

Using and Tailoring Microsoft Teams for Your Organization

How to handle surging activity in teams and boost security and compliance.

Using and Tailoring Microsoft Teams for Your Organization

Table of Contents

| | |
|---|--------------|
| Chapter 1: Introduction..... | pg 3 |
| <i>The New Culture of Teamwork.....</i> | <i>pg 4</i> |
| Chapter 2: Introductory Overview of Teams Components..... | pg 7 |
| <i>The Team Workspace.....</i> | <i>pg 7</i> |
| <i>Private Channels.....</i> | <i>pg 8</i> |
| <i>Tabs.....</i> | <i>pg 9</i> |
| <i>Third-Party Apps.....</i> | <i>pg 9</i> |
| <i>Chat and Meetings.....</i> | <i>pg 10</i> |
| Chapter 3: Configuring Teams..... | pg 11 |
| <i>Team Settings Configured By Owner.....</i> | <i>pg 11</i> |
| <i>Team Settings Configured By Administrator.....</i> | <i>pg 12</i> |
| Chapter 4: Tailoring Teams For Productivity..... | pg 18 |
| <i>Teams Cloning: The Copy and Paste For Teams.....</i> | <i>pg 18</i> |
| <i>AvePoint Cloud Governance.....</i> | <i>pg 19</i> |
| <i>Tailoring Teams Examples: Legal and Marketing Departments.....</i> | <i>pg 22</i> |
| Chapter 5: Taking Teams to the Next Level..... | pg 25 |
| <i>Optimizing and Delegating Administrator Access.....</i> | <i>pg 25</i> |
| <i>Information Management in Teams.....</i> | <i>pg 27</i> |
| Chapter 6: Case Studies..... | pg 29 |
| <i>Intrepid Travel.....</i> | <i>pg 29</i> |
| <i>Prudential.....</i> | <i>pg 31</i> |
| <i>Cambridge Consultants.....</i> | <i>pg 33</i> |
| Chapter 7: Additional Resources..... | pg 35 |



Introduction

Microsoft Teams is the fastest growing business application in Microsoft’s history for good reason. As the “hub for teamwork,” it is the unifying interface for what was previously a powerful but disparate toolset. As people started working from home in record numbers starting in March 2020, Microsoft Teams became essential technology and usage surged more than 110 percent.

However, as many organizations are discovering during their Teams rollouts, you simply can’t turn it on and hope for the best.

These “empty deployments” often result in patterns we have seen time and time again.

Either a surge of activity as users create Teams and invite other users as guests and then an adoption/productivity plateau outside of the occasional personal chat or VOIP call. Or in the case of a remote-first digital workplace, sprawling Teams and channels that make it difficult for users to find what they

need and for admins to ensure the right people have access to the right types of content.

To get the most out of Teams, you need to understand the key collaboration scenarios and associated regulatory requirements across the organization as well as each department and configure the service accordingly.

For organizations that have already seen an adoption plateau, or those that rapidly deployed Teams to support remote work during the COVID-19 pandemic, this eBook is for you too!

Each strategy discussed in this eBook can be layered on to improve existing implementations and mitigate many of the side effects of surging activity.

We’ll dive into the many ways of organizing Microsoft Teams to support the different shapes and routines of individual teams (and how to do it quickly by cloning). We will also include real examples of how to tailor different Teams components based on use cases, projects and departments seen in most organizations.

Both IT pros and business managers concerned with having the best of both sides will derive value from this eBook.

