 May to 2 July 2026.

This is an evidence-based look at how organizations govern the platform where their most sensitive work lives: who has access, who is accountable, what it costs, and what happens when AI is layered on top.

Why now

Microsoft 365 has quietly become the largest unstructured data estate most organizations own, and AI, in all its forms, is now reading it. Copilot was only the front door: enterprise AI assistants, connectors and agents all authenticate into the same tenant and inherit the same permission model. None of them create new access.

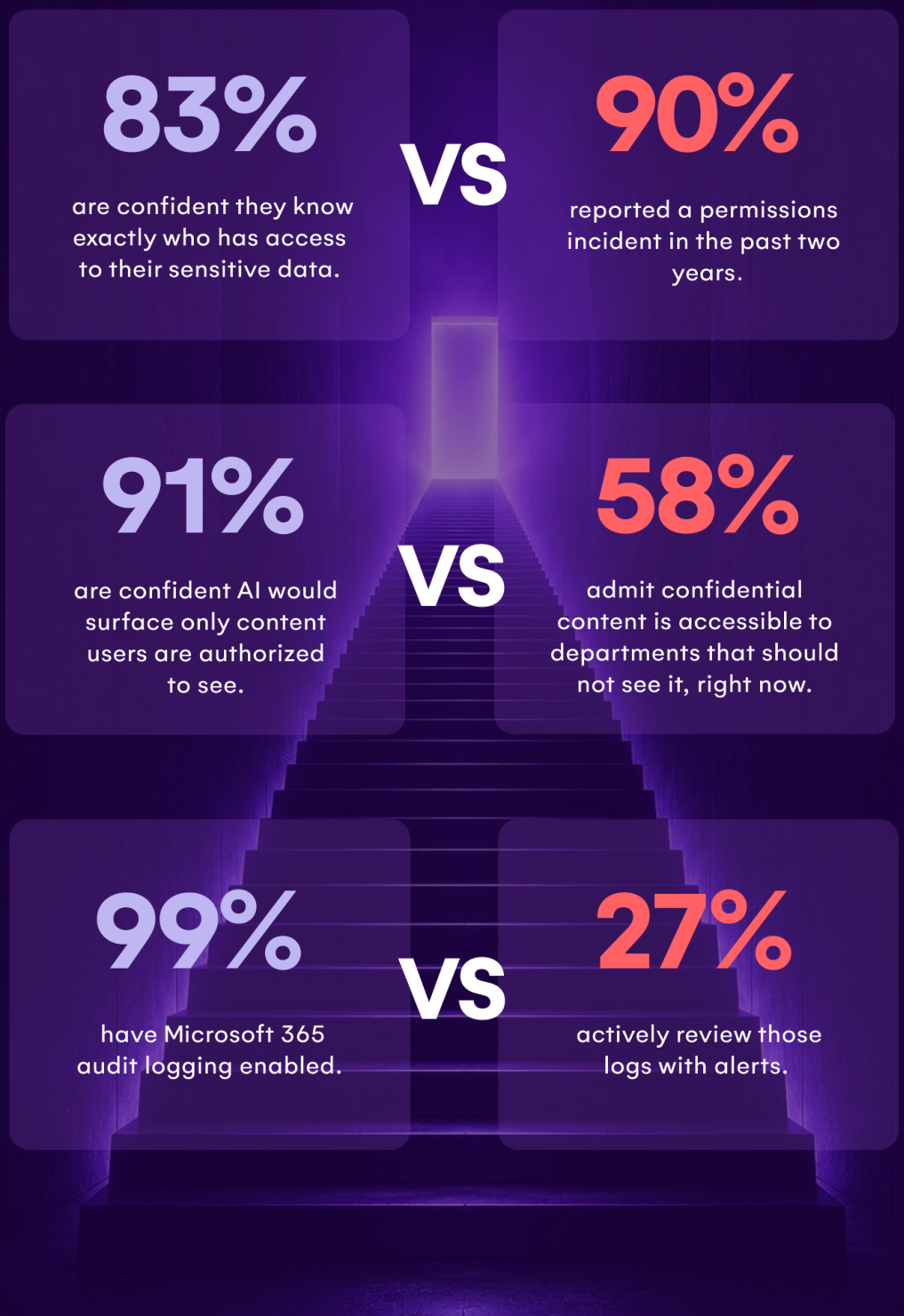
They use the access that already exists, at machine speed and at scale. In this study, 76% of organizations have already deployed or piloted AI tools that touch their M365 data. The distance between how well organizations believe that data is governed and what this research found is the subject of this report.

How to read it

Findings are organized into seven chapters, from governance maturity through to what would trigger investment. Along the way, you will find recurring elements: Reality Check callouts pairing confidence against contradicting evidence, Across the Atlantic notes comparing US and UK responses, Expert Lens commentary from Microsoft MVPs and Syskit leadership, and Voices from the field, respondents' answers in their own words.

THE GAP AT A GLANCE

327 IT and security decision-makers from the US and UK told us how their Microsoft 365 environments are governed today, and where the exposure lies.



THE GAP AT A GLANCE

5%

rate their Microsoft 365 governance as optimized.

The other 95% are somewhere on the way.

4%

could produce a full access report within an hour if an auditor asked today.

For most, the honest answer is measured in days.

43%

conducted a thorough permissions review before deploying AI.

The rest opened the front door before checking the locks.

CHAPTER 1

Where governance stands today

1 in 20

organizations call their Microsoft 365 governance optimized.

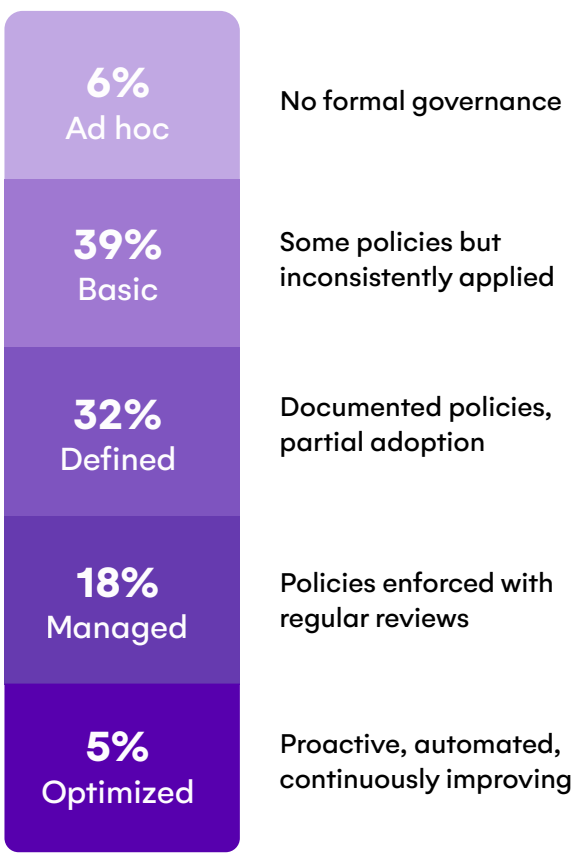
Before measuring the gap, we asked organizations to place themselves on the map. Their own answers set the baseline for everything that follows: maturity is modest, accountability is thin, and the boardroom is only half watching.

1.1 The maturity curve

Most governance is a work in progress. By its own admission.

Asked to rate the overall maturity of their **Microsoft 365 governance**, respondents placed themselves with unusual honesty. Just 5% claim the top level, optimized: proactive, automated, continuously improving. Only 18% more reach managed, with policies enforced and regularly reviewed. The center of gravity sits below: 32% describe their governance as defined but only partially adopted, 39% as basic with policies inconsistently applied, and 6% as outright ad hoc.

Read plainly: **77% of organizations,** by their own assessment, have governance that is not consistently enforced. And self-assessment tends toward optimism: these are decision-makers describing their own function. The chapters that follow test these self-ratings against what the same respondents told us about their day-to-day practices, and against what they admit is in their environments. The ratings do not survive the comparison.



1.2 Who owns governance?

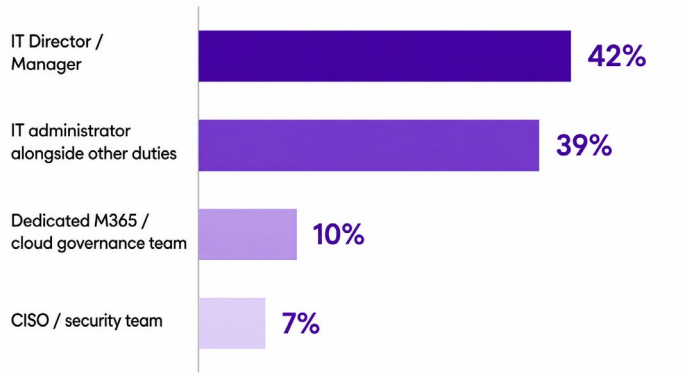
The largest content estate in the company is a part-time job.

Accountability for Microsoft 365 governance most often sits with an IT Director or Manager (42%) or with an IT administrator handling it alongside other duties (39%). Only 10% have a dedicated M365 or cloud governance team. Just 7% place accountability with the CISO or security team, a striking number given that everything in this report, access, oversharing, incidents, is a security surface.

The resourcing matches the org chart. Half of organizations dedicate one to two full-time equivalents to governing the platform, 45% manage three to five, and 5% get by with less than one person. For an estate holding thousands of users, tens of thousands of workspaces and the organization's most sensitive documents, governance is typically a desk, not a department.

Later chapters show what that desk is up against: manual reviews, self-written scripts, and now AI.

Who is primarily accountable for Microsoft 365 governance?



How many full-time equivalents (FTEs) are dedicated to Microsoft 365 governance?

Each icon represents 10% of organizations (n=327)

ACROSS THE ATLANTIC

The gap has a different owner on each side of it. In the UK, governance is director-led (50% vs 34% in the US). In the US, it lands on administrators with other duties (48% vs 31%). Same thin accountability, different org chart.

1.3 The board gap

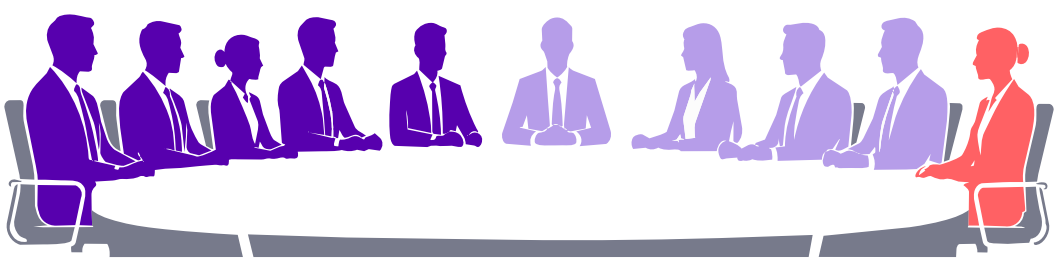
Half the boardroom is watching. The other half is waiting for an incident.

Governance rises or falls on leadership attention, and attention is split almost exactly in two. Half of respondents (50%) say their board or senior leadership is very well informed and actively engaged with the risks of poor M365 governance. Nearly as many (47%) say leadership is somewhat aware but does not treat governance as a priority. Only 3% report minimal awareness or none.

50%
Very well informed and actively engage with the risks of poor M365 governance

47%
Somewhat aware but do not treat governance as a priority

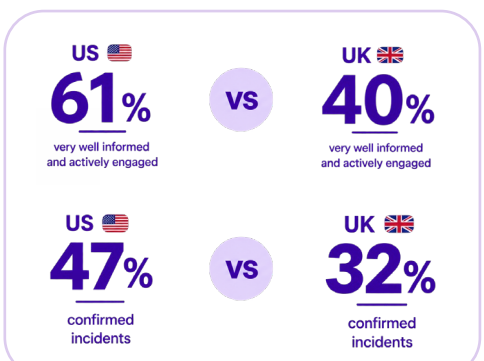
3%
Minimal awareness or none



That second group matters more than its label suggests, because of what comes later in this report: asked what would trigger more investment in governance tooling, the single most cited answer is a leadership mandate following a board-level discussion (45%). The people whose attention is missing are the same people who unlock the budget. For nearly half of organizations, governance is waiting on a conversation the board has not prioritized having, and the alternative triggers on that list, an audit finding, an incident, a breach, are all more expensive ways to start it.

ACROSS THE ATLANTIC

US boards report far higher engagement, 61% very well informed against 40% in the UK, the largest transatlantic gap in the study. Yet US organizations also report more confirmed incidents (47% vs 32%). Attention, it turns out, is not the same as control. Chapter 2 explains why.



