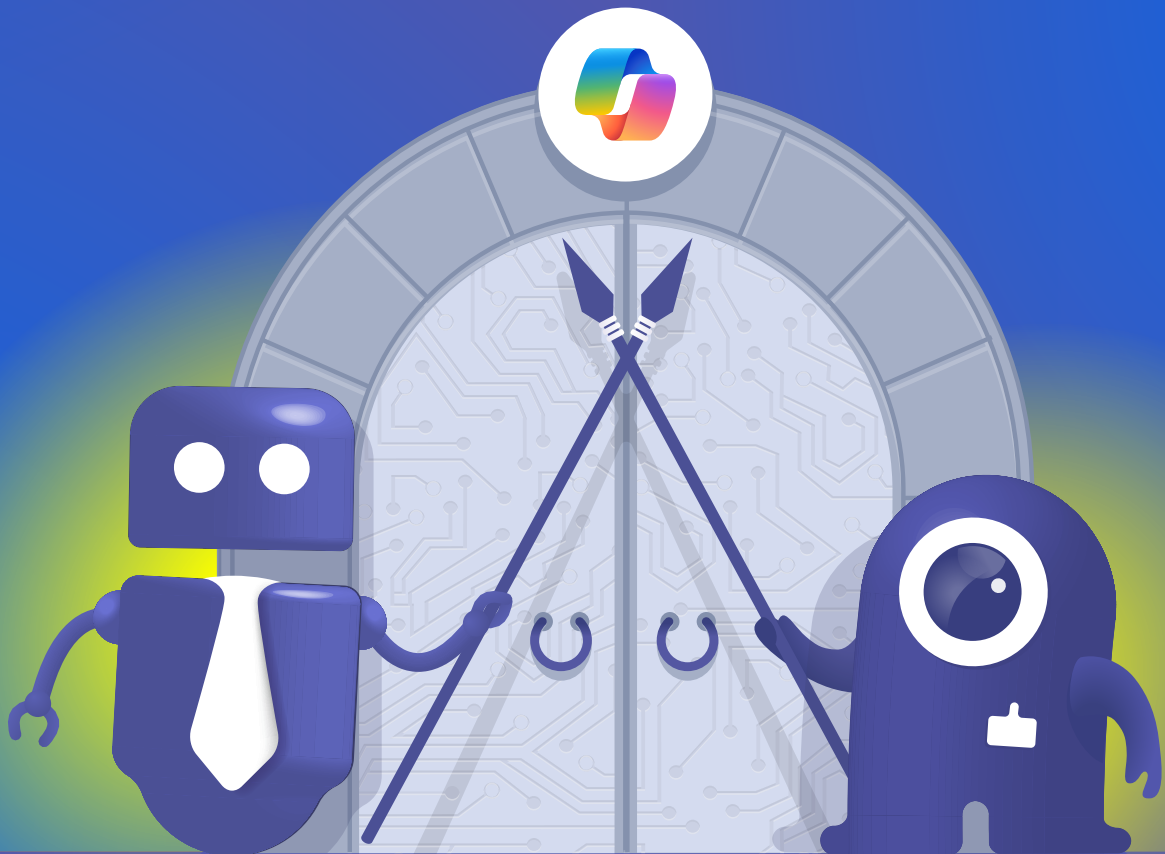


THE **5** MOST COMMON **GOVERNANCE PROBLEMS** IN **MICROSOFT 365**

—— And How to Solve Them with ——
Teams Manager & External User Manager



 SOLUTIONS
2SHARE

www.solutions2share.com

Microsoft 365 Governance: When Control Becomes an Illusion

You know the feeling. Monday morning, you open the Teams Admin Center and discover 47 new teams created over the weekend. None of them follow your naming convention. Half are duplicates. Three external guests have access to areas you didn't even know existed.

Welcome to the daily reality of IT admins running Microsoft 365 without structured governance. The platform is powerful, but that power becomes a liability when nobody sets guardrails. Teams channels multiply unchecked. SharePoint sites spring up without structure. External users retain access to data they have no business seeing. And you? You're always playing catch-up.

The frustrating part: you know something's off. But the problems are growing faster than you can fix them. Every day without clear governance processes widens the gap. And with every new tool (Copilot, Loop, Power Platform), the pressure keeps mounting.

This guide walks you through **the five most common governance problems** we see across organizations of all sizes, and shows you how to solve them with **Teams Manager and External User Manager**. No fluff, no abstract theory. Just actionable solutions that deliver immediate results.

PROBLEM 1

UNCONTROLLED TEAM CREATION: THE SPRAWL THAT NEVER STOPS

The Problem

Anyone can create a team. Anytime. No approval, no naming convention, no structure. What was meant to empower users has turned into pure chaos: 12 versions of “Project Phoenix.” Teams with no discernible purpose. Duplicates that nobody merges. And a search results page that frustrates more than it helps.