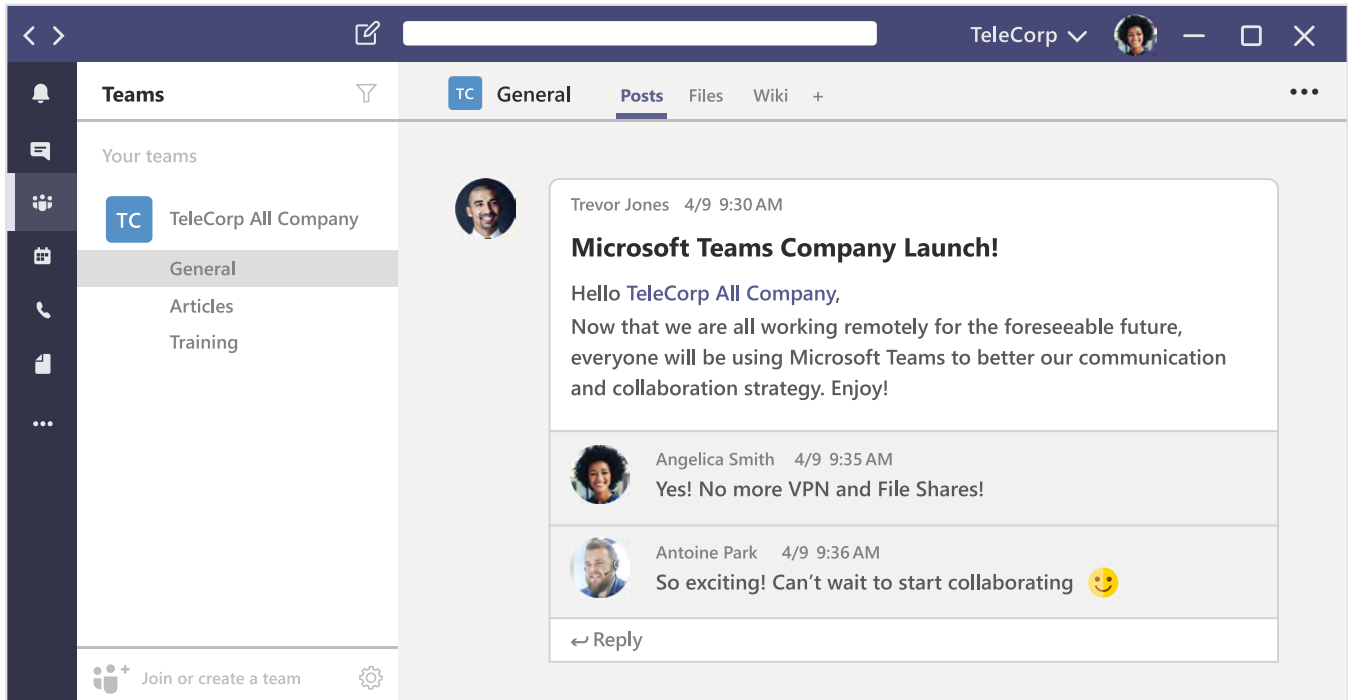
Note: The settings and information in this ebook may have evolved since publication. We will touch on governance and provide an introductory overview of different Teams components. However, Microsoft Teams governance is so important and nuanced that we devoted [an entire 50 page eBook to the topic](#).

We also have separate eBooks on everyday [Team etiquette](#) and [Office 365 backup strategies](#). If you are looking for additional information on these topics, we suggest you access these materials as well.

Now without further ado...



The New Culture of Teamwork



A new culture of teamwork is developing across organizations, as remote work becomes predominant and the older, disjointed and inefficient tools of yesteryear are replaced by modern tools for modern work styles.

The increased velocity of conversation, the greater porosity of organizational boundaries, and the growing demands for both productive collaboration and data protection is ruling out the continued usage of current tools.

Email, as the sole enterprise collaboration tool, just doesn't cut it anymore—either as a conversation medium or for sharing files. Delays, inefficiency, conversational confusion, and the never-ending stream of conflicting document versions result in a disjointed and confused digital workspace.

This can have negative repercussions for both productivity and security.

This is because the need for effective conversation, coordination and sharing of work in enterprise settings is being strongly influenced by changing patterns of interaction outside the enterprise. In their personal lives, your users are increasingly opting for

new chat-based tools such as WhatsApp, Facebook Messenger, and their ilk.

These streamlined and integrated social media and chat platforms are redefining expectations for communication at work. Equally, the concept of an “at work” location is changing too; the distinction is no longer between a work-only location and everywhere else. People need the freedom to work from anywhere, using new mobile devices and responsive applications.

Which is why, if these types of tools aren't provided by IT, people acquire them on their own and “shadow IT” starts spreading like weeds.

