The Value of Automated Office 365 & Teams Governance

A Companion Guide To The Office 365 Automated Governance Value Calculator

AvePoint®

The Value of Automated Office 365 & Teams Governance

A Companion Guide To The Office 365 Automated Governance Value Calculator

AvePoint®

Introduction

Congratulations on taking the first step in your Office 365 governance journey! This guide will help you understand the basics of governing Office 365 and how to evaluate its value for your organization.

First, we should start with a common understanding of what we mean when we use the term "governance" or "operational governance."

We define **OPERATIONAL GOVERNANCE** as the process of developing, implementing and enforcing policies for how IT applications are enabling business success, particularly in guiding user behavior and mitigating risk.

Within a successful governance policy framework, applications have defined ownership, including chains of responsibility, authority, and communication with measurement and control mechanisms in place.

This is particularly important in Office 365 and SharePoint, which empower end users with powerful features. The value of operational governance derives from allowing users to access these powerful features, but also having mechanisms for keeping risks in check.

Interpreting Your Results From the Calculator

If you haven't accessed the calculator, don't worry! This guide will still be a very helpful and relevant introduction to Office 365 governance.

If you have accessed the calculator, you know the main inputs are the number of users and effort levels related to current governance-related tasks. AvePoint then makes estimates based on a combination of actual customer examples and dozens of years of first-hand IT management experience by our own team members.

These are conservative estimates of how many minutes per year, per workspace in an environment, IT spends maintaining and managing settings and services for user productivity and service delivery. Then, based off of actual

customer examples and real-world experience, we can accurately estimate how much time can be saved per task through automation.

Once the time savings is quantified, we can convert this to a monetary savings by estimating the amount of salary per minute spent on each task. The salary assumptions are conservatively based on national averages for different types of workers.

While the value is impressive, it only scratches the surface of the value of automating the governance of Office 365.

For example, there are some regulated or security-minded organizations that have decided against turning on Microsoft Teams until certain
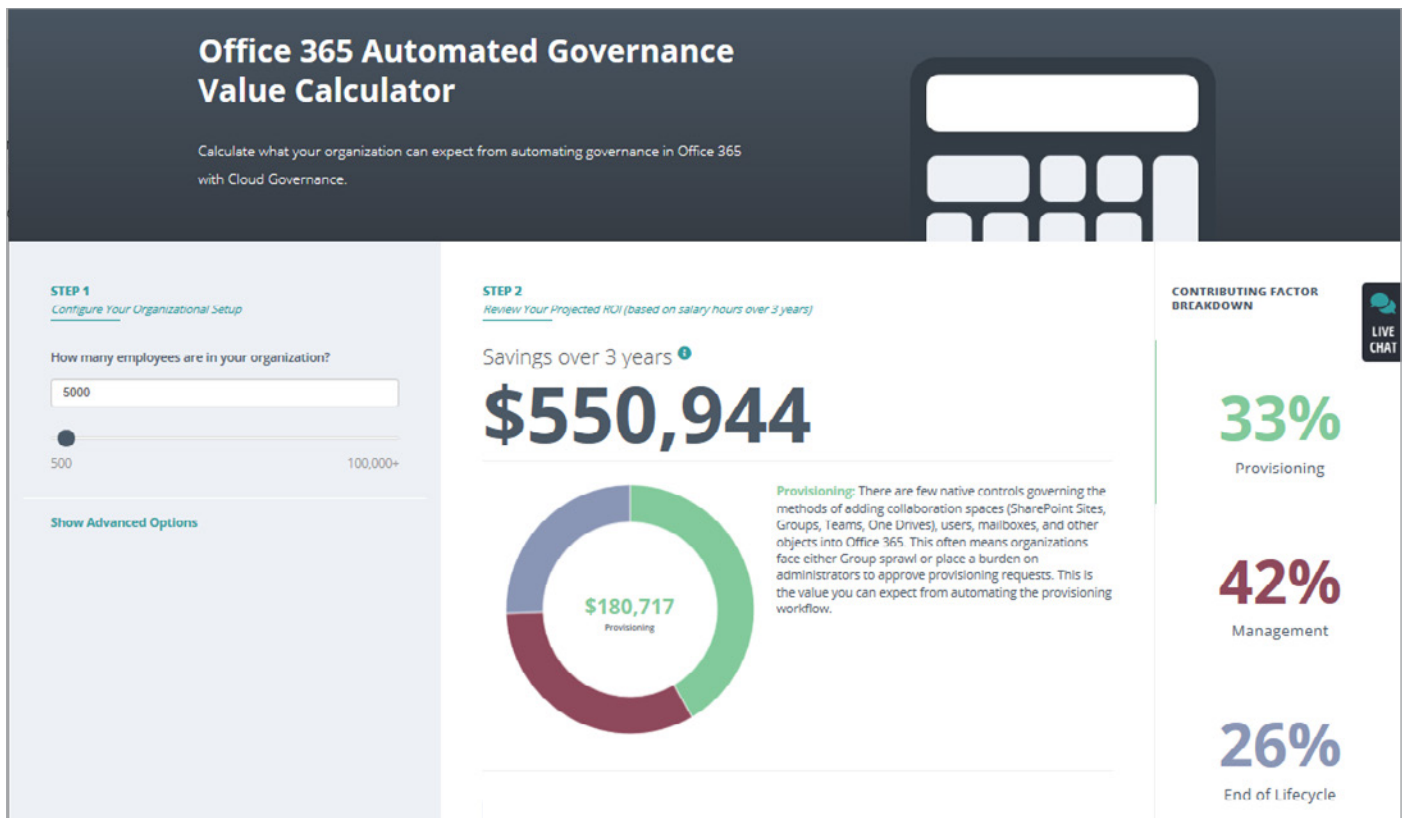
requirements not supported natively in Office 365 are met. The value in this case is being able to finally turn on Microsoft Teams and realize your full Office 365 investment!

This is where understanding the level of governance that is right for your organization (page 23), and how third-party tools can help you achieve your required governance level is critical.

Disclaimer: It's important to understand the values provided by the Office 365 Automated Governance Value Calculator are simplified estimates based on limited input data. This was done to make the calculator as accessible as possible for a broad spectrum of audiences. AvePoint can work with you to further refine the value of automated governance for your organization.

You can book a governance consultation with one of our experts. If downloading this guide was your first step in your governance journey, consider this the second.

You will also want to supplement the topline number provided by the calculator with a greater understanding of how Groups and modern workspaces work in Office 365 in the following sections.

However, if you want to jump to the explanation of how we made these calculations skip to page 28.

Section 1

Office 365 Governance: The Basics

AvePoint

Understanding Office 365 Groups & Modern Workspaces

Office 365 Groups

When you are talking about Office 365 governance, you are really talking about governing Groups, the underpinning technology of Office 365. You cannot understand Office 365 governance without an understanding of what you are governing.

What are Office 365 Groups?

Let's start with the official definition by Microsoft:

***Groups in Office 365** let you choose a set of people that you wish to collaborate with and easily* set up a collection of resources for those people to share. Resources such as a shared Outlook inbox, shared calendar or a document library for collaborating on files.

You don't have to worry about manually assigning permissions to all those resources because adding members to the group automatically gives them the permissions they need to access the tools your group provides. Additionally, groups are the new and improved experience for what distribution lists or shared mailboxes used to do.

Office 365 Groups

Outlook | OneDrive | OneNote | Calendar | Dynamics CRM | Delve | Yammer | Teams

Using Office 365 Groups to Manage Membership

Groups can be a confusing concept because it is not a tangible tool users can access like Microsoft Teams. Rather, it's the underlying framework for how the different tools within Office 365 are connected.

Office 365 Groups gather the identities of people who need to work together and creates a 'group identity' in Azure Active Directory.

For example, it would be cumbersome to create a Team for the Marketing Department in Microsoft Teams, add each person in the department as a member and then repeat the process across SharePoint, OneNote, and other Office 365 tools.

Prior to Office 365, the *IT department* typically had to grant and manage permissions for these types of workloads separately. Today, *users* can simply create the Team, which spins up all the resources listed above for all the members in that associated Group.

This example highlights the two factors that make Office 365 Groups such a dynamic, and sometimes challenging, technology concept.

**1.** By default, all end-users can set up the service themselves without the need for IT intervention.

2. While Groups facilitate collaboration through interconnected services they can also lead to "sprawl" and exponentially increase an organization's consumption of Office 365.

Lets take a closer look at both of these factors and how they can impact governance.

Self-Provisioning & Office 365 Groups Owners: There are two types of memberships in Office 365 Groups: the Owner and Member. The person who created a Group automatically becomes the Owner.

A Group Owner has a lot of power and responsibility including but not limited to the ability to add or delete members, grant owner-level permissions to members, enabling access to external users, determining if it is a public or private Group, and even deleting the Group (and data within).
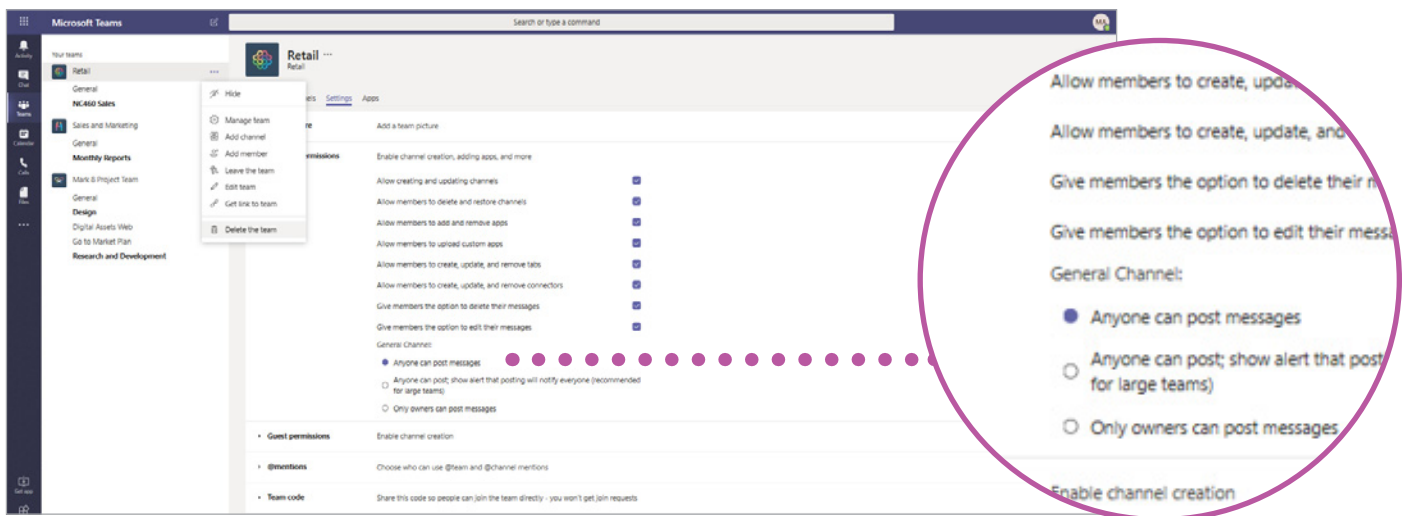
A Team Owner, which by default is the user who created the Team, has a lot of power including the ability to delete the Team and information within.