Two or three years ago, Microsoft 365 governance was often viewed as an IT housekeeping exercise rather than a business priority. If users technically had access to information they didn't need, but didn't know it existed, most organizations weren't overly concerned. AI has changed that completely. Tools like Copilot can instantly surface content from across Microsoft 365 using the permissions users already have, exposing years of oversharing, excessive access, forgotten sites, and ownership gaps. That's why ***visibility has become the foundation of governance****; you can't manage, secure, or govern what you can't see. Organizations first need to understand who has access to what, who owns it, and where sensitive information is exposed before they can control it.*

AI doesn't create new permissions; it shines a spotlight on existing ones. The risk is no longer hidden, and once people discover they can access information they shouldn't, the real question is often not if that access will eventually be misused, but when. Effective governance is therefore about creating visibility, accountability, and control before AI exposes the gaps for everyone to see.

FRANE BOROZAN,
Microsoft MVP

Three moves to make now

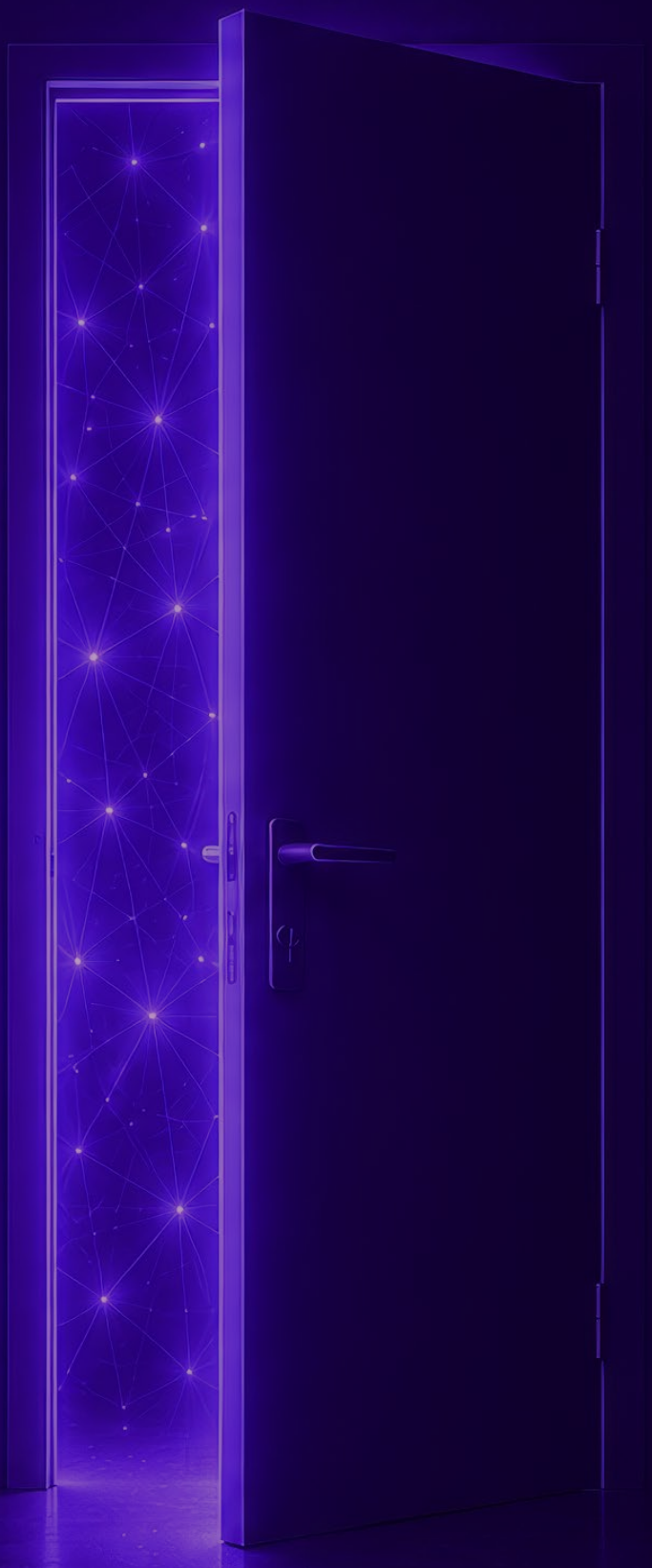
01 **Name a single accountable owner for M365 governance, with the role written down, not assumed.**

02 **Put M365 governance on the board risk register, so the conversation stops depending on an incident to start it.**

03 **Baseline your maturity honestly against the five-level scale in this chapter, and reassess annually.**

"Most parts of the business focus on doing their day jobs to the best of their ability. Data security is rarely front and centre, until one day we'll have a problem."

Survey respondent, asked in their own words to name the biggest barrier to better Microsoft 365 governance. Responses lightly edited for spelling and length.



CHAPTER 2

The Confidence Paradox

9 in 10

organizations experienced a confirmed or suspected security incident tied to misconfiguration or over-permissioned access in the past two years.

Confidence about Microsoft 365 access is nearly universal. So is the evidence against it. This chapter puts the two side by side: what organizations believe about who can reach their sensitive data, what they actually do to verify it, what they admit is exposed anyway, and the incidents that followed. Every answer in this chapter comes from the same people.

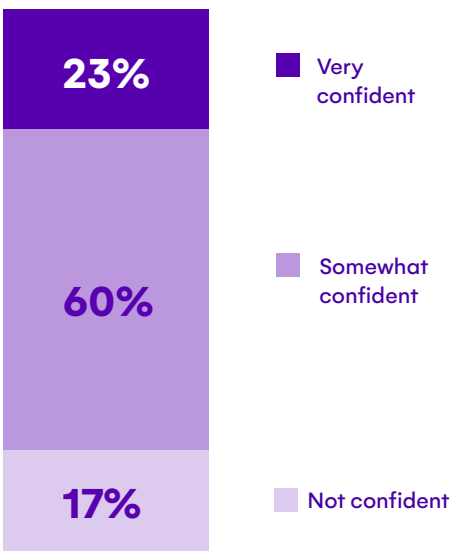
2.1 What they believe

Everyone is confident, but almost no one is certain.

Ask organizations whether they know exactly who has access to sensitive data at any given moment, and 83% say they are confident. But the composition of that confidence deserves a closer look: only 23% are very confident. The remaining 60% are somewhat confident, which in access **governance is less an answer than an open question.**

This is not an isolated reading. Confidence is the default answer throughout this study: 92% are confident departing employees lose access within 24 hours, 91% are confident AI tools would surface only authorized content. Whatever the question, roughly nine in ten organizations believe their controls hold, and in every case, the largest group is only somewhat sure.

That qualifier is where this chapter lives. In access governance, "somewhat confident" is not a mild form of assurance. It is what confidence sounds like when there is no practical way to check.



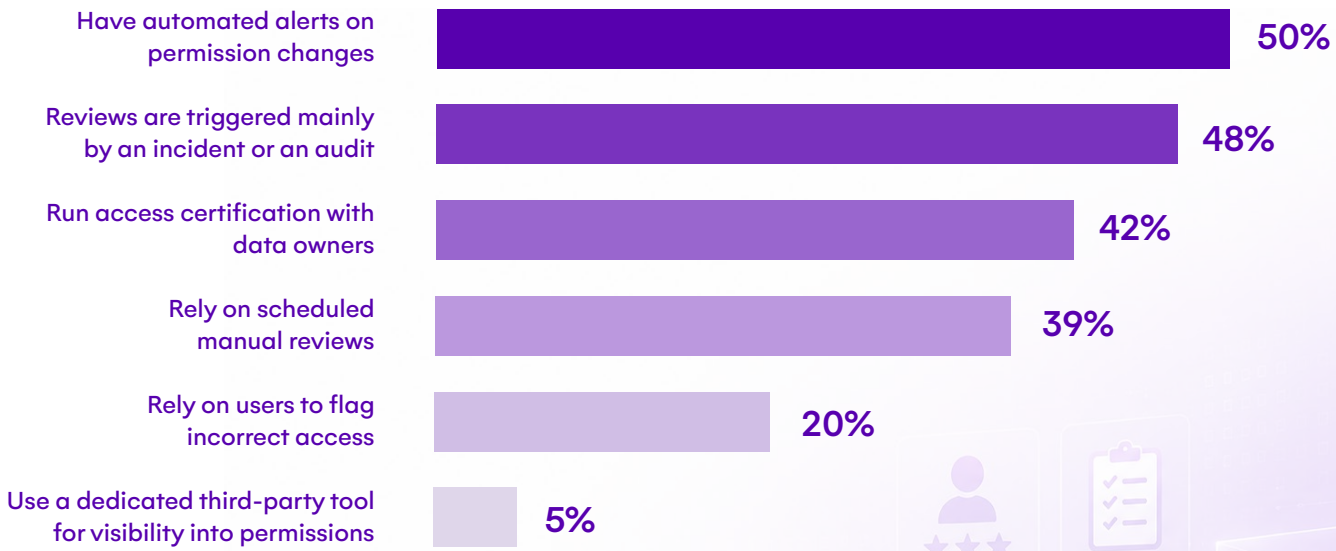
2.2 What they do

For nearly half, a permissions review starts when something has already gone wrong.

Confidence should rest on process, so we asked what organizations do to keep permissions accurate. Half (50%) have automated alerts on permission changes, and 42% run access certification with data owners. But 48% say reviews are triggered mainly by an incident or an audit, 39% rely on scheduled manual reviews, and one in five (20%) rely on users themselves to flag incorrect access. Only 5% use a dedicated third-party tool for permissions visibility.

Guest access, the fastest-moving part of any permission model, gets reviewed continuously in just 15% of organizations. For 44% it is a monthly exercise, for 32% quarterly, and 9% look at it annually or less often.

A review that begins after the incident is not visibility. It is forensics. And periodic reviews, sound practice though they are, are checkpoints, not surveillance: between them, an environment that changes hourly changes unobserved unless something automated is watching. For half of organizations, nothing is.



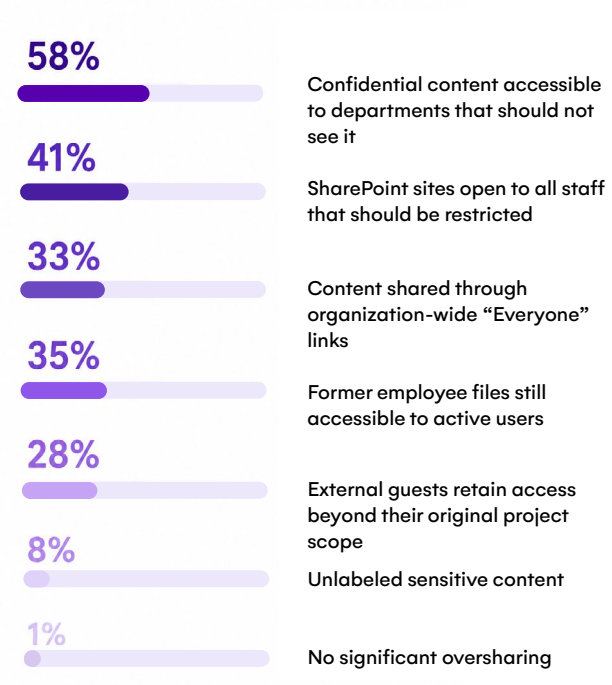
ACROSS THE ATLANTIC

Reactive reviewing is more common in the US, where 55% say reviews are triggered mainly by incidents or audits, against 41% in the UK.

2.3 What is actually exposed

99% acknowledge at least one live oversharing scenario in their own environment right now.

Then we asked what is actually sitting in their environments, and respondents answered against their own confidence. A majority, 58%, say confidential content is accessible to departments that should not see it. 41% report SharePoint sites open to all staff that should be restricted. A third (33%) have content shared through organization-wide "Everyone" links, 35% report former employees' files still accessible to active users, and 28% say external guests retain access beyond their original project scope. Only 8% flag unlabeled sensitive content, and just 1% say their environment has no significant oversharing at all.



Put differently: 99 out of every 100 organizations can name at least one way their own data is exposed today. This is the same population in which 83% expressed confidence about who has access. Both answers came from the same people, often minutes apart.

One nuance for fair reading: files left behind by former employees are not automatically a risk, since teams often need that continuity. They become one when nobody owns or reviews them, which, as the next chapter shows, is the more common condition.

83% are confident they know who has access to sensitive data. 99% acknowledge at least one live oversharing scenario. (Derivation: 100% minus the 1% reporting none.)