With low, or sometimes no monthly costs, it's easier than ever for each line of business to acquire its own Software-as-a-Service (SaaS) communication tool of choice. These easily available shadow IT cloud services lack governance and oversight, putting personal, sensitive and organizational data at risk of breach and misuse.

Trying to onboard employees into a bevy of disparate and separate resources is a hard task, resulting in greater onboarding time, more training sessions,

and an overworked IT department. Something has to change.

It is almost no wonder Microsoft Teams has taken the world by storm. The chat-based workspace for the enterprise delivers a unifying approach for modern work across Microsoft 365 (formerly Office 365), with a familiar conversational design to consumer tools and support for endpoint devices of all kinds, but with enterprise-oriented controls to support the digital transformation agenda.

Essentially, it federates a number of services and capabilities with which users are already familiar into a single pane of glass.

As a Microsoft offering, Teams's enterprise capabilities and cloud heritage creates a context defined by productivity, collaboration, and data protection.

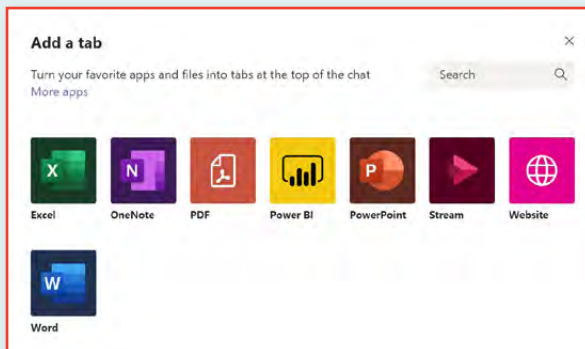
Nonetheless, using Microsoft Teams productively at an organizational level often requires extending native capabilities with third-party solutions. In particular, solutions that can provide appropriate guard rails, usage guidelines and automated policy enforcement to enable users to do the right thing. This helps avoid challenges (similar to those seen traditionally with undergoverend SharePoint deployments) such as sprawl, empty sites, and unquantified data protection risks.

At the tenant level, Microsoft's powerful administration toolkit for Microsoft Teams is generally an all-or-nothing proposition, meaning it doesn't fully support subset groupings of administrative rights for large and complex organizations. Likewise, all departments and lines-of-business in an overall Microsoft 365 tenant are constrained to the same tenant-wide settings. It is only with third-party tools that organizations can tailor settings like external sharing, private channel creation, and more by department (more on this later).

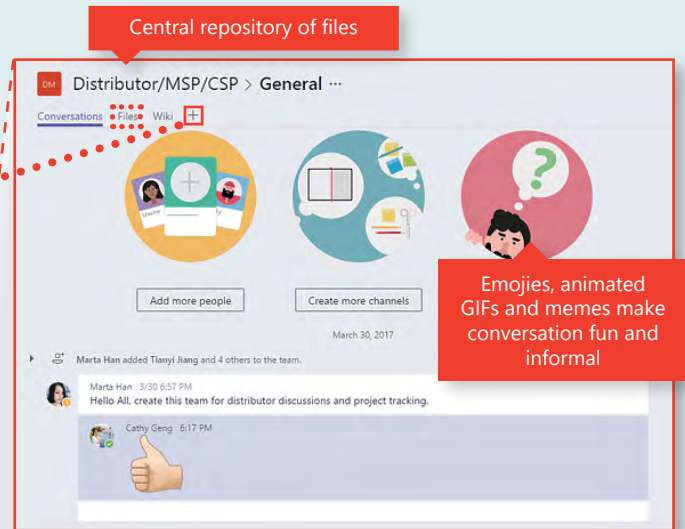
Some components of Microsoft Teams however are designed to be easily customized at the Team level. The following is a brief overview of those components, how they are organized and how they can be tailored to each department.