While the Owner must make these and other decisions, it is unlikely they have been trained in your organization's operational governance policies or think like an Office 365 administrator. For example, an Owner must decide whether to make a Group public or private, without fully understanding what that means (see page 15).

It's also not made readily apparent to Owners from the start that creating a Team will spin up additional services and it's also lacking strong native functionality to avoid Group duplication.

Turning Off Self-Provisioning: At this point you may be asking yourself, "can I just turn off the ability for users to self-provision Groups?" The short answer is yes, and while it can be an option during a pilot or initial roll out phase, just simply turning off self-service will have a *negative impact on the organization* in the long-term.

That is because, despite some of the challenges inherent in Groups, self-provisioning lets users collaborate quickly. The alternative, having IT approve each provisioning/creation request, will frustrate your users, leading to low adoption and shadow IT. At the same time, it will put a tremendous burden on your IT team.

A recent survey of IT professionals conducted by the AIIM (Association for Information and Image Management), and commissioned in part by AvePoint, found that 63 percent of respondents spent 4 to 8 hours or more doing routine SharePoint governance tasks such as provisioning, changing permissions, and changing site settings.

How many man hours per week (full-time equivalents, FTEs) do your admins spend doing routine SharePoint governance tasks such as: provisioning SharePoint site collections, changing site permissions, changing/resetting site settings/features, and cleaning?

2%	10%	25%	40%	7%	7%	9%
Less than 1 Hour	1-2 Hours	2-4 Hours	4-8 Hours	1-2 Days	More than 2 Days	We Don't Use SharePoint
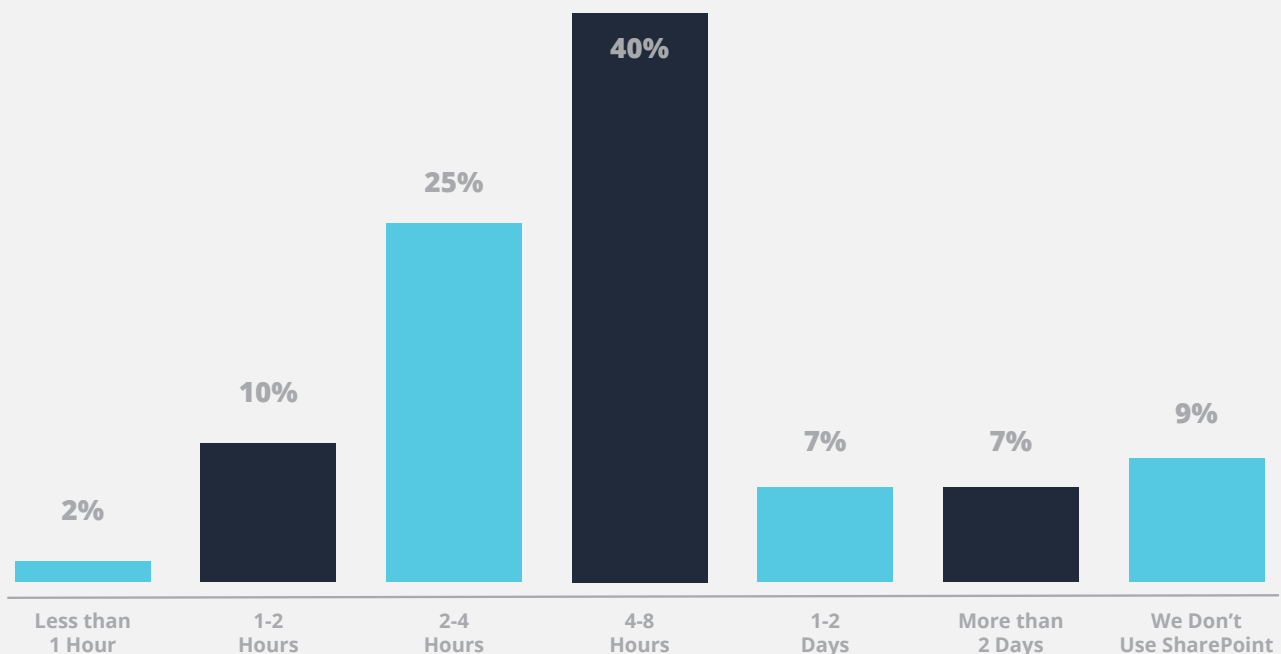
That's one full workday every week! This is time that could be better spent on more strategic tasks that add value to the organization.

There is a third way, which enables users to self-provision Groups while still giving IT the control to guide the process and enforce governance policies. This way is discussed in the section "The Third Way: AvePoint Cloud Governance" on .

Interconnected Services & IT Ownership of Office 365: As a result of the interconnectivity of tools and services, operating in Office 365 is fundamentally different than how IT departments have operated in the past.

IT roles like administrators of storage, databases, servers, applications and services are finding that their responsibilities begin to overlap.

As your organization moves to Office 365 it's important to delegate responsibilities clearly and have a single owner to oversee Office 365.

Gartner recommends, "Each service admin (Exchange Online, SharePoint Online, Teams, Microsoft Yammer) will have unique responsibilities for and uses of Office 365 Groups, but creation, lifecycle and organizing decisions must be made with the overarching Office 365 strategy in mind."

Not having clearly defined roles and an overall platform owner can lead to a number of issues, like improper user, license or security management; a lack of governance; or most commonly, implementations that take too long to roll out and lack enough governance and data management planning—which ultimately costs organizations both in terms of expensive resource consumption and unmitigated risk.


IN SUMMARY

Groups allow for the creation of a set of shared, interconnected tools and workspaces across Office 365 for a set group (small g) of people. Office 365 Groups are designed to enable self-service and dynamic collaboration that streamlines the traditional organizational hierarchy—the perfect answer to the way we work today.

However, they give a lot of power to end users and Group Owners. The decisions made by these Owners need to be aligned with the organization's governance policies. A best practice for IT teams is to have a centralized Office 365 owner or administrator who looks after the larger landscape as opposed to siloed workloads.

Modern Workspaces: Teams, SharePoint, Yammer and More!

Another challenge is that there are more than 20 ways to create a Group in Office 365 (depending on how you count) and what comes with that Group is not standardized. What services are created as part of that Group depend on where that Group was created.

Entry Points for Self-Service Provisioning
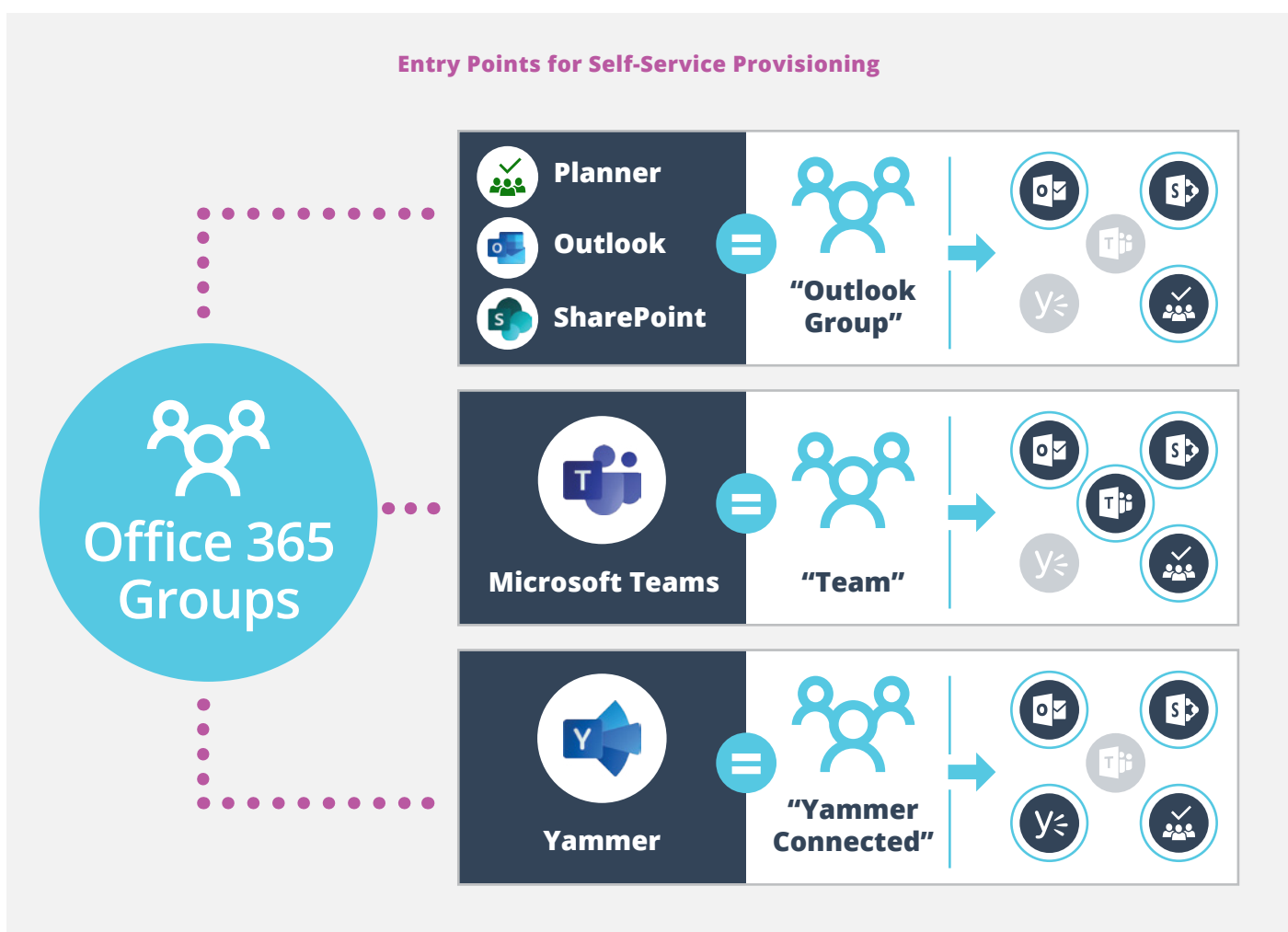
![] Microsoft Teams