83%
confident they know who has access

VS

99%
aknowledge at least one live oversharing scenario

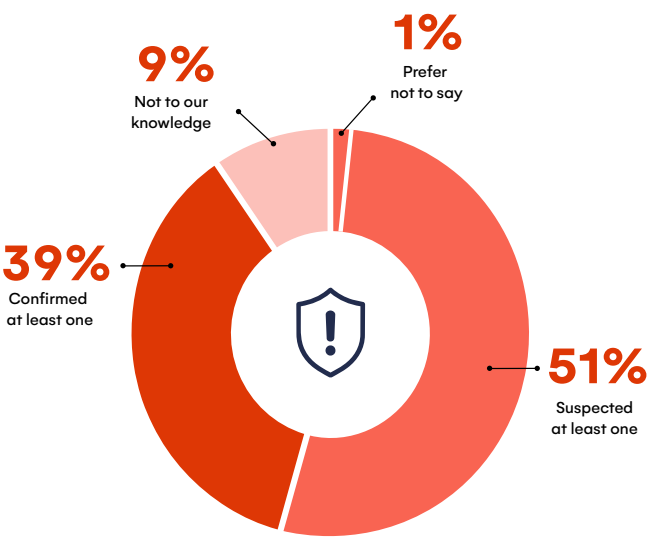
2.4 The receipts

9 in 10 have the incident to prove it.

If confidence were justified, incidents would be rare. They are the norm. Asked whether the organization experienced a security incident or data exposure caused by misconfigured permissions or over-permissioned access in the past two years, 39% confirm at least one outright. Another 51% suspect at least one. Only 9% say not to their knowledge, and even that phrasing, the questionnaire's own, quietly concedes the visibility problem this chapter documents: **you cannot rule out what you cannot see.**

Two years. Nine in ten. Not breaches by sophisticated attackers exploiting unknown vulnerabilities, but exposure through permissions the organization itself configured. The confidence gap is not an abstraction; it has an incident report attached.

To what extent, if at all, has your organisation experienced a security incident or data exposure event in the past 2 years attributable to M365 misconfigurations or over-permissioned access?

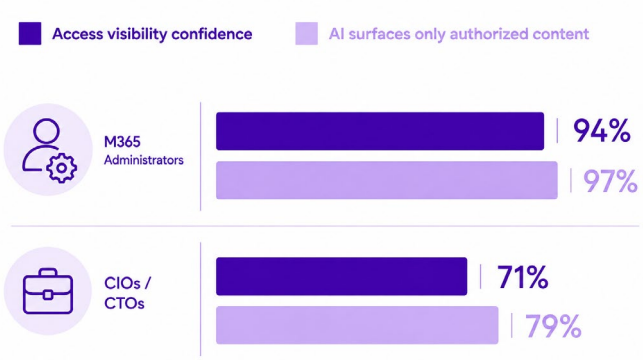


None of this describes careless teams. It describes a platform whose permission model outgrew the headcount, the tooling and the board attention assigned to governing it. The remaining chapters take that machinery apart, piece by piece.

The proximity paradox

Break the confidence question down by role and a second paradox appears.

M365 administrators, the people closest to the systems, are the most confident of anyone: 94% on access visibility, 97% on AI surfacing only authorized content. They also report the most confirmed incidents, at 50%. CIOs and CTOs, furthest from the console, are the least confident on both counts (71% and 79%). Proximity breeds confidence and incident awareness in equal measure, which suggests the confidence is not blindness but familiarity, and the incidents are not rare but routine. The people who see the most have simply stopped expecting the environment to be clean.



ACROSS THE ATLANTIC

Confirmed incidents are markedly more common in the US: 47%, against 32% in the UK. US organizations are also far more likely to report SharePoint sites open to all staff (51% vs 32%).

For me, the most interesting number in this whole chapter is how many people clicked "somewhat confident": a full 60% of them! Let's be real about what that actually means. It's "I really hope we're fine, but I have no way to confirm it for sure." And that is the most dangerous place to be, because ***"somewhat confident" means you don't have the tools or the processes to really know, and you're probably not investing in them either.***

So what finally changes your mind? An incident. And nine in ten people in this study said they've already had one. Look, I'm not blaming anyone here. Budgets are tight, and there's no easy, out-of-the-box tool that gets you to 100%. But "somewhat confident" isn't a strategy. It's a security breach waiting to happen!

VLAD CATRINESCU,
Microsoft MVP

Three moves to make now

01 Run one point-in-time access snapshot on your single most sensitive site, and compare it to what you expected.

02 Review every guest account older than 90 days; treat unreviewed guest access as expired by default.

03 Treat "somewhat confident" as a finding, not reassurance: if nobody can say when access was last verified, it has not been.

"Our IT team just lacks the time and resources to keep up with changing permissions."

Survey respondent, US, asked in their own words to name the biggest barrier to better Microsoft 365 governance. Responses lightly edited for spelling and length.

CHAPTER 3

Sprawl, drift, and ownership

47%

name workspaces with no active owner among their governance challenges, more than any other issue in the study.

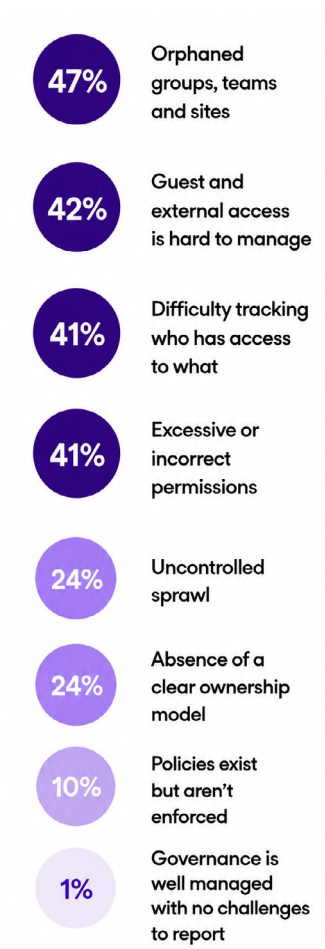
Content outlives the people responsible for it. This chapter follows what happens next: workspaces that lose their owners, ownership models that exist mostly on paper, and an accountability machine that sends reports out but rarely gets decisions back.

3.1 The challenge stack

Four challenges lead the list. All four are the same problem.

Asked which governance challenges their teams currently experience, respondents put orphaned groups, teams and sites at the top (47%), followed by guest and external access being hard to manage (42%), difficulty tracking who has access to what (41%), and excessive or incorrect permissions (41%). Uncontrolled sprawl (24%) and the absence of a clear ownership model (24%) follow. Just 1% say their governance is well managed with no challenges to report.

Look past the labels and the top four converge on a single underlying condition: the organization cannot reliably see the relationship between its people and its content. Who owns this workspace, who was invited into it, who can still reach it, and should they? Every leading challenge is that question wearing different clothes. And notably, only 10% blame unenforced policies, which suggests the problem is not that organizations lack rules. It is that the environment moves faster than anyone can apply them.



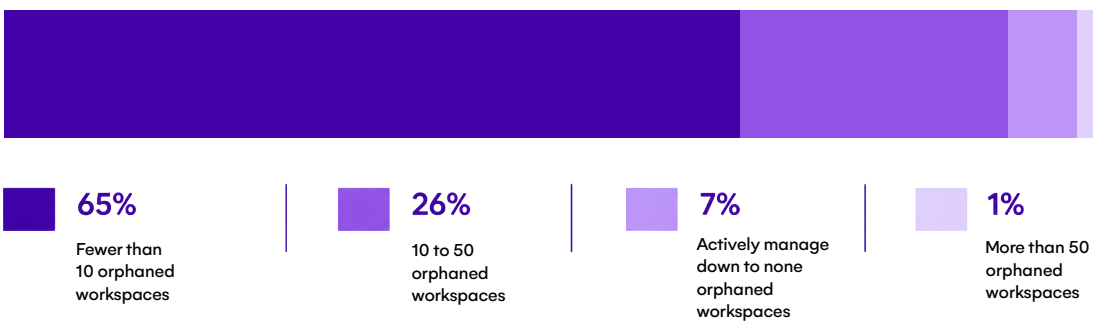
ACROSS THE ATLANTIC

The two regions worry differently. Guest and external access leads in the UK (48% vs 36% in the US); excessive or incorrect permissions weighs heavier in the US (46% vs 36%).

3.2 The orphan estate

More than 9 in 10 carry workspaces that nobody owns.

An orphaned workspace is a team, site or group whose owner has left the organization or moved on, leaving content, members and permissions with no accountable human attached. Asked to estimate how many they currently have, 92% of respondents report at least some: 65% estimate fewer than ten, 26% put the number between ten and fifty, and 1% report more than fifty. Only 7% say they actively manage orphaned workspaces down to none.



The survey measured the scale of the problem and how much it frustrates the people managing it. It did not ask why, so what follows is interpretation rather than finding, but the mechanics of orphanhood point to an answer. Ownership is where access decisions live. The day an owner leaves, a workspace's permissions freeze exactly as they were: every member, every guest, every sharing link persists, **and it is no longer anyone's job to ask whether they still should.** Every accountability mechanism in this chapter quietly assumes an owner exists: certification needs someone to certify, IT's periodic reports need someone to read them, a guest review needs someone who remembers why the guest was invited. An orphaned workspace is disconnected from all of it. Its content becomes deletion-proof in practice, because deletion is a decision and there is no decision-maker, which is how orphans quietly accumulate into the storage pressure Chapter 5 documents. And **AI has removed the obscurity that once protected them**: an assistant has no concept of orphanhood, so a five-year-old unowned site answers questions with the same authority as yesterday's curated one, stale content and all.

Here is the puzzle worth sitting with: this same population made orphaned workspaces the most cited challenge in the entire study, yet two-thirds estimate they have fewer than ten. Both answers can be true, and the resolution says something important about the problem. **Orphaned workspaces are not a stock to be cleared once; they are a flow.**

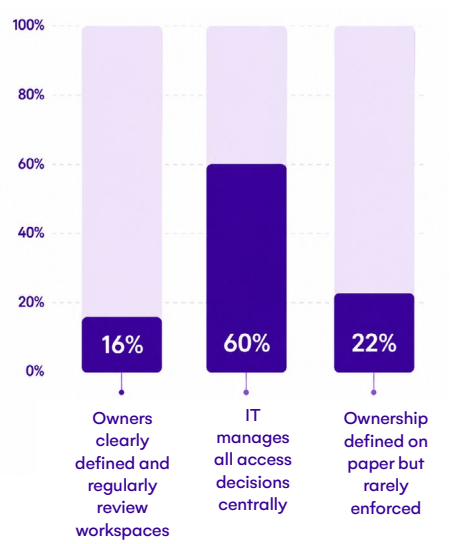
Every departure and every reorganization mints new ones, so even a team that cleans up diligently is running on a treadmill, which is exactly how a small standing number can remain a leading frustration. There is a second, humbler possibility the data cannot rule out: an orphaned workspace is invisible by definition until someone goes looking, and organizations can only count the orphans they have found.

3.3 Ownership on paper

The reports go out. The accountability rarely comes back.

On paper, the accountability machinery looks busy. To keep data owners responsible for their workspaces, 61% of organizations have IT send periodic reports to owners for review, 60% use automated reminders through Microsoft tools, and 39% run a formal access certification process in which owners must periodically re-approve access. 18% use a third-party tool to delegate governance to owners directly.

Then we asked which statement best describes how ownership actually works, and the machinery's output looks different. Only 16% say data owners are clearly defined and regularly review their workspaces. **For 60%, IT manages all access decisions centrally with no delegation to the business** at all, and for 22%, ownership is defined on paper but rarely enforced in practice. In other words: the reports and reminders flow outward, but in more than eight in ten organizations, the decisions they are meant to trigger do not flow back. The people who know what a workspace is for, the department heads and team leads, are the ones least involved in deciding who belongs in it. That leaves **IT making access judgments about content it did not create and cannot evaluate**, which is not a failure of effort. It is a structural mismatch between who has the context and who holds the controls.



Two human realities stand between most organizations and that model, and one respondent in this study named them both in a single sentence: owners reluctant to invest time in reviews, and users who want every file kept forever and reachable always. Neither is a character flaw, and neither is immovable. The 16% with working ownership are proof that participation can be won, and the pattern for winning it runs through this chapter's closing moves: shrink and simplify the ask until reviewing is easier than ignoring, and make retention a decision with an owner rather than a default with none.

ACROSS THE ATLANTIC

Working ownership is where the US leads most clearly: 22% report owners who are defined and actively reviewing, against 10% in the UK. UK organizations lean harder on third-party delegation tooling (23% vs 12%).