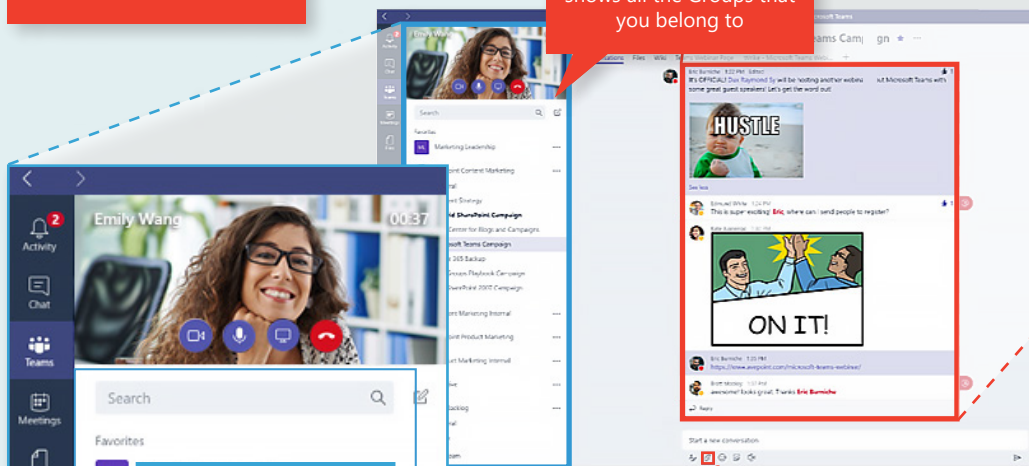
Tour of Microsoft Teams



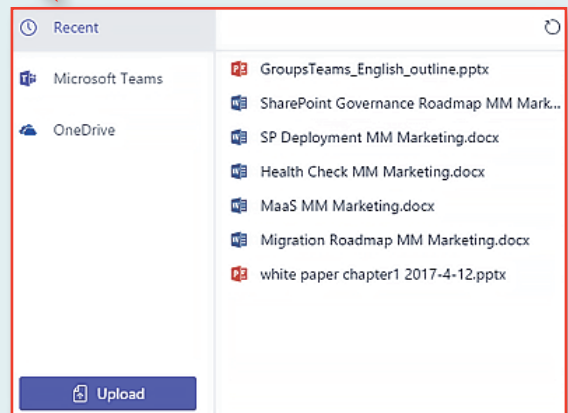
Microsoft Teams offers rich integration with some of the most commonly used applications



Left hand side panel shows all the Groups that you belong to



Channels help your team organize the conversation - you can dedicate a channel to a specific topic, project or discipline



Instantly upload and share files

Chapter 2

Overview of Teams Components

The basic shape of a workspace in Microsoft Teams has three components: the Team workspace (including the SharePoint file hosting), which acts as a permissions boundary; channels, which focus and divide attention areas; and tabs, which surface the key artifacts, data, and apps used by team members.

A common question is, “[when do I create a Team versus a channel?](#)” Think of channels as your attention boundary and the Team as your membership (who has access) boundary. More on private channels and how that comes into play later.

Complementary capabilities for Microsoft Teams outside of the Team workspaces include chat (for one-to-one and small group interaction), a consolidated calendar of scheduled events and meetings (which is, yes, connected to your Outlook calendar), and voice calling ... along with bots, apps, and more features literally coming month by month!

Now, let’s explore some of these components.

Team workspace

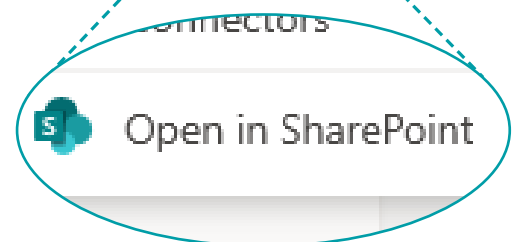
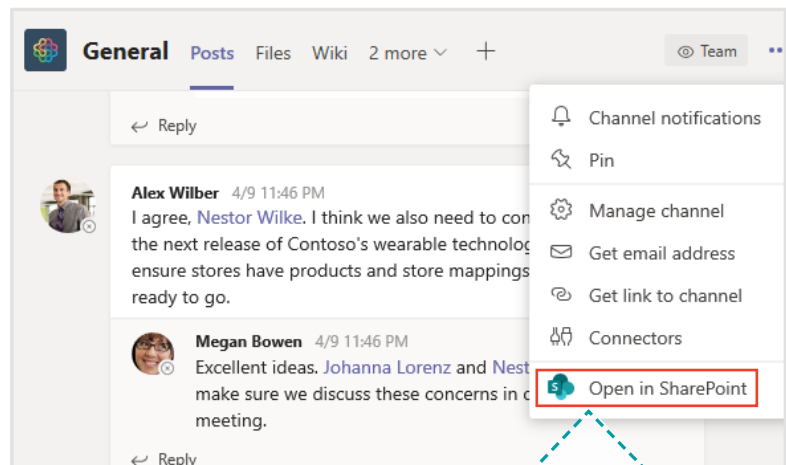
A Team (uppercase) workspace is the basic unit of team (lowercase) and group (lowercase) work, and everyone allowed into the workspace gets access to everything inside the workspace, with the exception of private channels.