What it is: The "productivity hub" in Office 365, Teams a provides single-point access to conversations, files, notes, and tasks. It combines the features of Skype (chat and conferencing), SharePoint and OneDrive (file sharing and collaboration), OneNote (note-taking), Planner (everyday project management), Stream (video sharing), plus in-app tabs that make other tools like GSuite, MailChimp, Salesforce, and more available right next to your work. It's considered by Microsoft to be the "inner loop" of collaboration for the people you work with frequently on

core projects. To read more about best practices, check out "Matt Wade's Definitive Guide To Everyday Etiquette in Microsoft Teams."

How Groups are Created (default settings):
In the Microsoft Teams app, select *Add team*. Select *Create a team*. Select what type of Team you want to create. Add a name and optional description for your team and set privacy preferences. If a Group already exists, you can opt to *add Microsoft Teams functionality* to the existing group. Select Next and your Team (and Group) is ready to go.

One Unique Governance Challenge: Microsoft has made Teams very easy to use and navigate. This leads users to create multiple Teams, inevitably creating Group sprawl, making content harder to find for users.

What Comes with A Group Created in Teams: Team, modern SharePoint team site, shared Exchange mailbox, Planner Plan, Power BI, a Stream and OneNote.

SharePoint

What it is: Primarily used as the main content collaboration, intranet or document management and storage system in Office 365. SharePoint is a highly customizable repository and communication tool that allows collaborators to store and find information in a centralized and highly-customizable space. It is also the engine that powers file collaboration in Teams.

How Groups are created (default settings):
Open SharePoint, select +*Create Site* from the navigation pane. Select *Team Site*. Enter a name and optional description of the *Group*, and set

the member settings. Click *Next*. Add additional Owners and Members. Click *Finish*, and voila! Your Group is ready to go.

One Unique Governance Challenge: If no governance tool or process is put in place, users can accidentally share all the information in a Site rather than a specific document with external users. Since many organizations use SharePoint as their main information repository, but most are not consistent with tagging their sensitive data, this can result in sensitive data leaks.

What Comes with A Group Created in SharePoint: modern SharePoint team site, shared Exchange mailbox, Planner Plan, PowerBi workspace and a Stream.

Yammer

What it is: An enterprise social network. Think of it as "Facebook but just for your organization." Microsoft describes it as the "outer loop" of communication where people can connect across the organization. It's best to use when you know someone in the organization knows the answer, but you don't know who.

How Groups are Created (default settings):
Open Yammer, Click *Create a group* from the navigation pane on the left side of the screen. Designate your Group as an *Internal Group* or *External Group*. Enter a name for the Group. Enter the names or email addresses of members under *Group Members*. Set privacy preference for the Group. To finish, click *Create Group*.

One Unique Governance Challenge: Once a different Office 365 Group or Team has been created, you cannot attach a Yammer Group

after the fact, which can cause naming conflicts as people attempt to create new Yammer Groups to correlate to existing workspaces.

What Comes with A Group Created in Yammer: modern SharePoint team site, shared Exchange mailbox, Planner Plan, PowerBi workspace and a Stream.

Teamwork in Microsoft 365

Inner Loop
People you work with regularly on core projects

Examples:
Team meetings & communication
Event planning
Sales Team planning

Teams

Content collaboration
SharePoint

Video & live events
Stream

Yammer

Outer Loop
People you connect with openly across the organization

Examples:
Corporate communications
CEO Town Hall Meetings
Employee Interest Groups

Outlook

Email
Pervasive availability. Targeted communications.

And More!

Groups can also be created in other types of Office 365 services such as Outlook, Planner, Forms, Stream, PowerBi, Admin Center and more. Therefore, it's important to govern at the Group rather than individual tool/service level.

IN SUMMARY

Because it is so easy for users to create Groups across modern workspaces in Office 365 it is important to understand what these workspaces are, how they are used and how they are connected.

Common Governance Challenges in Office 365

Due to the nature of Office 365 Groups, there are common governance challenges we have seen customers face time and time again.

Provisioning

There are few native controls governing the methods of adding (provisioning) collaboration spaces (SharePoint Sites, Groups, Teams, One Drives), users, mailboxes, and other objects into Office 365.

Challenge: Group Sprawl

Because of the lack of moderated controls, organizations are typically forced to put the full burden of creating users, workspaces, and sometimes even content on IT administrators. The only alternative involves allowing either all business users or subsets of users to create objects with little to no oversight.

Allowing objects to be created without proper enforcement can increase risk within organizations and create tons of "clutter" making it more difficult for users to find what they need.

Challenge: Consistent Naming Conventions

Out-of-the-box, Office 365 offers the ability to enforce a naming policy to assist in communicating the function of a group, membership, geographic region, or who created the group.

This approach adds either a prefix or suffix (or both) and is applied across the entire Office 365 tenant – meaning that all Teams in the organization are limited to having the same settings applied to them. This presents a challenge for any organization that has more than one division – which is generally the case.
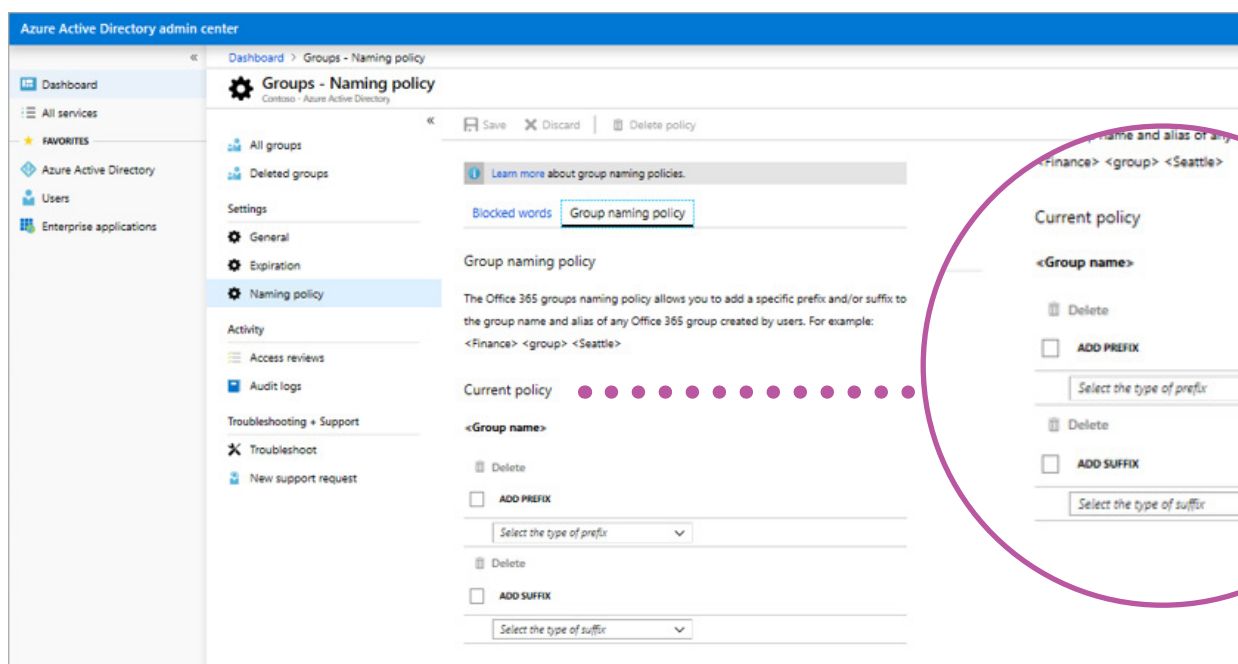
Divisions will often have different needs and preferences for naming and the Microsoft naming convention is one-size-fits-all within the tenant. The native naming functionality also relies heavily on Azure Active Directory properties being complete and correct for all employees—which is rarely the case.

Challenge: Public vs. Private Groups

When a new Group is created, owners are asked if it should be a public or private group. However, there is no clear messaging to users around the implications of this choice. Users are generally unaware that for public Groups anyone in the organization can see, alter and delete your files.

A public Group is exposed to all users within your Office 365 tenant, including any vendors or contractors to whom you may have granted an account within your Office 365 subscription. Users can browse, search, and instantly join a public Group.

Even non-members of a public Group can access, edit, and share all the Group's files and information. Every new user you add to your Office 365 tenant receives the same rights.