For you as an admin, this isn’t just annoying. It’s a security risk. Every uncontrolled team brings new permissions, new data silos, and new attack vectors. And the longer you wait, the bigger the mountain you’ll have to clean up.

What Happens If You Do Nothing

Picture this: a new employee searches for project documentation. They find seven teams with similar names, join the wrong one, and work with outdated data for two weeks. Or worse: they share confidential information in a team that should have been archived months ago. One that still has three former contractors listed as guests.

Sprawl doesn’t just eat up admin time. It erodes your users’ trust in the platform. When nobody can find anything, people go back to email and file shares, and your Microsoft 365 investment goes up in smoke.

The Solution with Teams Manager

Teams Manager picks up exactly where Microsoft leaves off. With **pre-configured templates**, you create standardized team structures for every use case: channels, folder structures, OneNote notebooks, and Planner tasks included. Your users select a template, fill in the required fields, and get a perfectly structured team.

Naming conventions are enforced automatically. No more creative abbreviations or typos in team names. On top of that, **approval workflows** ensure that every new team is reviewed before it’s created. And **de-duplication** automatically flags when similar teams already exist.

The result? Instead of chaos, you have clarity. Every team has a clear purpose, a consistent structure, and the right permissions from day one. Your users find what they’re looking for. And you save hours you used to spend cleaning up.

See how templates and naming policies stop sprawl in its tracks:

[Teams Manager Features at a Glance](#)

PROBLEM 2

ORPHANED TEAMS: THE INVISIBLE SECURITY RISK

The Problem

The project team finished their work. The campaign ran its course. The workshop was six months ago. But the teams? They're still there. With all the data, all the permissions, all the members. Including the external ones. Nobody thought to archive or delete them. Because who does that voluntarily?

Orphaned teams are like forgotten doors in a building. They look harmless, but each one is a potential entry point for security incidents. A substantial portion of Teams workspaces go inactive within the first year of creation and then just sit there, indefinitely.

What Happens If You Do Nothing

Imagine the audit scenario: your CISO asks for a list of all active teams with external access. You pull the data and discover that hundreds of teams show no activity for months, yet still contain sensitive data and active guest accounts. The cleanup takes weeks – weeks you don't have.

It gets worse with Copilot. The AI doesn't distinguish between active and orphaned teams. If a user has access to a long-forgotten team, Copilot can surface its contents in responses, including confidential project data that should have been archived ages ago.

The Solution with Teams Manager

Teams Manager brings **automated lifecycle management** to your environment. You define inactivity criteria and expiration dates (typically 12 months for project teams, longer for department teams). Before a team gets archived, owners receive an automatic reminder: "Do you still need this team?"

No response? The team gets archived automatically. Data is preserved, but the clutter disappears from active lists. Teams without owners are flagged and escalated. And the best part: you can define different lifecycle rules for different team types.

The feeling afterward? Relief. Your environment is clean. You know exactly which teams are active and which are archived. No more manual searching, no more endless lists with questionable status. Just clean, organized collaboration.

PROBLEM 3

GUEST ACCESS OUT OF CONTROL: WHEN EXTERNALS SEE MORE THAN THEY SHOULD

The Problem

External collaboration is a fact of working life. Agencies, consultants, freelancers, clients: they all need access to certain teams and data. The problem? In most organizations, anyone can invite guest users. Without approval. Without documentation. Without an expiration date.

That consultant who helped with a project 18 months ago? Still has access to your SharePoint site. The freelancer from the marketing campaign? Can still view confidential documents. Multiply that across hundreds of collaboration projects, and you've got an attack surface you can't even see.

What Happens If You Do Nothing

A former contractor whose account gets compromised gains access to your internal data through a forgotten guest account. Or a competitor hires the ex-freelancer who still has visibility into your strategic documents. These aren't hypothetical scenarios. They happen.

Without a systematic review process, guest accounts grow like mold in a basement: invisible but dangerous. And the true extent only becomes visible at the next security audit.

The Solution with External User Manager

External User Manager puts you back in control. Every guest invitation goes through an **approval workflow**: the user enters the guest's email address, selects the teams, and the designated approver decides. No more uncontrolled invitations.

On top of that, an **onboarding portal** ensures guests complete a defined process before gaining access: reading important information, confirming compliance documents, providing metadata. Only then is access granted. **Domain whitelisting** and blacklisting add an extra layer, ensuring only approved organizations can be invited.

The result: you always know which external users have access to which areas. No guessing, no hoping, no unpleasant audit surprises. Just full transparency and control.

See how the guest approval workflow keeps externals in check:
[Manage Guest Users Securely with External User Manager](#)

PROBLEM 4

COMPLIANCE GAPS: WHEN YOU HAVE NO ANSWERS AT AUDIT TIME

The Problem

The auditor asks a simple question: “Can you prove that all external users have signed a confidentiality agreement?” You know you sent NDAs. At some point. Via email. To some of them. But a complete, airtight documentation trail? That doesn’t exist.