Security over access to a workspace is controlled by a Microsoft 365 Group (formerly Office 365 Group)—if you are in the Group (uppercase) you have access and if not, you don’t—unless the Group is open to all within the Microsoft 365 tenant.

Within every Team workspace, channels are used to divide attention areas—such as by topic, by project, by client, by geography, by type, and so on.

And within each channel there are tabs, for enabling conversation within the channel and surfacing relevant resources, systems, information, and documents.

The minimum viable Team workspace has one channel (called General) and two tabs—one for conversations and one for file



sharing. The file sharing tab is actually a SharePoint surfaced within Teams, and the user can navigate to the full SharePoint site interface from that Team.

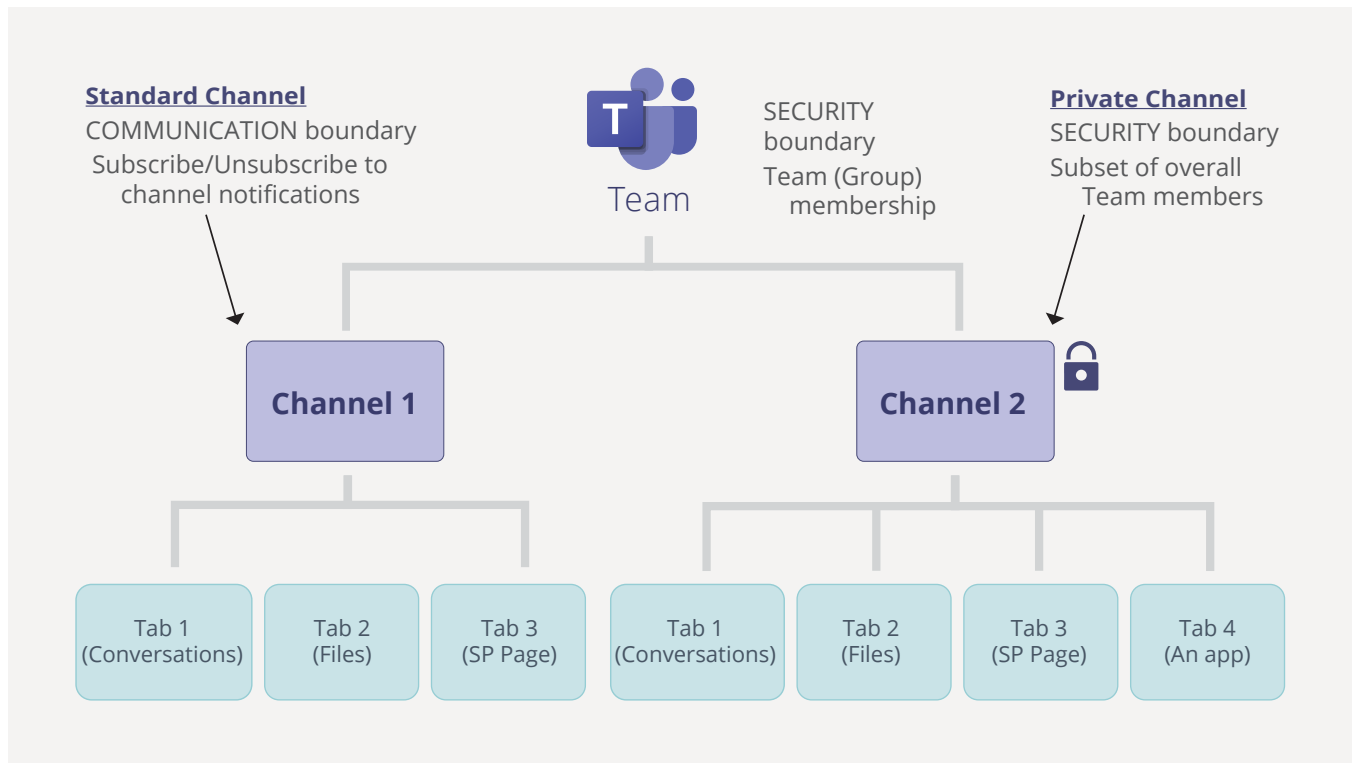
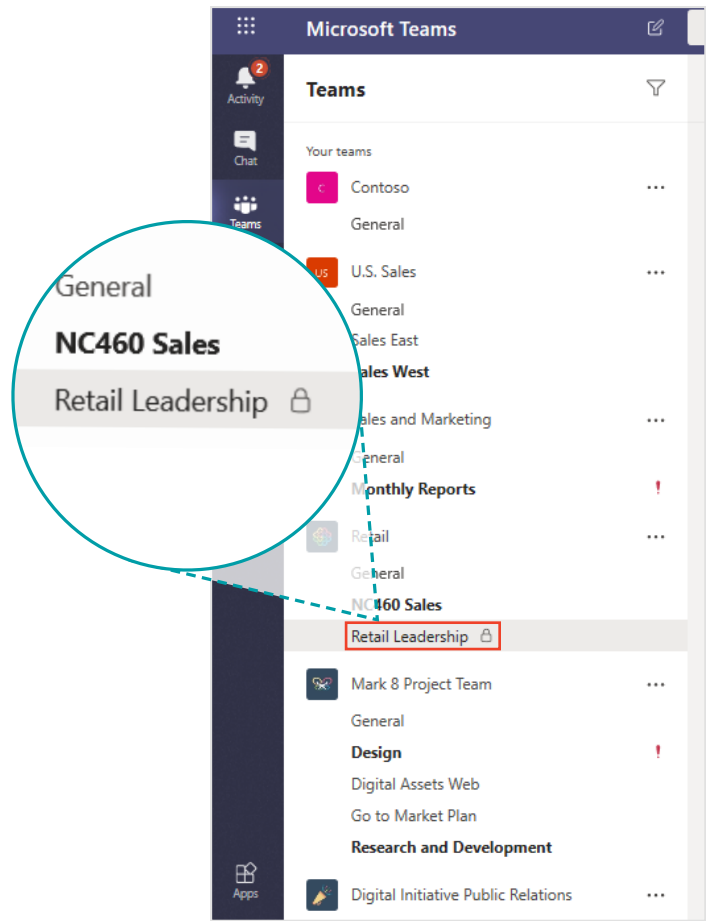
For Team workspaces with multiple channels, each team member can choose which of the channels (attention areas) they want to be notified about.

Private Channels

For the first three years of its existence, access to a Team workspace in Microsoft Teams gave access to all channels and all tabs. But as Teams gained wider adoption across many industries and organizations, private channels became the most requested feature on Microsoft User Voice.

Organizations needed more than merely the soft attention boundaries of a channel within a given team workspace. Channels themselves, thank you very much Microsoft, should also have the ability to enforce a security boundary.

While a separate team workspace could be created for a subset of users, that approach doesn't



always fit the work dynamics of a Team, and over time can lead to fracturing participation across too many Teams.

Microsoft used its annual Ignite conference in November 2019 to release private channels onto the scene, where membership can be defined at both the workspace level and the channel level. Membership for private channels is enabled for a subset of the overall team workspace membership list.

Tabs

While channels segregate attention, as the communication boundary, within a team workspace, the real work is done on the tabs.

Tabs host the conversation, provide access to a list of relevant files, display a Word document or Excel spreadsheet for co-authoring, show a Kanban board from Microsoft Planner or Trello for coordinating current work, and much more.

By design, every channel requires two core tabs for conversation and file access, but beyond those two, there are possibilities galore.