Setting a Group to private immediately prevents organization-wide access to files and information which may only be appropriate for the eyes of a few. However, even when a Groups is set to private, its membership is still visible throughout the entire organization.
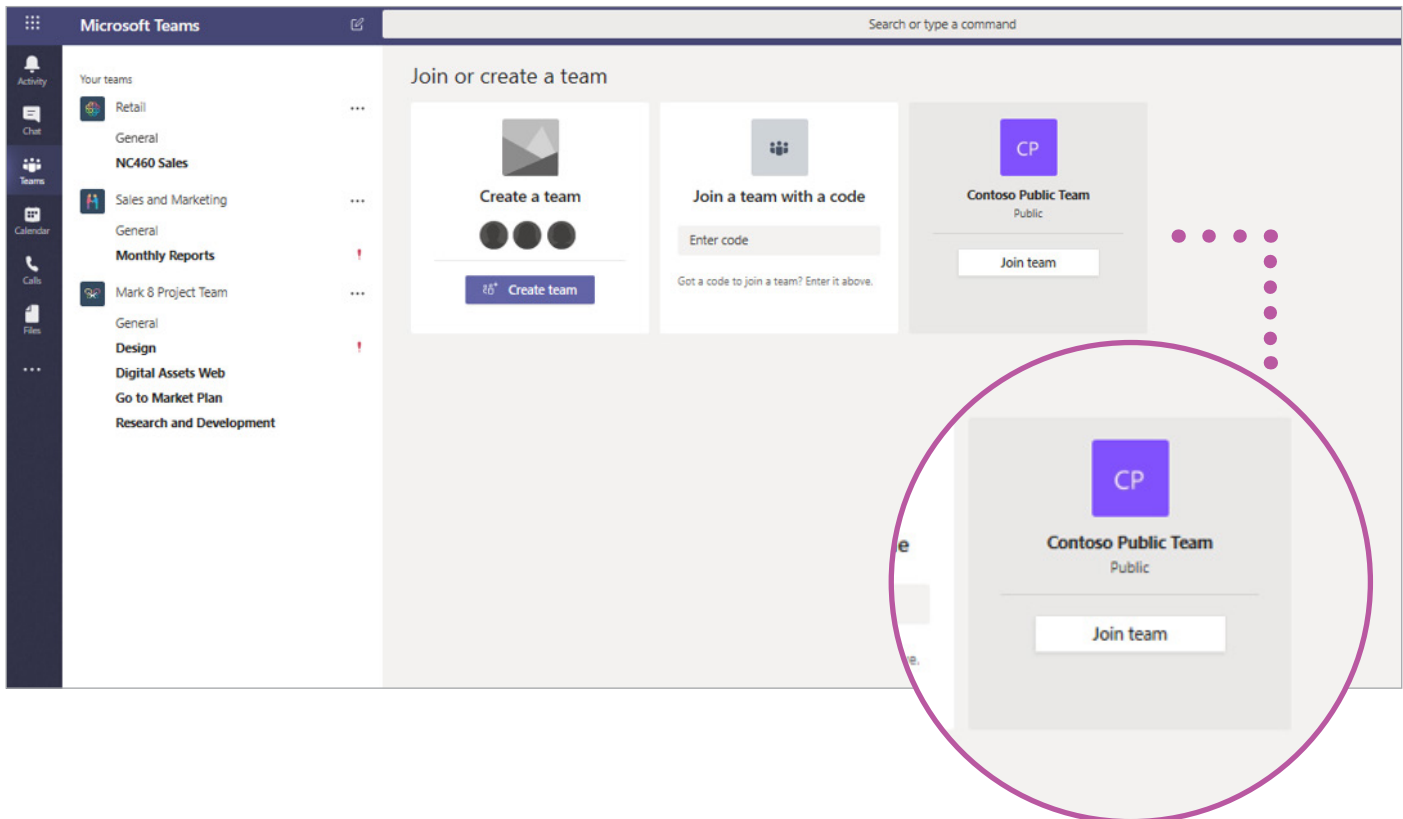
Challenge: External Access

The next issue to consider is sharing with external guest users whose accounts and credentials are not controlled within your Office 365 tenant. By default, at the tenant level, Office 365 Groups allow Owners (therefore end users) and Office 365 global administrators the ability to:
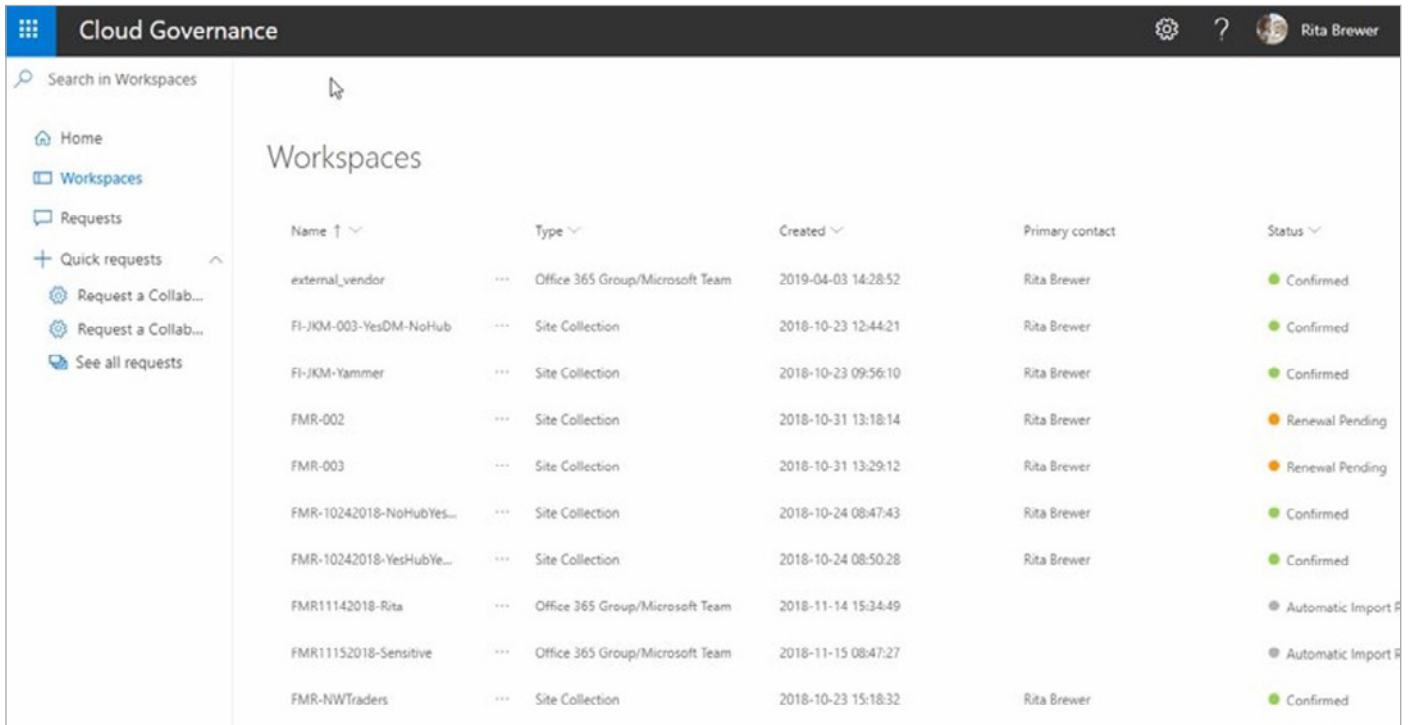
1. Add external guests as Members.

2. Provide external guests and Members access to Group files and OneNote.

Since this is at the tenant level, this is an all or nothing proposition. However, some departments may have a greater need for external collaboration and deal with less sensitive information. To establish multiple policies and more granular controls over external sharing, you need a third-party governance tool.

	Department A	**Department B**	**Department C**
External Sharing	No External Sharing	External sharing allowed in:	External sharing allowed only in:
Expiration/ Retention	**6 Months** after last accessed	**12 Months** after last accessed	**9 Months** after last accessed
Allow These Users to Create a Team	All requests through Central IT	All requests through Department IT	Only Joe, Sally, and Harold can create
Recertify Members	after **3 Months**	after **6 Months**	after **12 Months**

Management

Even in scenarios where organizations have control over the creation process, managing workspaces, users and other features through their lifecycle to maintain a secure and organized collaboration platform can be a challenge.

Challenge: Recertifications

Part of the ongoing management of Microsoft Teams and Office 365 Groups is recertifying permissions and metadata. In other words, making sure that the right people have the right authority in the Group and that the Group is labeled and categorized with the correct business context.

Recertification tasks are often manually intensive and require extensive communication between IT and business users. However, they're a critical component to ensuring ongoing secure collaboration.

Challenge: Correcting Non-Compliant Actions

As teams audit and review information in their systems, it will be necessary to correct settings and permissions that do not align with business policies.

For example, let's say that during the recertification process, it's discovered that a Group has several junior members with improper permissions. Perhaps they shouldn't be Owners of a particularly important Group or maybe they are in a Group that has sensitive information that they should not be able to access.

This can also require communication with end users and stakeholders to justify such changes and advise of the corrections. Depending on what needs to be corrected, this can involve a small number to many hours of communications and meetings, let alone the actual correction of solution settings to fix the problems.

Challenge: Reporting

Reporting is an important and frequent operational procedure that allows IT to communicate critical aggregate information to the business. Reporting on the number, membership, permissions, and purpose of Groups can be time consuming.

It is much more effective to automate administrative and security reports to be generated on schedules of the organizations choosing detailing:

- Why a site is provisioned
- Who is using it
- How it is being used
- Who has access
- Who has administrative rights to collaboration

End of Lifecycle

There are many things that happen to a Group or Team throughout its lifecycle. Some can be small such as membership changes, others can involve a complete change of ownership. And in the case where projects, committees, or virtual groups eventually disband—so too should the Group or Team itself.

Challenge: Granular Expiration Settings

This becomes yet another challenge with using Teams...what happens when the Team no longer has reason to exist? Because a Team sits on top of Office 365 Groups there are now a number of artefacts left behind:

|	
SharePoint site	Conversation History
Document Library	OneNote File
Planner Board	Mailbox

These artefacts could contain private information and cost money to continue to manage, backup and store. Obsolete artefacts also make your collaboration environment messy. Old Teams and Groups degrade content quality within the organization, making it hard for employees to find the right information quickly.