Here is the good news buried in this chapter: the answer is already sitting inside your business. The people who know exactly who belongs in a workspace — the finance lead, the team head — are right there, and every organization that struggles with access is one delegation model away from unlocking them. IT has carried this alone for years and done heroic work, but it was never meant to judge content it did not create. Handing that judgment back to the people who own the context is not offloading risk; it is putting the decision where the knowledge already lives.

And it works. The 16% with real, functioning ownership are proof this is winnable, not aspirational — and what they do is refreshingly simple to copy. They made the ask small enough to say yes to a review an owner can finish in two minutes, not an afternoon. They treat ownership as a living process rather than an annual cleanup, so it keeps pace with every new team and reorg instead of falling behind them. None of that requires a bigger budget or a reorg of its own. It requires trusting the business with a decision it is glad to make. Delegation is not just the model that scales — it is the one that makes everyone's job lighter.

GOKAN OZCIFCI,
Microsoft Regional Director and Microsoft MVP

CHAPTER 3

Three moves to make now

01 Inventory ownerless workspaces quarterly, and treat the inventory as a recurring process, not a one-time cleanup.

02 Enforce a two-owner minimum on every new team and site, so a single departure can never orphan a workspace.

03 Pilot access certification with one willing department before rolling it out, and design the review to take minutes, not afternoons: owner participation survives only when the ask is small.

VOICES FROM THE FIELD

"Data owners will never invest the time to participate, and everyone wants to keep all files forever and always have access to them."

Survey respondent, asked in their own words to name the biggest barrier to better Microsoft 365 governance. Responses lightly edited for spelling and length.

CHAPTER 4

The audit stopwatch

4%

could produce a full access report within an hour if an auditor asked today.

Nearly every organization in this study answers to at least one regulator, and nearly every one is confident its controls hold. This chapter tests readiness the way an auditor would: with a request, a clock, and a look at who is actually watching the logs.

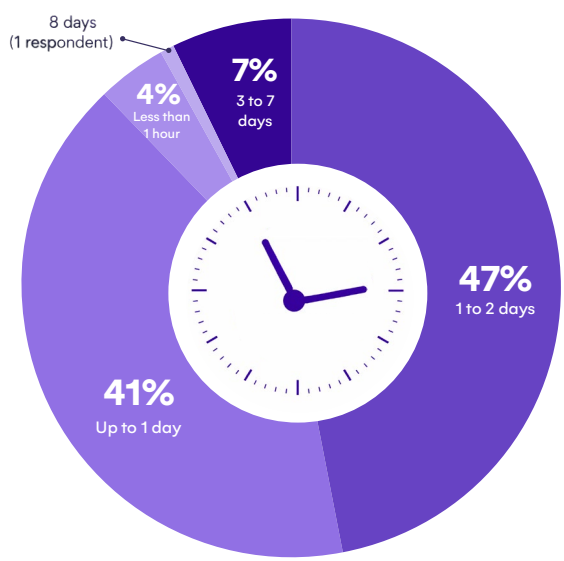
4.1 The stopwatch question

The audit request arrives today. How long until the answer leaves?

We posed a scenario every regulated organization eventually faces: an external audit request arrives requiring a full report on who has access to specific SharePoint sites and Teams, today. How long to produce it? Just 4% say less than an hour. 41% would need up to a day. For the majority, 55%, the honest answer is a day or more: 47% estimate one to two days, 7% put it at three to seven, and one respondent wrote in the far end of the scale, eight days.

Notably, not a single respondent chose "we would not be able to produce this report accurately". Everyone believes the answer is reachable; the question is only how long the reaching takes. And that is the generous scenario, an audit, where days are an inconvenience. Replace the auditor with an incident, and the same report becomes the breach-scoping question: **whose data was reachable, by whom, since when?** The clock that measures audit readiness also measures how long an organization stays blind at the exact moment visibility matters most.

If you received an external audit request requiring a full report on who has access to specific SharePoint sites and Teams today, how long would it take to produce that report?



ACROSS THE ATLANTIC

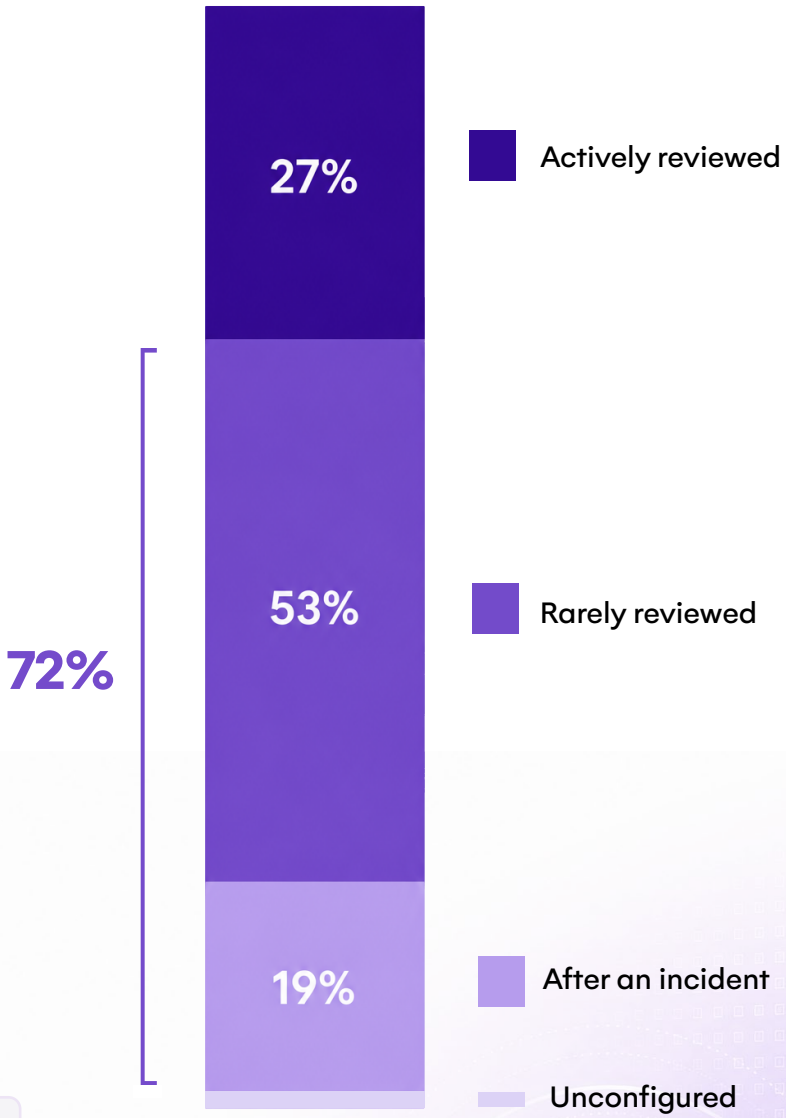
UK organizations edge ahead at the fast end (6% within the hour vs 2% in the US), while US organizations cluster in the up-to-a-day band (45% vs 37%).

4.2 Logs on, eyes off

The recording is on but almost nobody is watching the tape.

Microsoft 365 audit logging is close to universal: only 1% of organizations report it not configured at all. What happens to those logs is another matter. A majority, 53%, say logs are enabled but rarely reviewed proactively. Another 19% review them only after an incident, which is to say, once the log's job has changed from prevention to autopsy. That leaves 27% who actively review their logs with alerts, roughly one organization in four.

Combine the rarely-reviewed and after-incident groups and 72% of organizations are generating an audit trail that no one meaningfully watches. It is a peculiar equilibrium: the evidence is being collected continuously, at storage cost, in a form auditors and investigators will one day demand, and in seven out of ten organizations it accumulates unread. The capability gap of Chapter 2 reappears here in its purest form: **the difference between having visibility and having switched it on.**



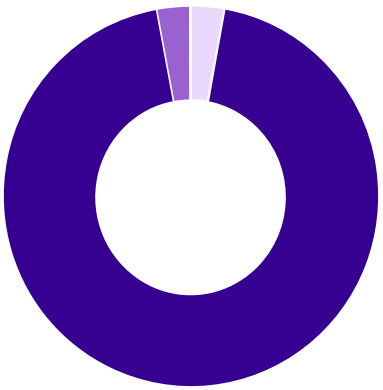
ACROSS THE ATLANTIC

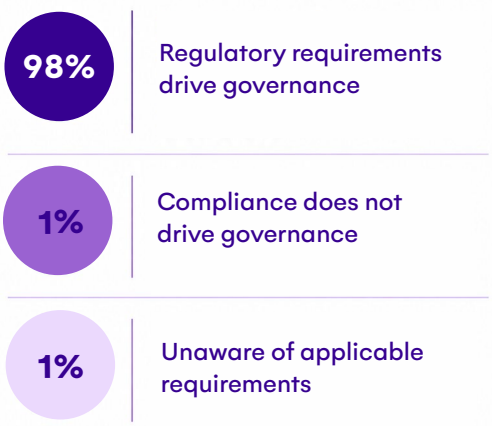
Active review is more common in the US (32% vs 22%). Reviewing only after an incident is a distinctly UK habit: 27%, against 12% in the US.

4.3 Regulated, and only somewhat ready

Almost everyone answers to a regulator, but only a few can answer one quickly.

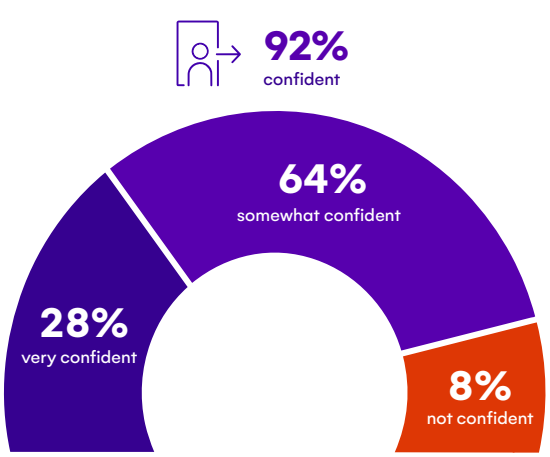
Compliance is not a niche condition in this sample. Asked whether regulatory requirements directly affect their M365 governance approach, respondents named frameworks spanning healthcare, government, security certification, data privacy and financial standards, and just 1% said compliance requirements do not drive their governance at all, with another 1% unaware of applicable requirements. Whatever the framework mix, the practical reality is near-universal: for 98 organizations in every 100, governance is not optional hygiene. It is a regulatory obligation with an examiner attached.





Which makes offboarding, the most auditable process of all, a fitting place to close. When a user leaves, **92% are confident their Microsoft 365 access is fully revoked within 24 hours.** The composition will be familiar by now: 28% very confident, 64% somewhat. Offboarding is where confidence meets the cleanest possible test, because every departure generates a receipt, and the receipts tell their own story in the next chapter.

3% say they have not caught themselves being overcharged or renewing licenses for users who had already left in the past year. (Blocking access does not unassign the license, and unassigning it does not shrink the bill on its own: committed counts carry into the next renewal unless someone right-sizes them first. The renewal is often the first audit an offboarding process ever gets. More in Chapter 5.)



The audit I walked into years ago wanted a binder: the policy, a diagram, a signed statement that controls existed. The audit I walk into now wants a screen — "show me who can open this site, as of today." I personally welcome this shift. Evidence-on-demand rewards the teams doing the real work and lets them prove it in a moment, instead of asking everyone to trust a document. It turns audit day from a scramble into a demonstration.

That is why the 4% who could answer within the hour are the most exciting number in this chapter. They are not outliers to envy; they are a preview of where everyone is heading, and the bar is closer than it looks — this is an afternoon's build, not a year's transformation. Better still, that same fast answer pays off twice. The capability that satisfies an auditor in an hour is the very one that gives you clarity in any moment that matters: who can reach this, and since when. Build readiness once, and you have handed your team confidence for every question that follows. That is a tremendously good place to be.

GOKAN OZCIFCI,
Microsoft Regional Director and Microsoft MVP

CHAPTER 4

Three moves to make now

01 Time yourselves, once, producing a real access report for one sensitive site. The number you get is your actual audit readiness, whatever the policy says.

02 Pick one audit-log alert that matters (permission changes on sensitive sites is a good first candidate) and give it a weekly review slot with a named owner.

03 Test the offboarding process against one real departure from last quarter: access, sessions, shares, and the license. The license is the step most processes miss.

VOICES FROM THE FIELD

"The biggest barrier to better Microsoft 365 governance in our organization is balancing security and compliance requirements with ease of access and productivity for employees."