Compliance around external access is a blind spot for many IT teams. There’s no single place where invitation dates, approvals, signed documents, and access durations are tracked. Everything is scattered across emails, Excel sheets, and individual colleagues’ memories.

What Happens If You Do Nothing

When a serious security incident involves an external user, you need to prove who approved access, when, what agreements were in place, and whether regular reviews took place. Without that documentation, you’re exposed – to auditors, to management, to regulators.

In regulated industries like health-care, financial services, or legal, this isn’t just an inconvenience. It’s a serious regulatory risk with potentially steep fines.

The Solution with External User Manager

External User Manager makes compliance second nature. Through the built-in **compliance document system**, you upload critical documents like NDAs, privacy policies, or terms of use. Every guest must read and confirm these documents before receiving access.

Every signature is **time-stamped and documented**, available for retrieval at any time. Combine that with **automated access reviews** at defined intervals: team owners regularly confirm whether guest access is still needed. No response? Access is automatically revoked.

At the next audit, you open External User Manager and everything is right there: who has access, since when, who approved it, which documents were signed, when the last review took place. Instead of stress, you have evidence.

See how Bioland manages compliance and guest access in one place:

[Bioland Case Study](#)

PROBLEM 5

MANUAL GOVERNANCE: WHEN YOUR IT TEAM SPENDS ALL DAY CLEANING UP

The Problem

Your team spends entire days identifying inactive teams, tracking down owners, cleaning up permissions, and reviewing guest accounts. Hours on end. Week after week. It feels like pushing a boulder uphill, because as soon as you finish one pass, the next one starts.

Manual oversight might work at 50 teams. At 500, it becomes impossible. And with every month your organization grows, the backlog gets bigger. Your admins are frustrated because they're spending their time on routine tasks instead of working on strategic projects.

What Happens If You Do Nothing

Manual governance doesn't scale. Full stop. Eventually, mistakes happen: a missed review, an overlooked guest account, an unnoticed permission change. And those are exactly the gaps that attackers exploit or that lead to compliance violations.

Then there's the human factor: when governance becomes a dreaded chore, diligence drops. Checks get done superficially or get postponed. The result: governance that exists only on paper.

The Solution with Teams Manager and External User Manager

The combination of Teams Manager and External User Manager **automates the entire governance chain**. Teams Manager handles creation, naming, lifecycle, and archiving. External User Manager handles invitation, approval, onboarding, compliance documentation, and regular review of all guest users.

Instead of manual Excel lists and PowerShell scripts, you have a centralized, integrated solution right inside Microsoft Teams. Your admins configure the rules once, and the system enforces them consistently. No exceptions, no forgetting, no manual errors.

Organizations using automated governance tools report **substantial reductions in time spent on routine compliance tasks**. That means your IT team can finally focus on what really matters: strategic projects, innovation, security architecture

Quick Reference:

5 Problems, 5 Solutions

PROBLEM	IMPACT	SOLUTION	OUTCOME
Uncontrolled team creation	Sprawl, duplicates, chaos	 Templates, naming, approval workflows	Structured, discoverable teams
No lifecycle processes	Orphaned teams, security gaps	 Auto-archiving, owner reminders	Clean, current environment
Guest access out of control	Unknown externals with access	 Approval workflows, onboarding	Full transparency over externals
Missing compliance docs	Audit risks, no evidence trail	 NDAs, signature tracking, audit trails	Complete documentation
Manual governance processes	IT team overloaded, error-prone	 +  Full automation	More time for strategic work



Teams Manager



External User Manager

The Next Step Is Yours

You now have a clear picture of the five governance problems that cripple Microsoft 365 environments most often. And you know what the solution looks like. The question is: how much longer are you going to wait?

Every day without structured governance means: more sprawl, more uncontrolled guest accounts, more security risks, more wasted admin hours. And with Copilot, every permission problem becomes immediately visible and exploitable.

The good news: you don't have to fix everything at once. **Start where the pain is greatest**, whether that's uncontrolled team creation, missing guest account oversight, or manual processes. Teams Manager and External User Manager can be rolled out gradually and grow with your requirements.

More than 60,000 installations worldwide

1.5 million users trust Solutions2Share products for their Microsoft 365 governance. From mid-sized companies to large enterprises, including organizations like the German Red Cross, Lucerne University of Applied Sciences and Arts, and Midwest BankCentre.

Ready to take control of your Microsoft 365 governance?

Book a Free Demo

solutions2share.com/book-a-demo

Questions?

Reach out directly:

sales@solutions2share.com

© Solutions2Share GmbH
Dieter-Streng-Str. 3
D-90766 Fürth| Germany
www.solutions2share.com

Managing Directors: Christian Groß, Wolfgang Groß
Company Registry: Local Court Fürth, HRB 16088
Privacy Notice:
<https://www.solutions2share.com/privacy-policy/>