The first thing that needs to be addressed is how to know when it's time to shut down the Team or Group. In many scenarios this will either happen manually or not at all—such that it will generally rely on a person to delete it themselves, ask IT to delete it, get prompted by IT or

someone else as to whether it is still required. Otherwise, the Team will simply stay there until IT decides to perform a clean-up.

It's possible to set tenant-wide expiration periods for Groups and Teams, to manually archive or delete Teams, but there are many hurdles to overcome in order to make these features actually align with business policies to ensure proper lifecycle management for any organization.

Naming conventions and labeling policies must be enforced for available organization wide policies to be effective.
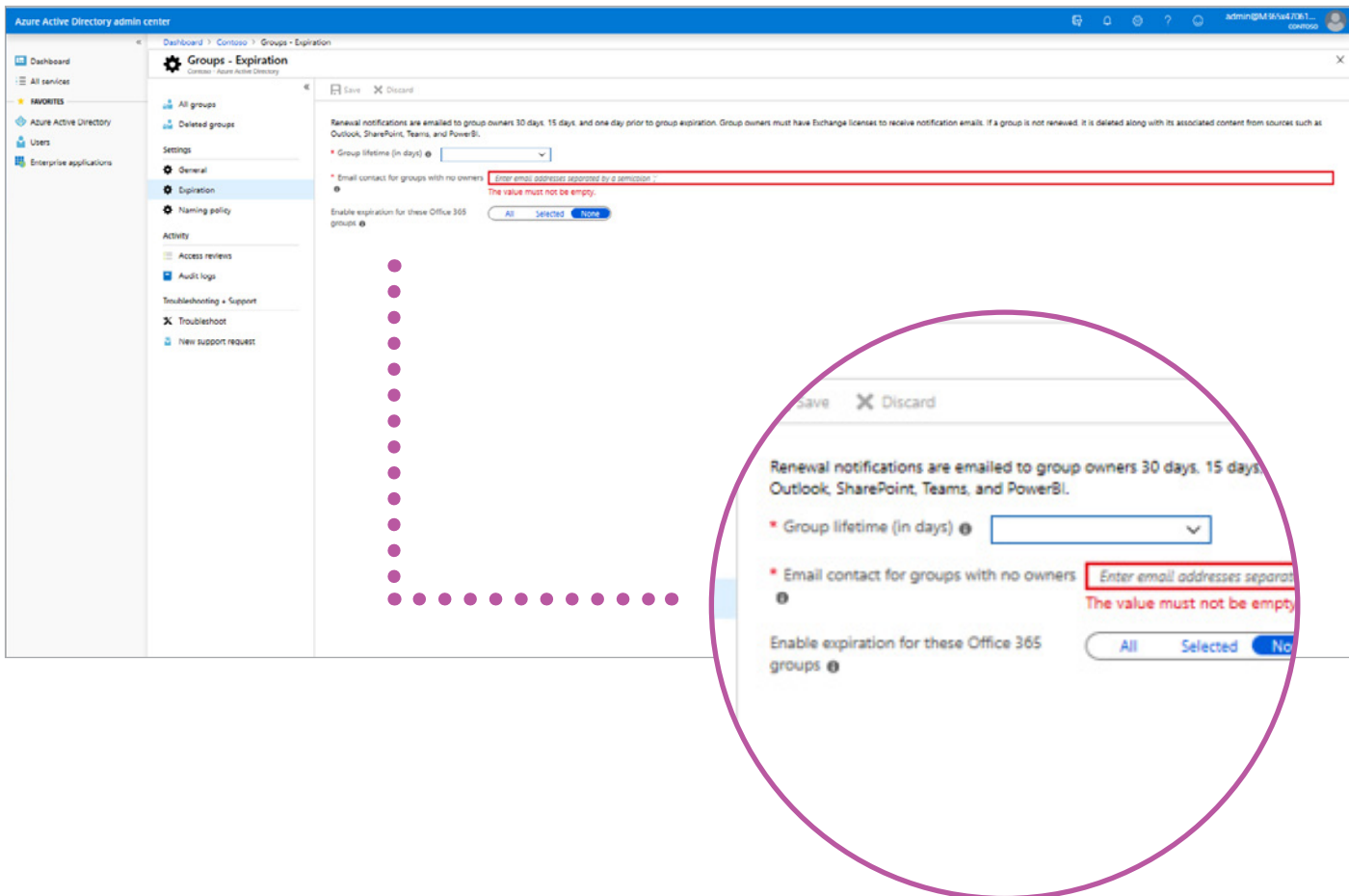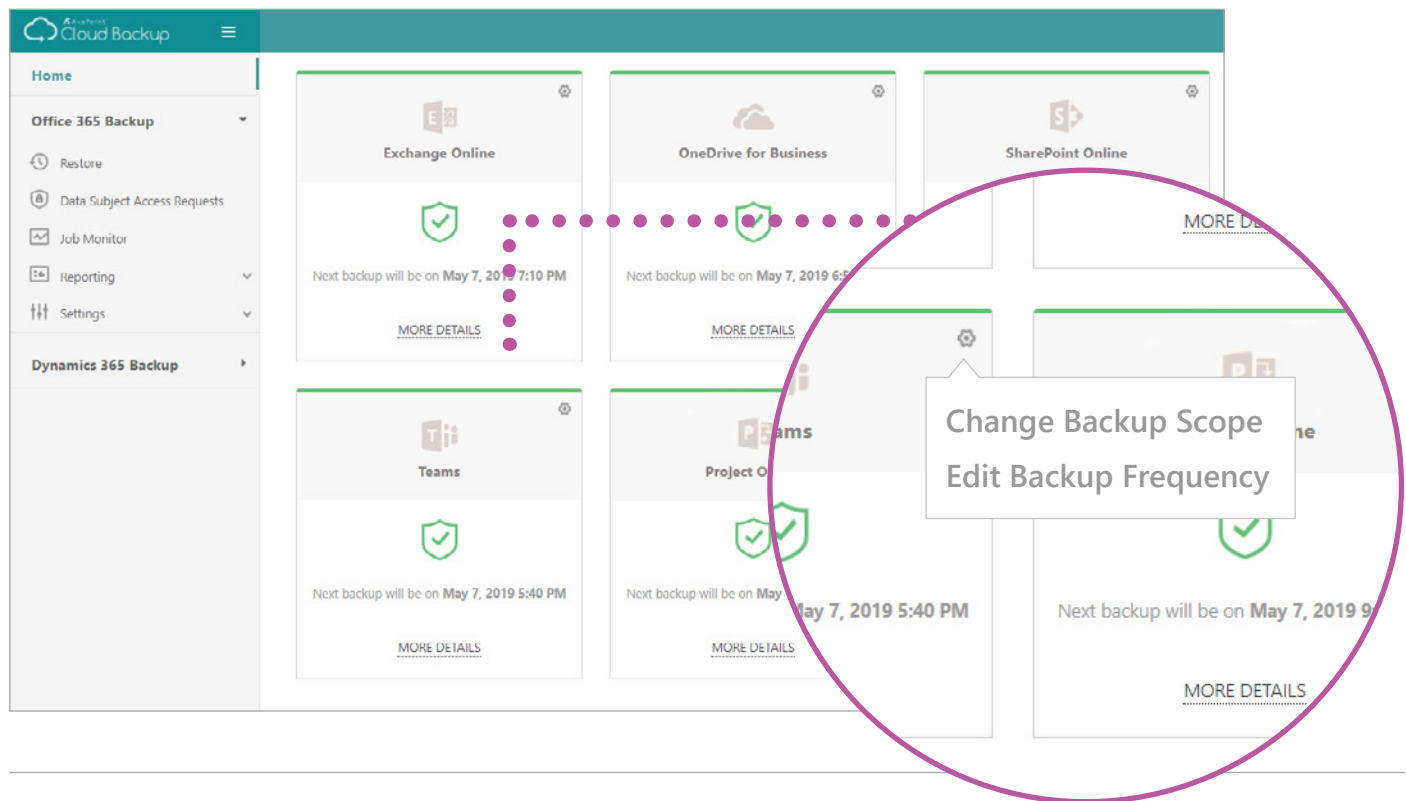
Challenge: Expiration Oversight and Reporting

In order to properly manage the lifecycle of data, organizations must have a high level of confidence that data is ready to be archived or deleted. Organizations need to have more than basic blanket controls when it comes to managing and enforcing lifecycle rules, and equally important, they need reporting and oversight over the process.

Challenge: Preventing Improper or Accidental Deletion By Owner

As previously mentioned, end users can become Owners of a Group or Team, with the power to delete the Group. What happens to the critical business information contained within when the owner either purposefully or accidentally deletes the Group?

Gulp... By default, if caught within 30 days it can be restored using native functionality. If it's been longer than 30 days past deletion, you will be wishing you had acquired a third-party Office 365 backup solution like AvePoint Cloud Backup (or grateful that you did).

IN SUMMARY

While provisioning may get the most attention, as that is where many important Group functions are first set, the ongoing management and end of lifecycle are equally, if not more important.