Survey respondent, US, asked in their own words to name the biggest barrier to better Microsoft 365 governance. Responses lightly edited for spelling and length.

CHAPTER 5

The hidden bill

9 in 10

estimate that at least one in twenty of their Microsoft 365 licenses is unassigned or sitting with an inactive user.

Governance failures are usually described in the language of risk. This chapter describes them in the language of money: licenses committed to people who left, storage bought under pressure, and a tooling stack whose true cost is counted in the hours and the people it depends on.

5.1 Paying for ghosts

The vendor notices before the customer does.

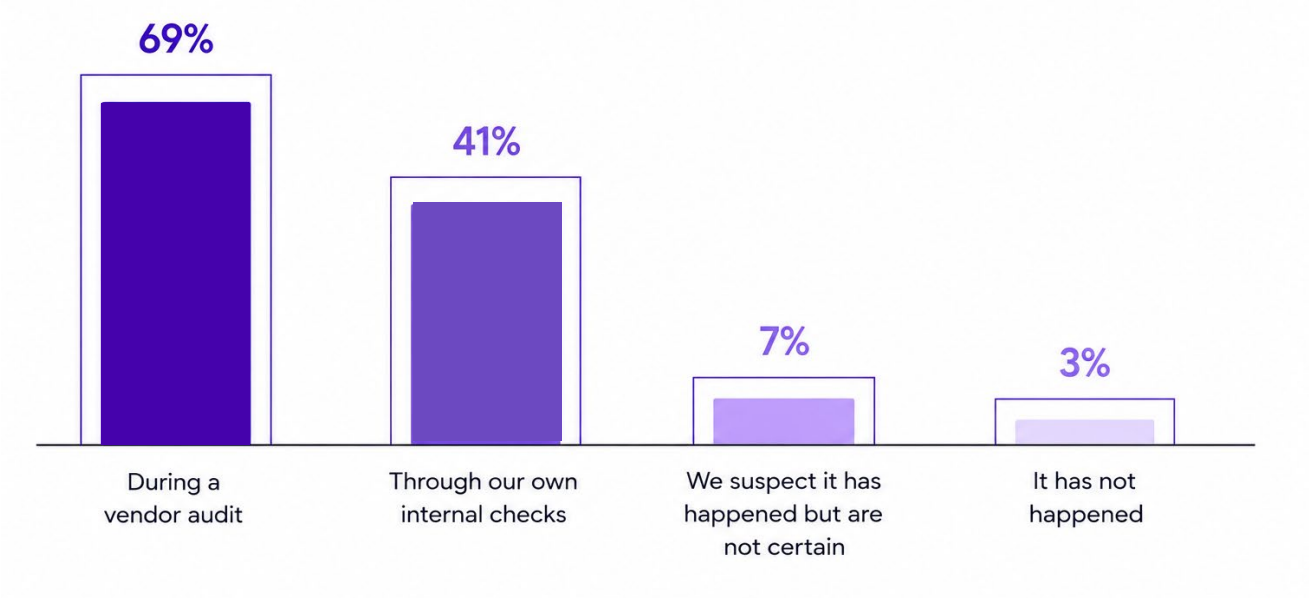
Asked what share of their Microsoft 365 licenses are currently unassigned or assigned to inactive users, 62% of respondents estimate 5 to 10%, and another 30% put it at 11 to 20%. Only 8% believe the figure is under 5%, and just 1% say they genuinely do not know. Taken together, **92% estimate that at least one license in twenty is doing nothing.**

To make that concrete in seats rather than currency: on a 5,000-seat tenant, a 10% idle share is 500 licenses, and because Microsoft billing follows committed counts rather than measured activity, those 500 seats carry into the next renewal unless someone reclaims the licenses and right-sizes the commitment first. The waste is not a leak that drains monthly. **It is a decision the organization re-makes, by default, at every renewal it enters unprepared.**

The receipts say the reconciliation is not happening in time. Asked how they caught being overcharged or renewing licenses for users who had already left in the past 12 months, more organizations say the catch came during a vendor audit (69%) than through their own internal checks (41%). Another 7% suspect it has happened but are not certain, and only 3% say they have not experienced it at all. Read those figures kindly, because they deserve it: this is not carelessness, it is the three-step problem in miniature. Revoking a leaver's access is security's job and mostly gets done, as Chapter 4 showed. Unassigning the license is an inventory task with no deadline. Reducing the committed count is a procurement decision that comes around once a term. Three steps, usually three owners, and the bill only shrinks if all three connect.

CHAPTER 5

How, if at all, has your organization caught being overcharged or renewing licenses for users who had already left the company in the past 12 months? (Multi-select)



There is a more optimistic way to read the same numbers, though it is interpretation rather than finding: **every idle license is also unspent capability**. A reclaimed seat can cover a new joiner instead of a new purchase, or bring an unlicensed team onto the platform.

Later in this study, **43% of respondents name demonstrated cost savings as a trigger that would unlock investment in governance tooling.** The license inventory is the rare governance exercise that can produce that demonstration by itself.

ACROSS THE ATLANTIC

US organizations estimate leaner (68% in the 5 to 10% band vs 56% in the UK, and fewer in the 11 to 20% band), yet report being caught by vendor audits far more often (78% vs 61%).

US 68% estimate leaner in the 5 to 10% band

vs

UK 56% estimate leaner in the 5 to 10% band

US 78% caught by vendor audits

vs

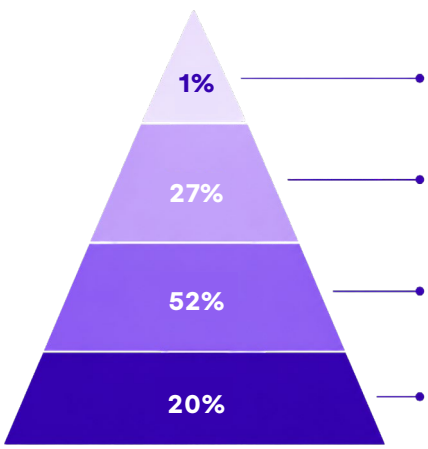
UK 61% caught by vendor audits

5.2 Storage surprises

Four in five learned about their storage the hard way, or nearly did.

SharePoint storage tells the same story on a different invoice. Just 19% of organizations say they actively manage storage and have never been close to their limits. For everyone else, storage is something that happens to them: 52% received warnings and addressed it before hitting the limit, and 27% hit quota limits and had to purchase additional storage. Combined, 79% have either been surprised or warned. Only 1% admit they have never checked.

Which of the following best describes whether your organization has ever been surprised by unexpected Microsoft 365 storage costs or hit a SharePoint storage quota limit?



Never checked
We haven't been surprised because we have never checked

Hit quota limits
We hit quota limits and had to purchase additional storage

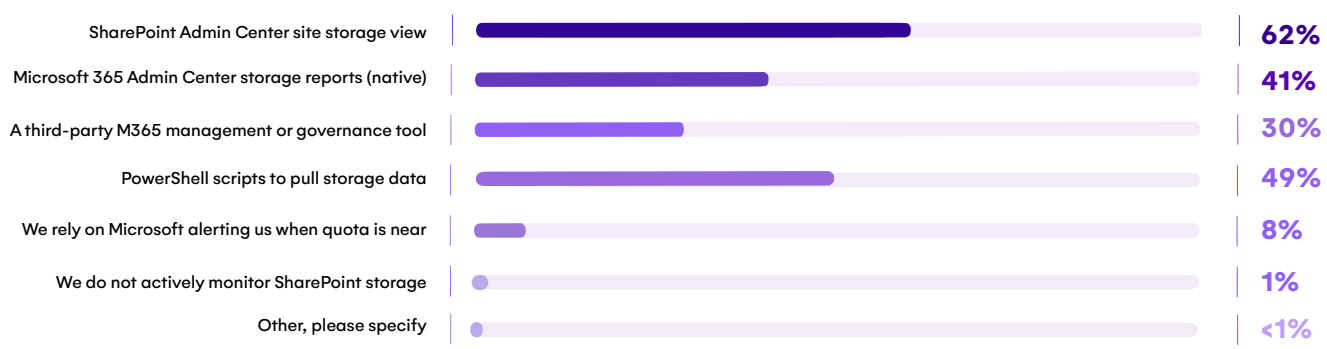
Monitored but not actively managed
We received warnings but addressed it before hitting the limit

Actively managed
Actively manage storage and have never been close to their limits.

ACROSS THE ATLANTIC

Hitting the quota and paying for more is nearly twice as common in the US: 35%, against 19% in the UK.

The monitoring toolkit explains some of the reactivity. Storage consumption is watched mostly through the SharePoint Admin Center's site storage view (62%), native Microsoft 365 storage reports (41%) and PowerShell scripts pulled together to extract the data (50%), with 30% using a third-party management or governance tool and 8% Relying on Microsoft to alert us when quota is near. These are point-in-time views assembled by hand, which is how an organization ends up negotiating storage purchases under deadline pressure rather than on its own schedule.

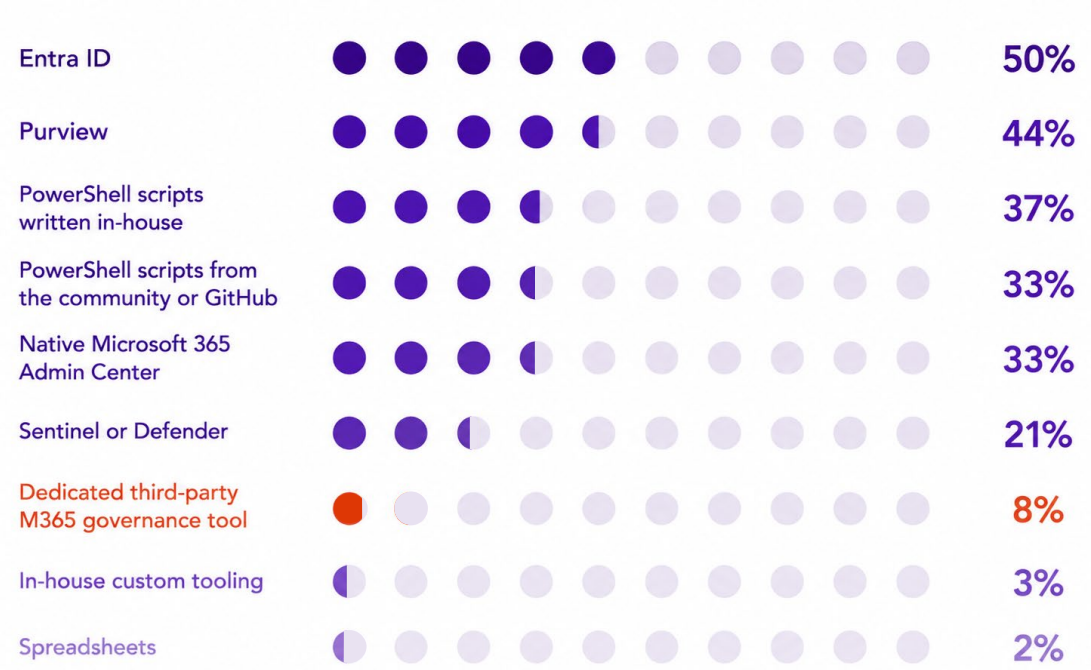


And the connection to the previous chapters is direct: the content that fills this storage includes everything nobody can delete, the orphaned workspaces of Chapter 3 among it, accumulating toward a quota with no owner to answer for it.

5.3 The toolbox

Enterprise governance, held together by scripts and the people who wrote them.

What does the governing itself? Microsoft's own platforms lead: Entra ID (50%), Purview (44%), the native Microsoft 365 Admin Center (33%) and Sentinel or Defender (21%). Alongside them runs a quieter workhorse: more than a third of teams (37%) use PowerShell scripts they wrote themselves, and a third (33%) use scripts from the community or GitHub. A dedicated third-party M365 governance tool is the primary choice for just 8%, with in-house custom tooling (3%) and spreadsheets (2%) rounding out the list.



None of this is bad practice in itself. Native tools are capable, and PowerShell is the honest workhorse of every Microsoft estate. The cost is structural rather than technical, and naming it is interpretation on our part, but the mechanics are plain. A script does exactly what its author understood on the day it was written, runs when someone remembers to run it, and is documented in precisely one place: that person's head.

Set this against Chapter 1's resourcing reality, where half of organizations govern the platform with one to two people, and the fragility compounds: the governance stack and its institutional knowledge frequently share a single point of failure, and that point of failure takes annual leave, changes jobs, and appears in Chapter 4's offboarding statistics like everyone else.