Stay up to date with
the latest information.
Check out our blog.

www.avepoint.com/blog

AvePoint
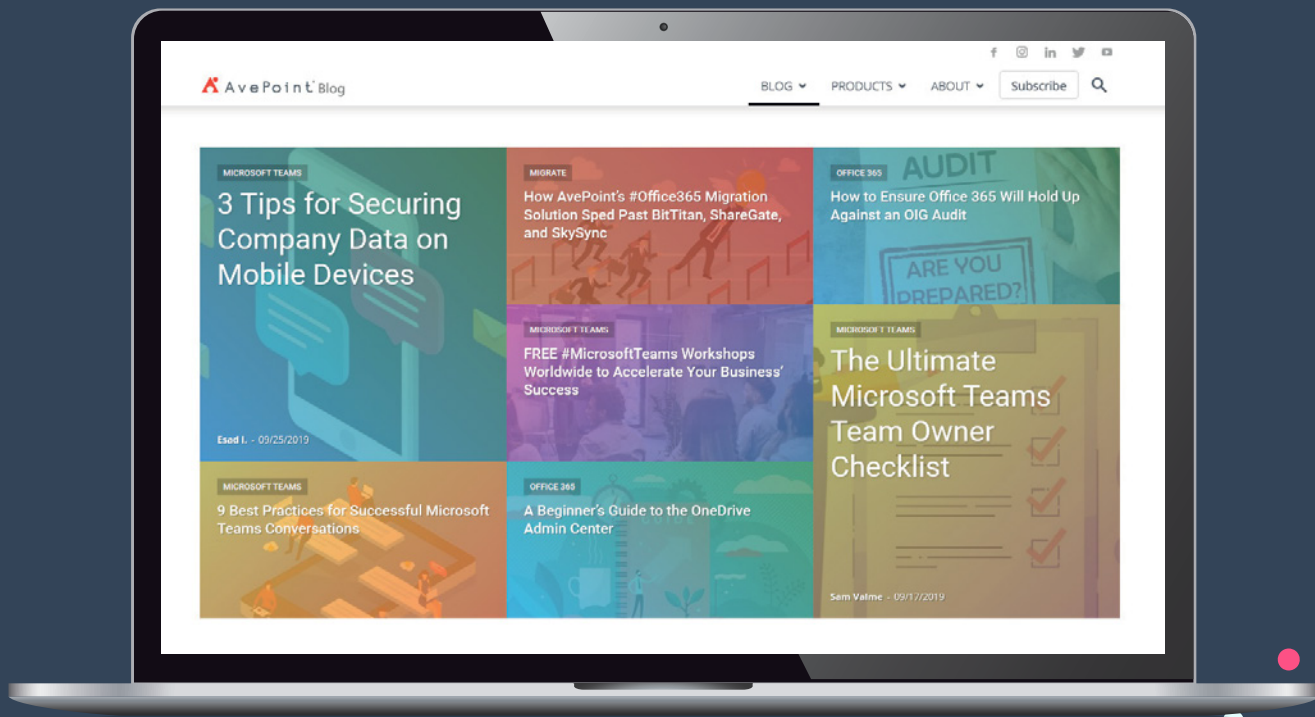
Section 2

Right Sizing Your Level of Governance

AvePoint®

Right-Sizing Your Level of Governance

For each organization, there is a balance between providing your users unfettered access to Office 365 services and ensuring the proper procedures and policies are being followed. It's important you find what level of governance is right for your organization based on a number of key criteria.

Once that is determined, you will be able to make informed decisions around the tactics required to establish, maintain and enforce the selected governance level.

Questions to Determine Your Level of Governance

1 *Who should be able to create Office 365 Groups and Microsoft Teams, and what does that process look like?*

We find that the appropriate approvers may be business owners, but IT needs to approve the type and scope of what's available to which subset of users. Content owners and stakeholders understand their processes and the information in their collaboration spaces, but this does not mean they can be trusted to manage the complex governance and security of integrated applications like Microsoft Teams.

There needs to be enough control to keep the creation process in line with business policies. At the same time, the process also needs to be quick and simple enough for end users to understand it. IT tickets and emails are really not the best way to do this, especially on a large scale.

2 *For what purpose should users be able to create Groups and Teams?*

At first, it may seem great to allow everyone to provision these spaces. However, we've seen organizations with 2,000 users that have 2,500 Office 365 Groups! It's super important to communicate with your users and stakeholders and come up with criteria around how and why it's ok for people to create collaboration spaces.

3 *How can your organization manage access and ownership?*

Does your department have the appropriate resources to monitor and keep track of Group/Team roles and access? Do they understand the power of Admins (new), Owners, Members, and External Members in Microsoft Teams? Keeping track of who has access and administrative rights over the features that Office 365 Groups and Microsoft Teams bring to the table is vital to managing risk and resources.

4 *What applications and services will users be allowed to add?*

It is now possible to control which applications and integrations can be added to Microsoft Teams at the Team level. A common scenario is when IT doesn't want to enable external sharing. Should users then be able to connect their Microsoft Teams to other cloud storage solutions? Planning policies and a process that enforces them is very important when it comes to how this is managed.

5 *How will you structure and enforce properties and naming conventions?*

As previously mentioned, controlling how people name Groups and Teams and being able to apply properties based on how people are using Microsoft Teams and other collaboration spaces is key when it comes to maintaining the lifecycle of your data. You cannot apply policies and maintain the lifecycle of your data if you don't know why a Microsoft Team exists and what kind of information resides within its storage areas.

6 *What content in which Teams will be saved, archived or deleted, and after how long?*

Even though Microsoft Teams is a new format for collaboration, people will still be sharing files and documents back and forth, and those files will still be stored within the SharePoint sites that support the Team. This means that the classic questions around content lifecycle, records management and data protection/DLP will still need to be addressed.

IN SUMMARY

If you find the answers to your questions above are some version of A) anyone B) for any reason C) or it doesn't matter, then an ungoverned system might be appropriate for your organization. If your answers are some version of A) a controlled subset of users B) it depends C) I don't know but it needs to be done, then a light or fully-governed system is more appropriate.

Symptoms of an Under-Governed System

Under-governed collaboration systems are full of pain points and opportunities for operationalization. Here is how to find out if your collaboration system may be under-governed.

1 **Users struggle to find information** as they are forced to sort through the confusion of randomly and similarly named content and collaboration spaces.

2 **IT tickets, emails to stakeholders and questions slow production.** People attempt to look for the proper applications and collaboration spaces to complete their tasks, and as they attempt to find work arounds, more out-of-policy content is created.

3 **Business processes vary from department to department.** There is no consistency across the organization causing IT security teams and users to spend time explaining processes and content every time any audits or risk reduction activities take place.

4 **Inconsistent training.** IT cannot create uniform trainings for the organization because of a wide variety of business practices.

5 **Shadow IT emerges.** The security or legal teams start to realize that the tools at their disposal designed to mitigate risk have been neither sufficient nor properly implemented, causing the organization to go through an in-depth security audit and content restructuring project that becomes a major burden on the entire organization.

6 **Ad-hoc and informal processes.** Users and stakeholders do their best to come up with ways to work, but their processes are inefficient and do not adhere to business policies.

7 **Fire-fighting by the IT Team.** Corrective actions, lots of communication and troubleshooting and many user requests burden the IT team on a constant basis.

8 **Slow adoption**. The team is unsure of where and how users are finding value in your systems. Because they are unaware of how to collaborate more efficiently, users do not feel like their lives are much easier or that they are able to get more done.

Right-Sizing Office 365 Governance

Recommended Features for Ungoverned, Lightly Governed and Fully Governed Organizations

M	Office 365 Feature
A	AvePoint Feature
*	Planned
$	Requires AAD Premium

LEVELS OF GOVERNANCE:

🟧 Ungoverned 🟥 Light ⬜ Full
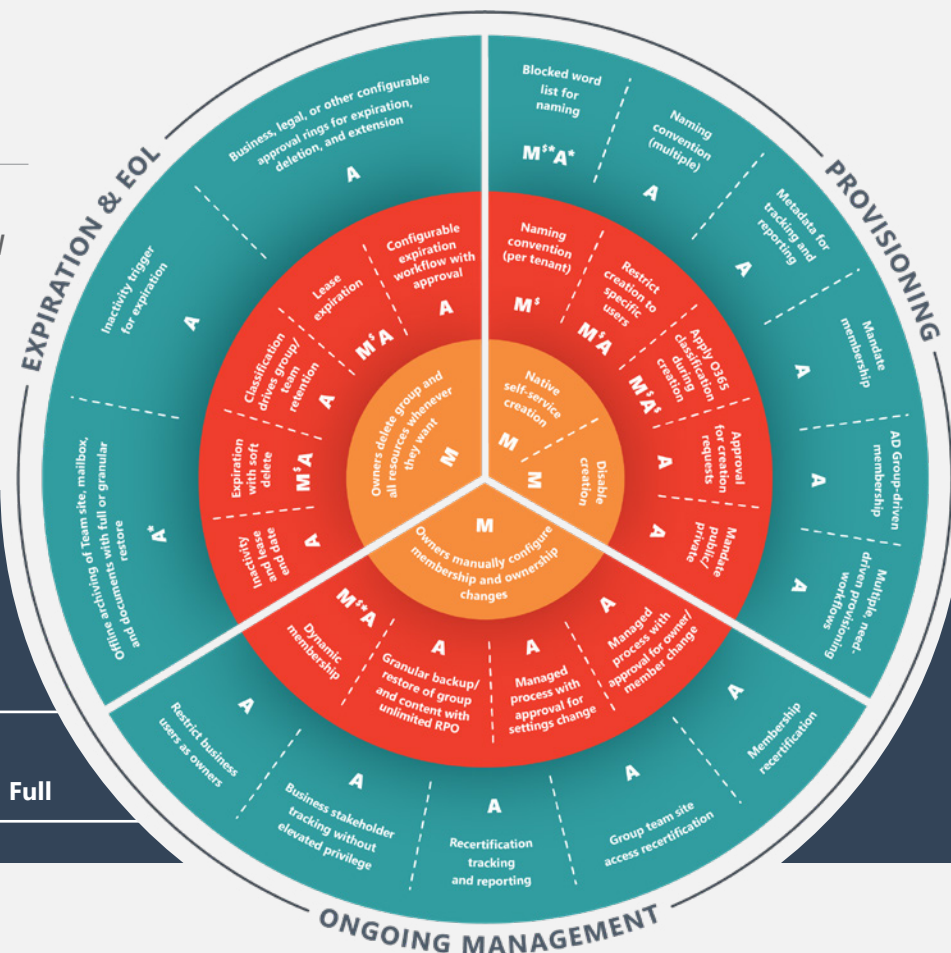
The Third Way: AvePoint Cloud Governance

Commonly there are attributes of your workspaces that you'll want to understand— things like:

- Who is the business owner of this workspace? Did they formally accept responsibility for managing it?

- When was the last time someone attested that the access permissions to the workspace were correct?

- What department owns this workspace?

- What's the primary purpose of this workspace?

- What's the highest level of sensitivity for the work being done here?

- When was the last time this workspace had all the above information validated?

Normally you would gather the information above during a managed provisioning process. But if you want to remove barriers to productivity for your users and leave the native Office 365 self-service provisioning of Office 365 workspaces active, how can you ensure that you collect these necessary details and, as importantly, keep them current over time?

AvePoint's Cloud Governance solution has long supported the ability to have an automated and fully-managed provisioning process for SharePoint and Office 365, giving you control of every option and setting available to the user, and then allowing you to pass that request through a fully configurable approval process.

AvePoint Cloud Governance latest feature is called "Automatic Import" but we refer to it internally as "create and chase." Essentially, it allows you to leave the native self-service options for Office 365 turned on, but then automatically chase the requesting user and require them to formally accept ownership of the workspace

and supply any necessary additional governance details, such as those listed above.

See how AvePoint Cloud Governance can accomplish all of this as well as enabling:

- **Improved operations** - Formalization of processes, available services, and IT SLAs
- **Improved IT Spend ROI and productivity** - User visibility into organizational content structure so they know where to find, and when to use content and applications, so the organization truly reaps the benefits of their spend on Office 365.
- **Risk avoidance** - Security and permissions structures are enforced so that users only have appropriate rights or access, and the purpose of content is clearer to everyone in the organization, reducing unintentional breaches.

Visit **avepoint.com/products/cloud/office-365-governance/** to request a demo or free trial.
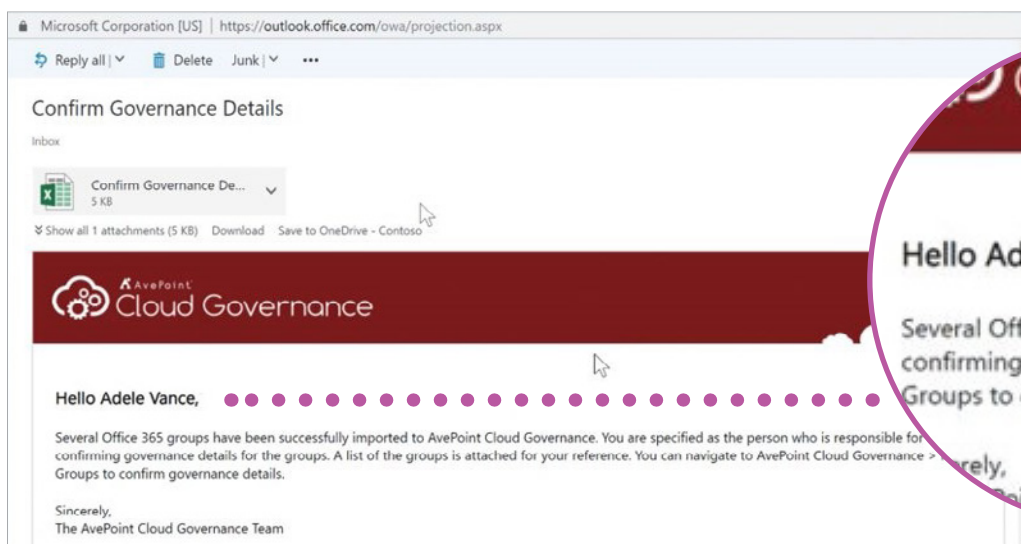
How We Calculate the Value of Automated Governance

Automated Governance Value Calculator Explanations

Understanding the process played out by IT in order to maintain operational governance is critical when we look at productivity and time savings calculations.

For this series of calculations, savings comes as a combination of hours saved by IT no longer being forced to manually configure collaboration spaces, and admins and users alike not having to communicate to clarify understanding of what is possible from what the users need.

As IT teams become less burdened with processing these requests, they in turn can work on strategic solutions to add further increased productivity to business operations.

However, while it's critical to understand this, we're just scratching the surface when it comes to understanding the value of automated governance. Arguably the risk reduction, having easy to find content, and additional security provided by a well-governed system are just as, if not more important than the time you are saving your IT admins and end users.

Provisioning

Requirement verification

When it comes to creating workspaces in Office 365, many organizations limit creation to a set of users or admins who have the responsibility of receiving requests, then creating the workspaces with the necessary security and content settings applied. This process can take many hours for a number of different reasons. Sometimes, the person who should or can have access to a certain workspace might need to be verified before it's created.

Often, users are unclear in their requests, and admin teams may need to go back and forth communicating with one or more users to clarify what is needed and verify that the user's request is within organizational policies. Once the requirements have been clarified and verified, then the security and content settings need to be applied for the workspace in question. After it's created, users may go back and forth with the admins again to request changes or corrections needed as a result of the initial provisioning process.

Many of our customers admins spend hours and hours per workspace walking through this process. In some organizations, it's not unusual for the entire provisioning process to take from two to six weeks from start to completion, though admins may only spend a dozen or more hours per site communicating and adjusting settings in Office 365.

PROVISIONING TOOL

We have conservatively estimated that it takes an average of within a range of about two to five hours of time per workspace per year to review requests, communicate with end users and align with policies.

Management

Permissions Recertification

In order to run a permissions audit in Office 365, one must either navigate through the SharePoint settings:

Or run a PowerShell script to get the permissions to a location:


```
PS C:\WINDOWS\system32> Get-SPOSite | ForEach {Get-SPOUser -Site https://m365x102466.sharepoint.com/sites/ContosoMarketi
ngCentral } | export-csv -path .\user.csv
```

	A	B	C	D	E	F
1	#TYPE Microsoft.Online.SharePoint.PowerShell.SPOUser					
2	DisplayName	LoginName	IsSiteAdmin	IsGroup	Groups	UserType
3	Adele Vance	adelev@m365x102466.onmicrosoft.com	FALSE	FALSE	System.Collections.Generic.List`1[System.String]	Member
4	Alex Wilber	alexw@m365x102466.onmicrosoft.com	FALSE	FALSE	System.Collections.Generic.List`1[System.String]	Member
5	Allan Deyoung	alland@m365x102466.onmicrosoft.com	FALSE	FALSE	System.Collections.Generic.List`1[System.String]	Member
6	All Users (windows)	windows	FALSE	TRUE	System.Collections.Generic.List`1[System.String]	Member
7	Christie Cline	christiec@m365x102466.onmicrosoft.com	FALSE	FALSE	System.Collections.Generic.List`1[System.String]	Member
8	Debra Berger	debrab@m365x102466.onmicrosoft.com	FALSE	FALSE	System.Collections.Generic.List`1[System.String]	Member
9	Diego Siciliani	diegos@m365x102466.onmicrosoft.com	FALSE	FALSE	System.Collections.Generic.List`1[System.String]	Member
10	DProdMGD105_spocrwl_191167	dprodmgd105_spocrwl_191167	FALSE	FALSE	System.Collections.Generic.List`1[System.String]	Member
11	Emily Braun	emilyb@m365x102466.onmicrosoft.com	FALSE	FALSE	System.Collections.Generic.List`1[System.String]	Member
12	Enrico Cattaneo	enricoc@m365x102466.onmicrosoft.com	FALSE	FALSE	System.Collections.Generic.List`1[System.String]	Member
13	Everyone		TRUE	FALSE	TRUE	System.Collections.Generic.List`1[System.String]	Member
14	Everyone except external users	spo-grid-all-users/0ce5452f-a6b8-4ed7-8355-7c43846024cc	FALSE	TRUE	System.Collections.Generic.List`1[System.String]	Member
15	Grady Archie	gradya@m365x102466.onmicrosoft.com	FALSE	FALSE	System.Collections.Generic.List`1[System.String]	Member
16	Henrietta Mueller	henriettam@m365x102466.onmicrosoft.com	FALSE	FALSE	System.Collections.Generic.List`1[System.String]	Member
17	Irvin Sayers	irvins@m365x102466.onmicrosoft.com	FALSE	FALSE	System.Collections.Generic.List`1[System.String]	Member
18	Isaiah Langer	isaiahl@m365x102466.onmicrosoft.com	FALSE	FALSE	System.Collections.Generic.List`1[System.String]	Member
19	Johanna Lorenz	johannal@m365x102466.onmicrosoft.com	FALSE	FALSE	System.Collections.Generic.List`1[System.String]	Member
20	Joni Sherman	jonis@m365x102466.onmicrosoft.com	FALSE	FALSE	System.Collections.Generic.List`1[System.String]	Member
21	Jordan Miller	jordanm@m365x102466.onmicrosoft.com	FALSE	FALSE	System.Collections.Generic.List`1[System.String]	Member
22	Lee Gu	leeg@m365x102466.onmicrosoft.com	FALSE	FALSE	System.Collections.Generic.List`1[System.String]	Member
23	Lidia Holloway	lidiah@m365x102466.onmicrosoft.com	FALSE	FALSE	System.Collections.Generic.List`1[System.String]	Member
24	Lynne Robbins	lynner@m365x102466.onmicrosoft.com	FALSE	FALSE	System.Collections.Generic.List`1[System.String]	Member
25	Megan Bowen	meganb@m365x102466.onmicrosoft.com	FALSE	FALSE	System.Collections.Generic.List`1[System.String]	Member
26	Miriam Graham	miriamg@m365x102466.onmicrosoft.com	FALSE	FALSE	System.Collections.Generic.List`1[System.String]	Member

Once the information is gathered, then the roles must be checked against business policies and the nature of the content to successfully complete an audit/recertification of this information.

If done properly, this process can take several hours for each collaboration space. Permissions recertification with AvePoint Cloud Governance enables administrative and security reports to automatically be generated on schedules of the organizations choosing. This means that depending on why a site is provisioned, who is using it and how it is being used, reports showing who has access and who has administrative rights to collaboration spaces can automatically be generated for review.

Metadata Recertification

In order to make certain that the properties and classification of collaboration spaces and content match business policies, IT must com-municate with users to confirm the purpose of use. Once this is done, usage must be checked against business policies.

Communication between IT and end users for this purpose and analyzing the usage of content can also take a great deal of time.