This is also where the economics of the chapter close their loop. One respondent in this study described **the barrier to better governance as staffing and resources aligned to a non-revenue generating activity,** and as a description of perception, it is exact. But the receipts in this chapter say the perception is wrong on its own terms: idle licenses re-committed at renewal, storage bought under pressure, and specialist hours spent maintaining scripts are all real money already being spent. Governance does not need to generate revenue to pay for itself. It needs to stop the spending that nobody decided to do.

ACROSS THE ATLANTIC

Third-party tooling for storage monitoring is a UK habit (36% vs 24%); US teams lean harder on the SharePoint Admin Center view (69% vs 55%).

As someone who literally wrote a book on PowerShell for Office 365, I of course love the tool! But it's surprising how many teams rely on PowerShell alone for their governance. The catch is that PowerShell needs knowledgeable people to maintain those scripts. The cmdlets don't change as often as the UI, but we still get major shifts, like the way the AzureAD and SharePoint PnP PowerShell modules changed over the years. ***And if your organization loses the key person who wrote all those governance scripts, that can quietly open holes in your whole strategy.*** *So depending on the size of your organization and your team, PowerShell might be exactly right, or you might end up spending more time building and maintaining scripts than you would on a third-party governance tool that a dedicated team builds and keeps current for you.*

VLAD CATRINESCU,
Microsoft MVP

CHAPTER 5

Three moves to make now

01 Run the license reconciliation before your renewal, not after: reclaim idle seats, reassign where there is real demand, and take the right-sized count into the negotiation.

02 Set storage alerts below Microsoft's own thresholds, so the conversation about growth happens on your schedule instead of at the deadline.

03 Document what your scripts do and when they run, while their author still works for you, and give every critical script a second owner.

VOICES FROM THE FIELD

"Staffing and resources aligned to a non-revenue generating activity."

Survey respondent, asked in their own words to name the biggest barrier to better Microsoft 365 governance. Responses lightly edited for spelling and length.

CHAPTER 6

AI on ungoverned ground

77%

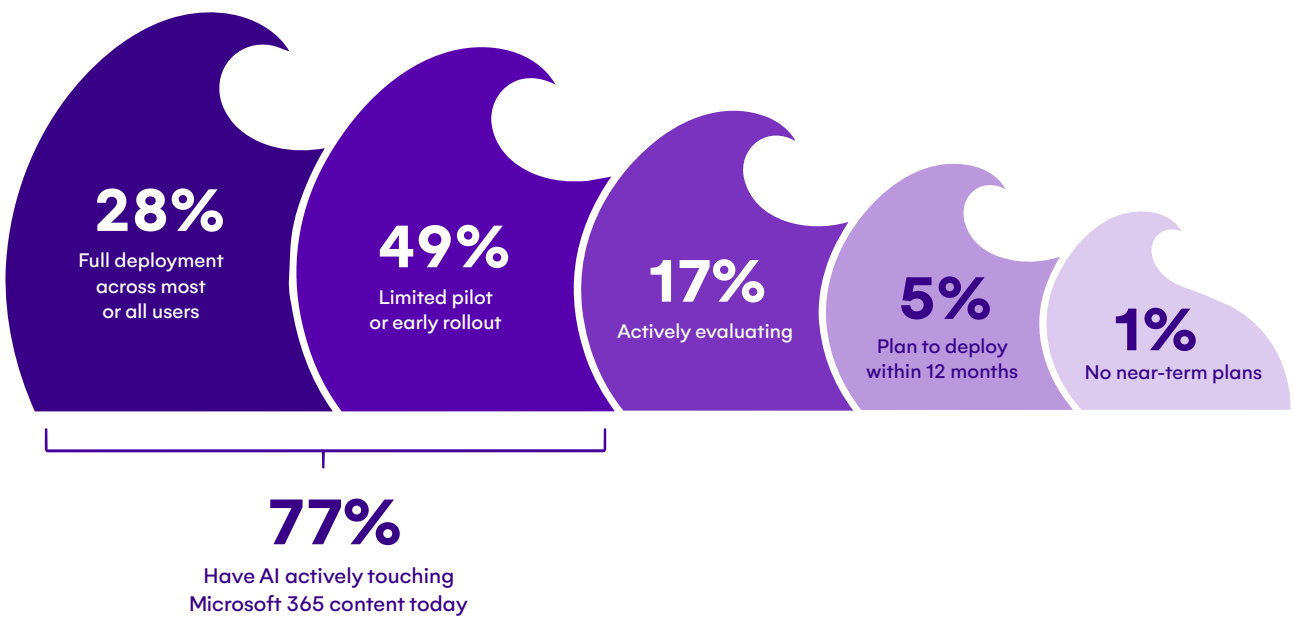
have deployed or piloted Microsoft 365 Copilot or another enterprise AI tool that accesses their M365 data.

Everything this report has documented so far, the thin accountability, the unwatched logs, the orphaned workspaces, the admitted oversharing, was survivable for one reason: **exposed content was hard to find**. AI makes it instantly findable. The protection that obscurity quietly provided now has to come from the permission model itself. This chapter measures how ready organizations are to provide it.

6.1 The adoption wave

The question is no longer whether AI reads your tenant. Only how much of it.

Adoption is not coming; it has arrived. Asked to what extent their organization has deployed or piloted Microsoft 365 Copilot or any other enterprise AI tool that accesses M365 data, 28% report full deployment across most or all users and 49% are in a limited pilot or early rollout, which puts 77% with AI actively touching their data today. Another 17% are actively evaluating and 5% plan to deploy within twelve months. The number of organizations with no plans in the near term rounds to 1%.



Note what this study measured and what it did not: respondents told us AI accesses their M365 data, not which tools do the accessing. Copilot is the recognizable front door, but the questionnaire deliberately covered the whole category, and the category is the point. **Every assistant, connector and agent that authenticates into the tenant inherits the same permission model**, so from a governance standpoint they are one phenomenon: a new class of reader, arriving faster than the permission model is being repaired.

ACROSS THE ATLANTIC

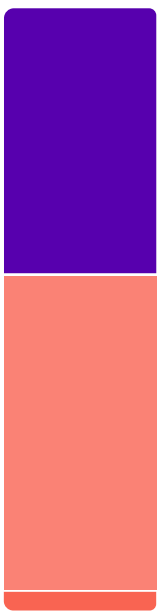
The US is further down the road: 34% fully deployed against 22% in the UK.

6.2 Deployed first, checked later

For most organizations, the front door opened before anyone checked the locks

Deploying AI on Microsoft 365 has one obvious prerequisite: knowing what the permission model will let it retrieve. So we asked organizations that have deployed or piloted AI whether they conducted a formal review of M365 permissions and data access to identify oversharing risks first. Fewer than half, 43%, completed a thorough review before deployment. A majority, 53%, did a partial review, and 4% are planning one they have not started.

The candor cuts both ways here, and deserves saying so: almost nobody skipped the question of permissions entirely, which speaks well of the teams involved. But a partial review of a permission model is a sample, and Chapter 2 established what the full population looks like: **99% of organizations acknowledge at least one live oversharing scenario**. Reviewing part of a model known to contain exposure does not remove the exposure. It removes the part of it you looked at.



With regards to deploying or piloting an AI tool, to what extent, if at all, did your organisation conduct a formal review of M365 permissions and data access to identify oversharing risks?

- 43% A thorough review was completed before deployment
- 53% A partial review was done but not comprehensive
- 4% We are planning a review but haven't started

250 respondents whose organizations have deployed or piloted AI tools.

ACROSS THE ATLANTIC

US deployers were more likely to complete a thorough review first: 47%, against 39% in the UK.

6.3 The overconfidence peak

The highest confidence in the study meets the lowest amount of checking.

Here the report's central gap reaches its widest point. Asked whether they are confident that AI, if deployed today, would surface only content users are explicitly authorized to see, 91% say yes. The composition is familiar: 26% very confident, 65% somewhat, and just 1% concede they have not assessed it or genuinely do not know.

Hold that number against the rest of this study, all of it supplied by the same respondents. A majority (58%) admit confidential content is accessible to departments that should not see it. Fewer than half of deployers completed the thorough permissions review that would justify the confidence. And the mechanics, to be clear, are reasoning rather than a survey finding, but they are not complicated: an **AI assistant enforces permissions faithfully and exactly as it finds them.**

It does not break your permission model. It believes it, at retrieval speed, for every user, on every query. Which means AI does not create a single new exposure; it converts every existing one from something a person would have to go looking for into something a question can surface. The 91% may well be right that AI will only show users what they are authorized to see. Chapter 2 documented what they are authorized to see.

91%

confident AI would surface only content users are authorized to see

58%

admit confidential content is accessible to departments that should not see it

These two numbers come from the same respondents.

BY ROLE

M365 administrators — Most confident — **97%**

CIOs and CTOs — Least confident — **79%**

BY INDUSTRY

Healthcare — Outlier skeptic — **76%**

Software — High AI confidence with the study's highest admitted oversharing — **96%**

6.4 The agent frontier

The next reader does not wait to be asked.

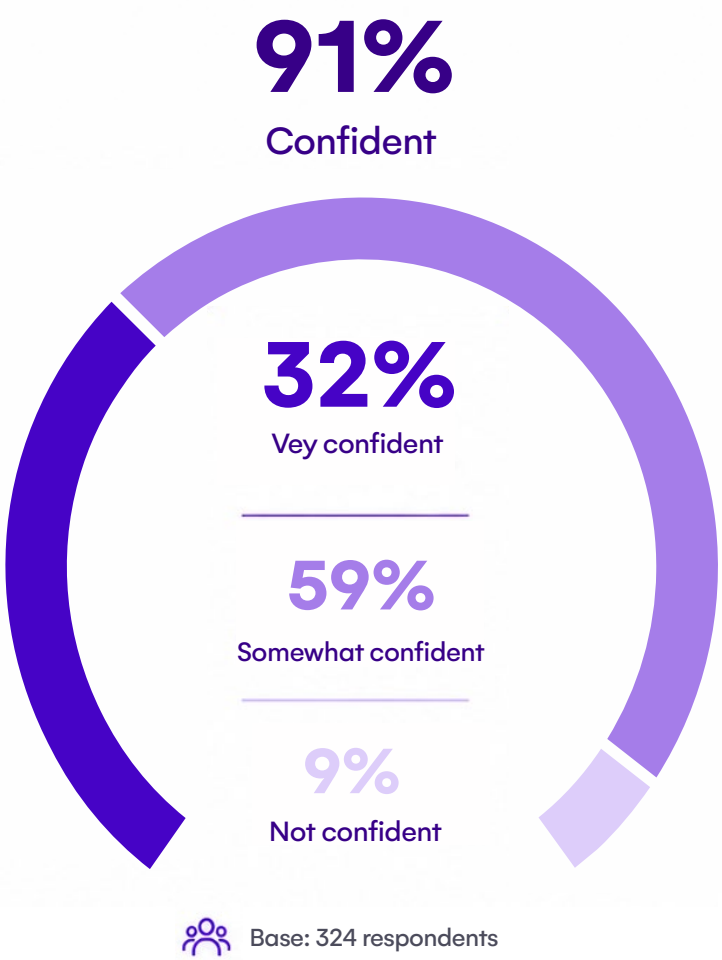
Assistants answer questions; agents act. They run tasks, follow schedules and chain steps together inside the environment, and by their nature they hold standing access rather than momentary attention. In this study they are already ubiquitous by self-report: asked how their organization governs AI agents operating within Microsoft 365, just 1% of respondents say they have not deployed any.

The governance picture respondents describe looks, on its face, orderly. 38% say agents are reviewed and approved before deployment, 27% monitor agent activity through audit logs or third-party tooling, and 22% have a formal policy defining what agents may access.

A smaller group is candid about the gap: 9% say agents operate under the same permissions as the user who deployed them with no separate controls, and 3% have no specific governance framework at all.

Confidence follows the same pattern as everywhere else in this report: 91% are confident they have full visibility over which agents are active and what data they can access, a net built the familiar way, 32% very confident and 59% somewhat.

This report will not adjudicate how solid that orderliness is; the survey recorded what respondents say, and that is what is presented here. What can be said, as reasoning rather than finding, is structural: **whatever an organization's agent governance looks like, it stands on the same permission foundations every previous chapter has examined.** An approved agent inherits the oversharing beneath it exactly as an assistant does, with one difference: it inherits it continuously, without a human typing the question. The agent frontier does not introduce a new kind of risk. It removes the last human checkpoint from the old one.