With Cloud Governance, it is possible to contextually add metadata to collaboration spaces as they are being provisioned, and force accuracy by adding properties reflecting the business use. This is done based on the users, user properties, organization structure and by forcing the requester to select among a few options during the provisioning process.

More than the hours of work per site, automating metadata recertification reduces risk. It can also drastically reduce the time that end users spend looking for information by keeping collaboration spaces and content properly labeled and organized, search results become more efficient.

Correcting Non-compliant Access & Settings

As teams audit and review information in their systems, it will be necessary to correct settings and permissions that do not align with business policies. This can also require communication with end users and stakeholders to justify such changes and advise of the corrections.

Depending on what needs to be corrected, this can involve a small number to many hours of communications and meetings, let alone the actual correction of solution settings to fix the problems.

AvePoint's Cloud Governance brings with it the ability to automatically enforce business policies, such that if users make changes to settings or permissions that are out of business policies, the actions can be automatically reverted by the solution with notifications sent to the appropriate parties. It's also possible to send notifications without corrections, or make corrections without notifications.

MANAGEMENT TOOL

We have conservatively estimated a range within about two to six hours per year, per workspace with most of this being IT administrator time and a smaller proportion being time spent by end users.

End of Lifecycle

Archiving & Managing Content Lifecycle in Office 365

The implications of a well-enforced lifecycle process are clear: users find relevant content faster, and don't waste as much effort re-creating what's already there.

In addition, organizations do not have to worry about retaining relegated content for discovery, and the ability to more quickly and accurately assess information reduces risk and shortens any audits that may need to take place.

In order for the tenant-wide archiving and retention settings to work in Office 365, users must strictly adhere to correct labeling and naming conventions, which makes the systems available difficult to enforce.

As the volume of content and collaboration spaces increase in the tenant, so too does the work required for IT to confirm that content can be deleted or archived and tracked. And to do this again, it requires communication back and forth with the content owners to confirm the nature of the content, and whether it can be removed or archived. As users continue to use Office 365, more and more content is added

to the environment, but studies are showing time and again, only about 20% of that content remains relevant.

By automating and enforcing metadata policies, naming conventions, and keeping an accurate record of how users are interacting with content, organizations already have a baseline to understand what needs to be kept long-term, and what can be deleted after various increments of time.

AvePoint's Cloud Governance can allow organizations to apply retention policies for various times on content based on the nature of the content and its relevance to users based on their roles, and any of the factors we've explored above. This means that far beyond blanket retention policies, organizations have an enormous amount of control over archiving or removing stale data and irrelevant content as soon as allowed by business policies and regulations. The solution provides reporting on all lifecycle management activity and adds approval workflows, so neither IT nor business users get any surprises.

Extension of Workspaces

In addition, the solution enables a request for an extension, so if users still need content, they can request that a collaboration space it remains active, but IT has the ability to add an approval to this, and the users must provide a reason to keep the content.

END OF LIFECYLCE TOTAL

We have conservatively estimated a within about one-to-three hours per year per workspace to review content, communicate with end users and ensure proper expiration policies are followed.

The Numbers: Web Calculator Assumptions

The following table outlines our assumption for how many "minutes per workspace, per year" assumed for every level of effort outlined by admins seeing workspaces in Office 365 for the web calculator. The tasks associated with the categories listed below correspond with outlines described above.

Minutes Per Workspace, per Year	Low Effort	Medium Effort	High Effort	With AvePoint
	PRE	PRE	PRE	POST
Services and Provisioning	**120**	**185**	**275**	**115**
Communications and planning	30	60	120	20
Provisioning and Setup	90	125	155	95
Auditing and Security	**130**	**235**	**336**	**58**
Updating Security and Configuration Changes	40	50	60	30
Auditing Roles and Permissions	39	80	120	20
Collecting Metrics and Reporting	51	105	156	8
Life-Cycle Management	**72**	**144**	**216**	**31**
General Workspace Management	30	60	90	15
Archiving and Deleting Workspaces	42	84	126	16

The calculator assumes a standard rate of $67.67 per hour (this rate is a national average for IT workers with PTO and holiday time removed in consideration from the calculation).

For the web calculator, we assume that an organization has 12% the number of active workspaces in Office 365 as they have employees.

Additional Assumptions: In addition to these assumptions, the growth of adoption of Office 365, the cost of paying information workers to

utilize and maintain AvePoint's Cloud Governance Solution, as well as the list cost of our product licenses have all been factored into the equation.

For Additional Factors and Custom ROI Estimates, Contact Us Today! Our teams have the ability to custom tailor all of the factors listed above and more to your organization's estimates or actual numbers.

Real World
Results

AvePoint

Real World Calculations

The following data has been aggregated from a real customer example with data specific to their organization. If you reach out to our team, we can customize all estimates specifically for your organization to come up with accurate potential benefit that can be reached with the implementation of our Cloud Governance solution

Example: International Luxury Good Company

Headcount: 38,000 employees

Starting Number of Workspaces: approximately 12,000

Workspace Growth Rate: 30% per year

Manual vs. Automated Work Tasks: All tasks are manual.

Maintenance Staffing: One employee will spend 25% of their time maintaining our solution

Additional Factors Going into Estimate:

1. This customer is starting with a pre-existing workspace count in Office 365 of 12,000. 12,000 workspaces are a lot to manage from a governance operations perspective.

2. After 3 years the customers site count more than doubles in size.

3. Only a single User Type and salary is specified.

Time Workload Estimates

Provisioning | .98 hours for each existing workspace | .66 hours for each new workspace

Management | 12.17 hours for each existing workspace | 0 hours for each new workspace

Expiration | .58 hours for each existing workspace | 0 hours for each new workspace

Time Savings Estimates

Year 1:   160,725 hours

Year 2:   208,942 hours

Year 3:   281,624 hours

CASE STUDY

SUCCESS HIGHLIGHTS

Enabled the deployment of Office 365 and Teams by extending strict internal container governance policies to the provisioning of new sites, Teams and Groups.

Worked closely with Microsoft to obtain necessary APIs to remove security concerns around service accounts.

Provided close monitoring into the container access of internal and external users.

Cut deployment timeline from six to three months.

Customer Profile

The global pharmaceutical company is a public, Fortune 500 company based in the United States. It has more than 65,000 users and 20 terabytes of data within its SharePoint environment. The company has been an AvePoint customer since 2007, previously using Governance Automation to govern the provisioning and lifecycle of its on-premises SharePoint sites. It has a large internal IT team and places a priority on security.

The Challenge

One of the global pharmaceutical company's highest priorities is to attract the next generation of talent. The company believes implementing and maintaining a modern workspace, in this case Office 365 and specifically Microsoft Teams, is a key enabler for this goal.

During an 18-month migration and cycle to the cloud, the company discovered it could not turn on Microsoft Teams given its internal security and governance policies. At the global pharmaceutical company, container level access is paramount. All containers must be tagged, classified and monitored with internal and external access fortified.

It's also important for the company to have a clear understanding of which users have access to what collaboration

containers, particularly external users. This is somewhat complicated by the fact the company employs numerous 1066 contractors on multi-year contracts that it considers external users.

Additionally, the company's security team preferred to avoid service accounts where possible to manage Office 365.

The AvePoint Solution

AvePoint played the role of trusted adviser throughout the company's transition to the cloud, frequently consulting on matters related to governance. AvePoint is deploying its Governance Automation solution (soon to be its Cloud Governance solution once the company is all-in the cloud) to enable the use of Microsoft Teams so that is compliant with internal governance policies.

Every time a Team, SharePoint site or Office 365 Group is created it is automatically classified by AvePoint's governance solution using the company's low impact, medium impact or high impact definitions.

Low impact containers have no secure information and can be public, medium impact containers might possibly have some secure information and permission management is needed, high- impact containers have information only certain people should have access to and settings need to be recertified on a regular basis.

These classification and governance policies are inclusive of all resources that get spun up in conjunction with the creation of a Team including OneNote, SharePoint and Outlook.

All Team names are also governed and approved to avoid the unauthorized use of Team names like "IT Help Desk" or "CEO Team #1."

AvePoint, as one of 40 Tier Zero Microsoft partners worldwide, also worked closely with Microsoft and lobbied on behalf of the global pharmaceutical company to get key APIs released. These APIs allowed AvePoint to "dumb down" the service accounts and lower their permission and access to company systems, completely removing all implementation concerns from the security team.

The Bottom Line

By automating this governance process across all user requests for the creation of new virtual workspaces, other companies that have reported their processes have been reduced from four days to four hours. For the global pharmaceutical company, it has been the difference between fully leveraging Office 365 and Microsoft Teams or remaining on the sidelines.

The company deployed a test tenant and a production tenant as part of its move to the cloud. It set a six month deployment timeline for AvePoint's governance solution, but has cut that in half. All testing has been completed and live deployment will take place in November of 2018.

The next priority for the company will be to create divisional policies on recertification and permissions of containers. AvePoint will be with them throughout their digital transformation to ensure their success.

AvePoint
525 Washington Blvd, Ste 1400 | Jersey City, NJ 07310
P: +1.201.793.1111 | **E:** sales@avepoint.com
www.avepoint.com

RESOURCES

NEXT STEPS

- **Governance Value Calculator & Consultation Request**
- **Cloud Governance Product Page & Request a Demo**

UNGATED

- **AvePoint Blog**
- **Matt Wade's Definitive Guide to: Everyday Etiquette in Microsoft Teams**
- **What to Use When Infographic**

WEBINARS

- **Tailoring Microsoft Teams & Delegating Administration in Office 365**
- **6 Expert Microsoft Teams Adoption Strategies THAT WORK**
- **How Microsoft Upgraded 200,000 Users from Skype to Microsoft Teams (And You Can Too!)**
- **Beginner to Super User: Top 10 Microsoft Teams Tips**
- **How To Achieve 90% Microsoft Teams and Yammer Adoption in 3 Months**

EBOOKS

- **How to Use and Manage Office 365 Groups and Microsoft Teams**

AvePoint®