My view is that most organizations are approaching AI readiness as an AI project when it's really a permissions project (remember AI can see only data end user has access). The first thing I see companies do is pilot Copilot, create AI policies, and discuss use cases. The first thing they should do is gain visibility into their Microsoft 365 environment because you can't govern, secure, or fix what you can't see.

The challenge is that partial permission reviews create a false sense of confidence. Teams review a sample of sites, clean up a few obvious issues, and assume they're ready, while oversharing, orphaned workspaces, and excessive permissions remain hidden elsewhere in the tenant. AI doesn't create new access; it simply exposes existing access at a scale and speed humans never could.

In my experience, 2026 is the year of agents and the next rising challenge is agents. Unlike assistants that answer questions when prompted, agents have standing access and operate continuously. If your permission model isn't governed, you're no longer exposing information only when someone asks for it you're enabling always-on systems to act on top of those same governance gaps. The foundation of AI readiness is therefore not AI itself, but visibility, permissions, ownership, and governance.

FRANE BOROZAN,
Microsoft MVP

CHAPTER 6

Three moves to make now

01 Run an oversharing assessment before the next expansion of any AI rollout, and treat what it finds as the rollout's real prerequisite list.

02 Scope AI pilots to workspaces that are owned, reviewed and recently cleaned, and widen the scope only as the cleanup widens.

03 Inventory every agent in the environment today: what it can read, what it can do, and who answers for it. Standing access deserves a standing owner.

REALITY CHECK

91% are confident AI would surface only content users are authorized to see.

43% of those who have deployed or piloted AI completed a thorough permissions review first.

Base for the second figure: 250 respondents whose organizations have deployed or piloted AI tools.

CHAPTER 7

What would move the needle

3%

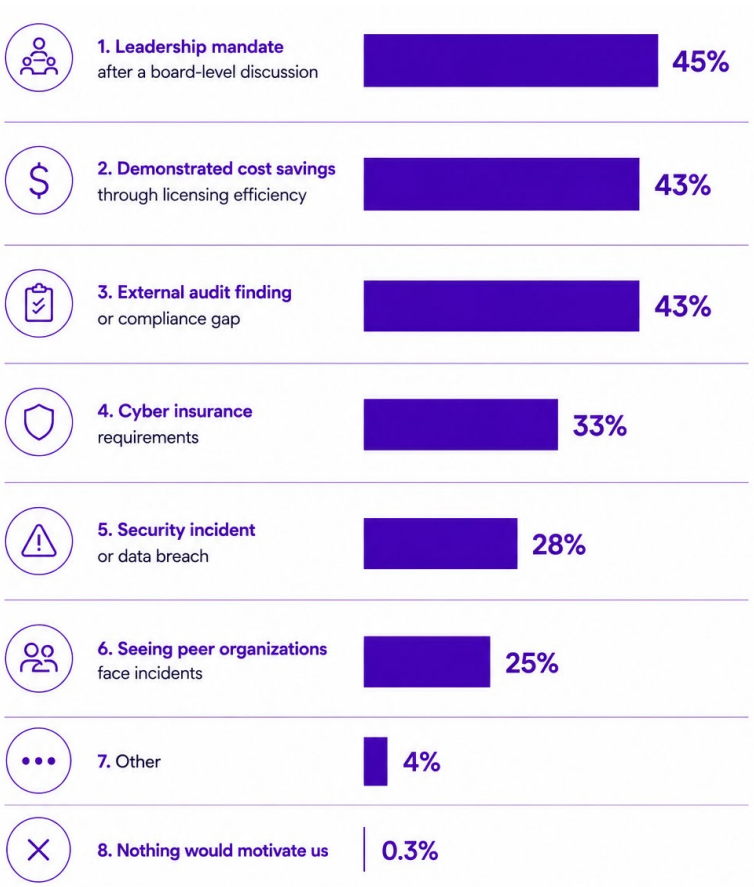
say getting ready to implement AI would motivate their organization to invest more in M365 governance tooling in the next 12 months.

Six chapters have measured the gap. The last question is what would close it, so we asked directly: what, if anything, would unlock more investment in governance tooling? The answers reveal how organizations actually decide, and one number reveals what they have not yet connected.

7.1 The triggers

Investment follows a mandate, a saving, or an auditor. Almost never the thing that changed everything.

Asked what would motivate more investment in M365 governance tooling over the next 12 months, respondents describe a familiar corporate physics. A leadership mandate after a board-level discussion leads (45%), with demonstrated cost savings through licensing efficiency (43%) and an external audit finding or compliance gap (43%) effectively tied behind it. Pressure from cyber insurance requirements moves a third (33%), a security incident or data breach 28%, and watching peer organizations face incidents 25%. Almost nobody is unmovable: just 0.3% say nothing would motivate them.



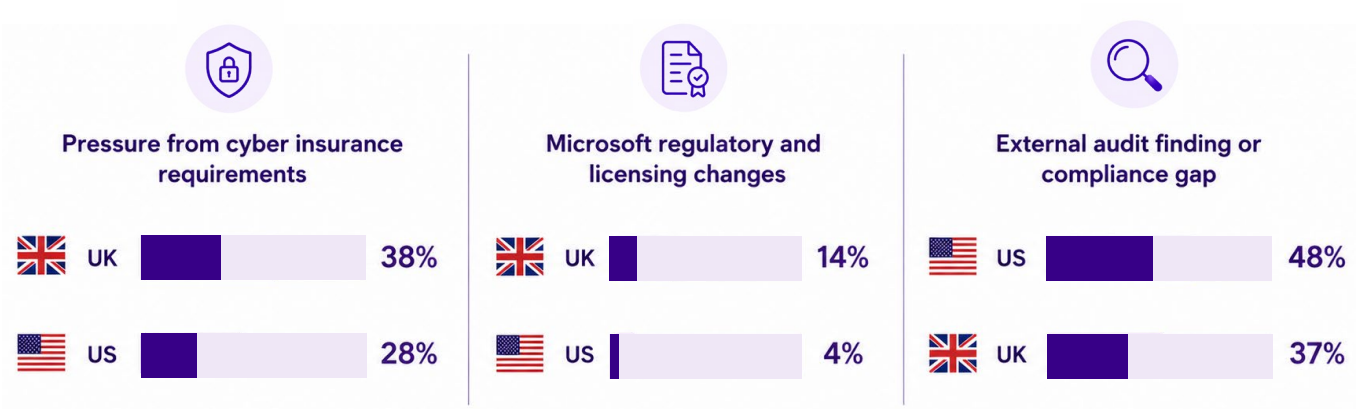
At the bottom of the list sits the number this report exists to explain: getting ready to implement AI would motivate 3%. Set that against Chapter 6, where 76% of the same respondents have AI deployed or piloting against their M365 data today. To be precise about what the question measured: this is investment in governance tooling specifically, and it is possible some AI-readiness spending routes through AI program budgets instead. But the most economical reading, and we offer it as interpretation, is simpler: **organizations have not yet connected the technology they are adopting fastest to the discipline it depends on most.** The permission model became AI's retrieval layer, and in the budget conversation, almost no one has noticed.

The pattern sharpens across the Atlantic. In the US, the market furthest along in deployment (34% fully deployed, as Chapter 6 showed), the AI trigger rounds to 1%. In the UK it reaches 5%. Both figures are small enough that the gap between them should be read gently, but the direction is the point: where AI adoption runs hottest, its connection to governance tooling is faintest. Adoption does not appear to be teaching the lesson; if anything, the organizations deepest in are the least likely to name it.

There is one more loop to close, and it runs back to Chapter 1. The most powerful trigger is a leadership mandate (45%), and the most common obstacle, per the same study, is leadership attention: 47% of boards are aware of governance risk but do not treat it as a priority. The lever and the blocker are the same people. Every alternative trigger on this list, the audit finding, the insurance requirement, the incident, is a more expensive way of starting the same board conversation.

ACROSS THE ATLANTIC

The triggers wear national colors. UK organizations answer to insurers (38% vs 28%) and to Microsoft's own regulatory and licensing changes (14% vs 4%); US organizations answer to auditors (48% vs 37%).



7.2 In their own words

We asked what stands in the way. These are the answers, unedited in substance.

At the end of the survey, respondents could describe the biggest barrier to better Microsoft 365 governance in their own words. Their answers group around three themes, and they read like a summary of this report written by its subjects.

Respondents' answers in their own words, lightly edited for spelling and length.

01 TIME, HEADCOUNT AND COMPETING PRIORITIES

> *The biggest barrier is limited time and resources to consistently enforce governance policies across a growing and complex Microsoft 365 environment, especially given competing IT priorities and skills constraints.*

Survey respondent, UK

02 CONSISTENCY AT SCALE, WITHOUT SLOWING THE BUSINESS

> *The biggest barrier is keeping policies and user access consistent across a large organization. It can be difficult to manage permissions and security without slowing down employee productivity.*

Survey respondent, US

03 THE PERCEPTION PROBLEM

> *Perception of high cost to low value.*

Survey respondent

> *Full backing from management to enforce downstream.*

Survey respondent

CHAPTER 7

Read together, the four answers retell the report. Too few hands (Chapter 1), an environment that outruns manual enforcement (Chapters 2 and 3), and a leadership perception that governance costs more than it returns, a perception Chapter 5's receipts contradict line by line.

The barriers, in the end, are not technical. They are organizational, which is the most hopeful finding available: organizations decide their org charts, their board agendas and their budgets. Nothing in this report requires waiting for anyone else.

You made it to the end, which already puts you in a minority: most governance reports get skimmed for the scary number and closed. So let me hand you the number worth carrying out of here. Only 3% of organizations say preparing for AI would move them to invest in governance tooling. 76% already have AI reading their data. Every board deserves to see those two figures side by side.

Your peers told us why it matters: ***the strongest investment trigger is a leadership mandate, and nearly half of leadership teams are not looking.*** *The lever and the blocker are the same people. Be the one who puts the number in front of them.*

We will run this study next year, and the year after. Measuring honestly, so organizations can govern with evidence instead of belief, is the work we have chosen.

TONI FRANKOLA,
CEO, Syskit

CHAPTER 7

Three moves to make now

01 Take one number from this report to your next board or leadership meeting, and ask for governance on the risk register. The mandate that 45% are waiting for starts as an agenda item.

02 Build the cost-savings demonstration yourself: the license reconciliation from Chapter 5 produces, in most organizations, exactly the evidence that 43% say would unlock investment in governance tooling.

03 Make governance review a stated prerequisite in every AI rollout approval, so the connection that only 3% have made becomes policy in yours.

The Industry Lens

Same platform, same gap, different accents.

Six industries in this study have enough respondents to compare responsibly: Manufacturing (64), Professional Services (39), Healthcare (38), Education (35), Government (34) and Software (33). Their gaps rhyme, but each sector carries the problem with its own accent, and two of them, Software and Healthcare, tell opposite stories worth reading side by side.

Software: moving fastest, exposed most, and sure of itself

The software industry leads the study on nearly every dial at once. It has the most full AI deployments (45%, against 28% overall), the highest self-rated maturity (30% managed or optimized, including the study's largest optimized share at 12%), and board engagement above everyone else (61% very well informed). It also admits the most exposure: 76% say confidential content is accessible to departments that should not see it, the highest in the study, and 52% report a confirmed incident. The sector that best understands the technology is the one running it over the most acknowledged oversharing, at full speed, with its leadership watching.

Healthcare: regulated, unhurried, and hardest to impress

Healthcare is Software's inverse, and its numbers form the most internally consistent profile in the study. It rates itself the most mature by far (47% managed, well above the 18% overall), reports the fewest confirmed incidents (29%), admits the least oversharing (45%), has deployed the least AI (18% fully deployed), and is the study's outlier skeptic on AI respecting authorization: 76% confident, against 91% overall. Whether decades of HIPAA-shaped discipline produced the maturity or the caution produced both is interpretation we will not settle here; what the data shows is a sector that moved slowest and has the least to confess.

Government: the slowest stopwatch, the quietest boardroom

Two government figures stand out. Not one government respondent said they could produce a full access report within an hour, the only quotable sector at zero. And government boards are the least engaged (38% very well informed, against 50% overall), even though its AI adoption (29% fully deployed) actually matches the study average. Deployment without the evidence machinery or the leadership attention is the government pattern in miniature.

Manufacturing: the mainstream, with an engaged board

The study's largest sector is its baseline: close to the average on maturity, incidents, oversharing and AI confidence, with solid adoption (34% fully deployed). Its one distinction is at the top: 58% report boards that are very well informed and engaged, second only to Software. In manufacturing, the attention is there; the chapters of this report describe what it should be aimed at.

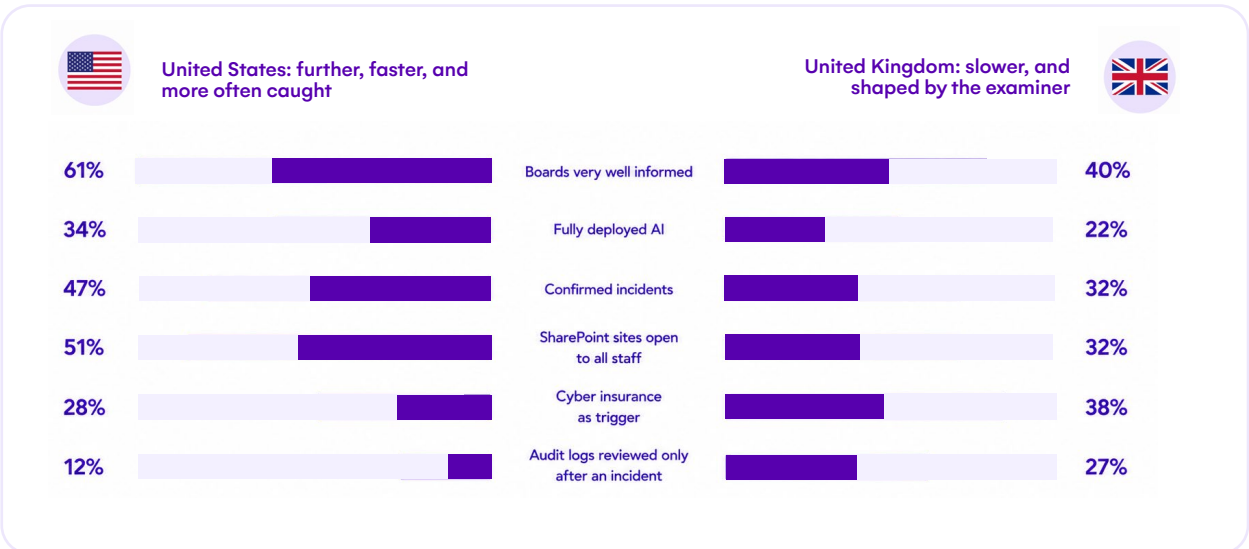
Professional Services pairs the study's highest AI confidence (97%) with its best audit stopwatch (8% within the hour). Education rates its own maturity lowest of the six (14% managed or optimized) while remaining among the most AI-confident (94%), the sector-level version of the confidence gap.

Industry figures are shown only where base sizes reach 30 respondents. Smaller industry subgroups in the sample (including Retail, Finance and Aviation) are excluded from sector comparisons as directional only.

Across The Atlantic

Two speeds. One gap.

Half of this study answered from the United States (161 respondents), half from the United Kingdom (166). Throughout the report, margin notes have flagged where the two diverge; this spread assembles the pattern. It is not a story of one market doing governance well and the other badly. It is two different ways of carrying the same gap.



The United States: further, faster, and more often caught

The US profile runs hotter on nearly every dial. Boards are far more engaged (61% very well informed, against 40% in the UK, the widest national gap in the study). AI deployment leads (34% fully deployed vs 22%), pre-deployment permission reviews are more often thorough (47% vs 39%), audit logs are more often actively watched (32% vs 22%), and working data ownership is twice as common (22% vs 10%).

And yet the receipts run hotter too. US respondents report more confirmed incidents (47% vs 32%), more SharePoint sites open to all staff (51% vs 32%), more storage quota purchases under pressure (35% vs 19%), and more license overcharges caught by the vendor rather than internally (78% vs 61%). Reviews are also more often reactive, triggered mainly by an incident or an audit (55% vs 41%). More attention, more adoption, more machinery, and more evidence of the gap. Which returns us to the observation from Chapter 1: attention is not the same as control.

The United Kingdom: slower, and shaped by the examiner

The UK profile is more cautious and more externally disciplined. Governance answers to institutions: cyber insurance moves 38% (vs 28%), and Microsoft's own regulatory and licensing changes move 14% (vs 4%). Accountability is more often director-led (50% vs 34%, where the US leans on administrators with shared duties), and third-party delegation of governance to data owners is nearly twice as common (23% vs 12%). The sharpest UK worry is the guest list: external access is the leading governance challenge there (48%, vs 36% in the US). The cost of the caution shows in the log habit: UK organizations are more than twice as likely to look at audit logs only after an incident (27% vs 12%).

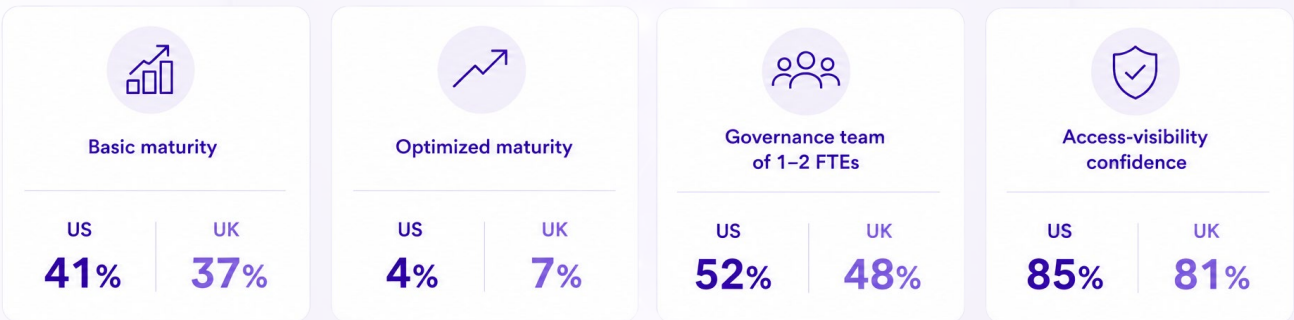
Who has more incidents? The data cannot say.

Add each country's confirmed and suspected incidents together and both arrive at roughly nine in ten (93% in the US, 87% in the UK). The difference is in the mix: the US confirms more (47% vs 32%), while the UK suspects more without confirming (55% vs 46%). Whether that means American organizations have more incidents or simply detect and confirm more of them, this survey cannot distinguish, and we decline to guess. Either reading supports the same conclusion: on both sides of the Atlantic, the incident is the norm, not the exception.

The shared ground

Strip away the accents and the foundations are the same country. Maturity self-ratings are nearly identical at every level of the scale (41% of US and 37% of UK respondents call their governance basic; 4% and 7% call it optimized). Half of organizations on both sides run governance with one to two full-time equivalents (52% US, 48% UK). Confidence is the default in both markets (access-visibility confidence: 85% US, 81% UK). The gap between what organizations believe and what they admit is not a national condition. It is the condition.

Bases: US 161, UK 166. Country figures reflect where respondents' organizations are headquartered for survey purposes; multinational operations may span both regimes.



WHAT TO DO NEXT

The gap is a condition and conditions can be changed.

Everything this report has measured, the thin staffing, the unwatched logs, the ownerless workspaces, the reviews that start after the incident, is a condition, not a verdict. And Chapter 7 ended on the reason for optimism: the barriers respondents describe are organizational, which means organizations control them. What follows is not a transformation program. It is the same five-level scale respondents used to rate themselves in Chapter 1, turned into a path: find your level, take the next step, and ignore the rest of the mountain for now.

L1

Ad hoc. No formal governance; things are handled reactively. 6% of this study placed themselves here. The next step is a name. Governance without an accountable owner cannot improve, because improvement is nobody's job. Name one person, write the role down, and give them this report.

L2

Basic. Some policies exist but are inconsistently applied. 39% of the study, the largest group. The next step is one true fact. Skip writing more policy and establish one piece of ground truth instead: a point-in-time access snapshot of your single most sensitive site, compared against what you expected. Chapter 2 suggests the comparison will be motivating.

L3

Defined. Documented policies, partially adopted. 32% of the study. The next step is closing the paper-practice gap. This is the level where ownership exists on paper and rarely in practice, the 22% condition from Chapter 3. Enforce a two-owner minimum on every workspace, run the first quarterly inventory of ownerless ones, and put automated alerts on permission changes so the environment is watched between review checkpoints.

L4

Managed. Policies enforced with regular reviews. 18% of the study. The next step is making the machinery cheap. Enforcement that depends on human heroics decays; Chapter 5 showed where. Redesign owner reviews to take minutes rather than afternoons, give one audit-log alert a weekly slot with a named owner, and run the license reconciliation before the renewal, which also produces the cost-savings evidence that unlocks further investment.

L5

Optimized. Proactive, automated, continuously improving. 5% of the study. The next step is keeping it true under AI. Make a governance review the stated prerequisite in every AI rollout approval, inventory every agent and its standing access with a named owner for each, and re-baseline against this scale annually, because Chapter 6's lesson applies most to the organizations with the most to protect: the permission model is now the product.

TEN QUESTIONS YOUR TENANT WOULD ASK YOU

Respondents answered these questions for this study. Answer them for your own environment, honestly, and count the yeses

01	Is there one named, accountable owner for Microsoft 365 governance?	Yes	No
02	Has your board or senior leadership discussed M365 governance risk in the past year?	Yes	No
03	Could you produce a full access report for your most sensitive site within a day?	Yes	No
04	Do you have automated alerts on permission changes?	Yes	No
05	Has guest access older than 90 days been reviewed this quarter?	Yes	No
06	Do you know, today, how many workspaces have no active owner?	Yes	No
07	Do defined data owners actually review access to their workspaces?	Yes	No
08	Are audit logs reviewed on a schedule, with alerts, by a named person?	Yes	No
09	Were assigned licenses reconciled against departures before your last renewal?	Yes	No
10	Is a permissions review a stated prerequisite in your AI rollout approvals?	Yes	No

0 to 3

Start at Level 1 or 2 above.

Build the foundation. Name an owner and establish basic control.

4 to 6

You are living the paper-practice gap of Level 3.

Close the gap between policy and practice. Enforce consistently.

7 to 8

Level 4; make the machinery cheap.

Enforce with regular reviews. Make it easy, automated, and routine.

9 to 10

Level 5, and this report suggests you are rarer than you think.

Keep it true under AI and stay vigilant.

One caution from our own data: self-assessment tends toward optimism, so score the environment you have, not the one the policy describes.

METHODOLOGY

The gap in this report was measured in the same way every organization can measure its own: by asking, honestly, and comparing the answers. That comparison is available to you today.

The research

The State of M365 Governance Report 2026 is based on a survey of 327 IT and cybersecurity decision-makers with responsibility for Microsoft 365 governance, working in organizations of 500 or more employees in the United States (161 respondents) and the United Kingdom (166 respondents). Respondents span IT and security leadership and practitioner roles, including Microsoft 365 administrators, IT directors and managers, CISOs and security leads, and CIOs and CTOs. Fieldwork was conducted by Censuswide between 18 May and 2 July 2026.

Of the 327 respondents, 316 were recruited through Censuswide's independent research panels and 11 through channels connected to Syskit. All quantitative findings in this report are driven by the full sample; where the small Syskit-connected group could plausibly influence a figure, it was checked against the external sample separately during production.

How to read the figures

Percentages are rounded to whole numbers, so displayed figures may not sum to exactly 100. Questions marked "select all that apply" are multi-select; their percentages intentionally total more than 100 and are never summed in this report. Net figures (for example, "confident") combine the component answers of a single-select scale, as provided in the research tables. Where a figure in this report is derived from more than one answer option, the derivation is stated alongside it.

The full sample answered every question except where noted: the pre-deployment review question was asked of the 250 respondents whose organizations have deployed or piloted AI tools, and the agent-visibility question of 324 respondents. Country comparisons use the full national bases (161 and 166). Industry findings are quoted only where an industry's base reaches 30 respondents; smaller industry subgroups are treated as directional and excluded from sector comparisons.

What this research is, and is not

Every finding in this report reflects what respondents told us about their organizations: their assessments, estimates, practices and admissions. No Microsoft 365 environments were accessed, scanned or observed in the making of this study, and no finding should be read as a measurement of any tenant. Where the report moves from what respondents said to why we believe it is so, the text says so explicitly.

METHODOLOGY

At the end of the survey, respondents could describe the biggest barrier to better governance in their own words. This open question was optional, and a minority provided written answers; the quotes presented throughout this report are drawn from those responses, lightly edited for spelling and length, and attributed anonymously in line with market research practice.

Findings may be quoted freely with attribution.

Please cite as: **Syskit, The State of M365 Governance Report 2026,** and link to https://www.syskit.com/ebooks/state-of-m365-governance-report-2026 where possible.

For media inquiries, additional data cuts or interview requests: *marketing@syskit.com*