The Conversation tab separates conversations into different streams, automatically structuring the

conversational dynamics into topics, responses and replies, and removing forever the mess of Reply All in email.

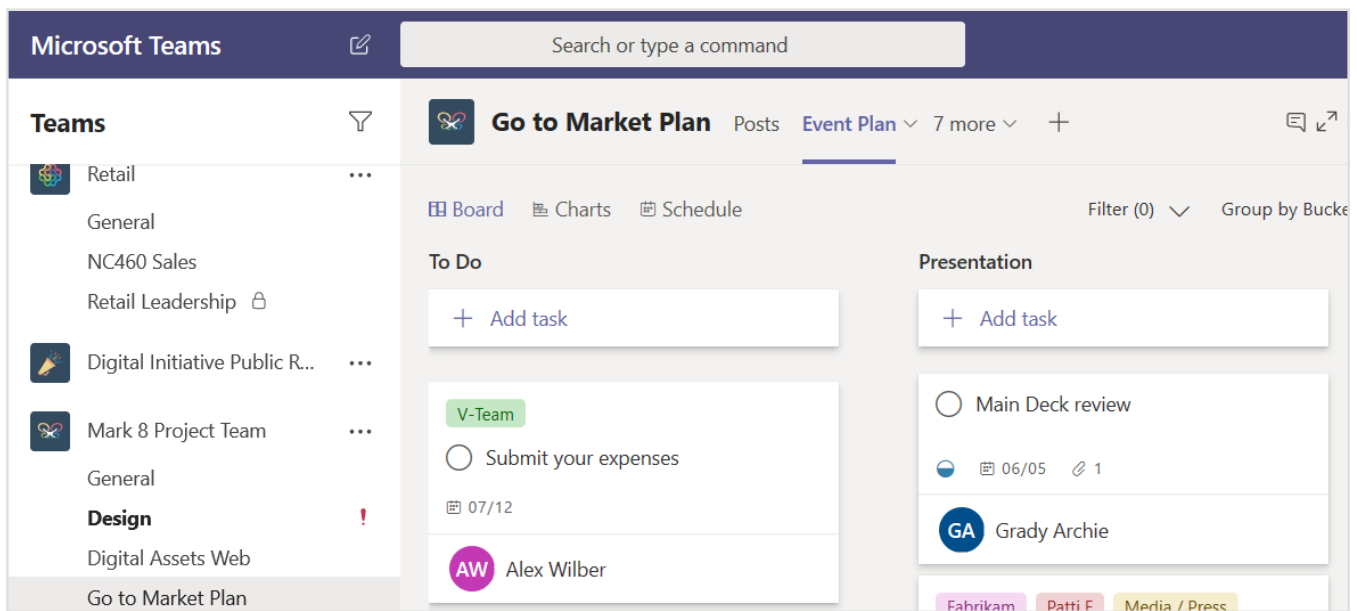
The Files tab stores all of the documents, presentations, spreadsheets and other file types associated with the channel, offering an integrated experience for file sharing (again with SharePoint as the backend).

The ability to display a Word document in a tab provides integrated co-authoring within the team workspace, removing the burden and inefficiency of co-authoring through email attachments.

Third-Party Apps

Microsoft offers a strong collection of tools in Microsoft 365 for productivity and collaboration that can plug into Microsoft Teams. However, Teams was also designed to be as extensible as possible so instead of forcing people to only use Microsoft tools in Microsoft Teams, third-party apps can be integrated into the Teams experience.

People and groups don't have to make a wholesale migration of their tooling to Microsoft 365 as part of embracing Microsoft Teams, but can keep using those that align with their rhythms. With several



You can integrate Planner as a tab in Teams as well.

hundred apps certified to work within Microsoft Teams—such as Trello, Lucidchart Diagrams, Smartsheet, MailChimp and MindMeister—your users don't have to look elsewhere or switch context to another tool, because everything is surfaced within Teams as the center of gravity.

This is critical to adoption and productivity. If the working group can leverage Teams beyond just chat and collaboration, to incorporate its mission-critical day-to-day work, then adoption will be stickier and satisfaction will be higher.

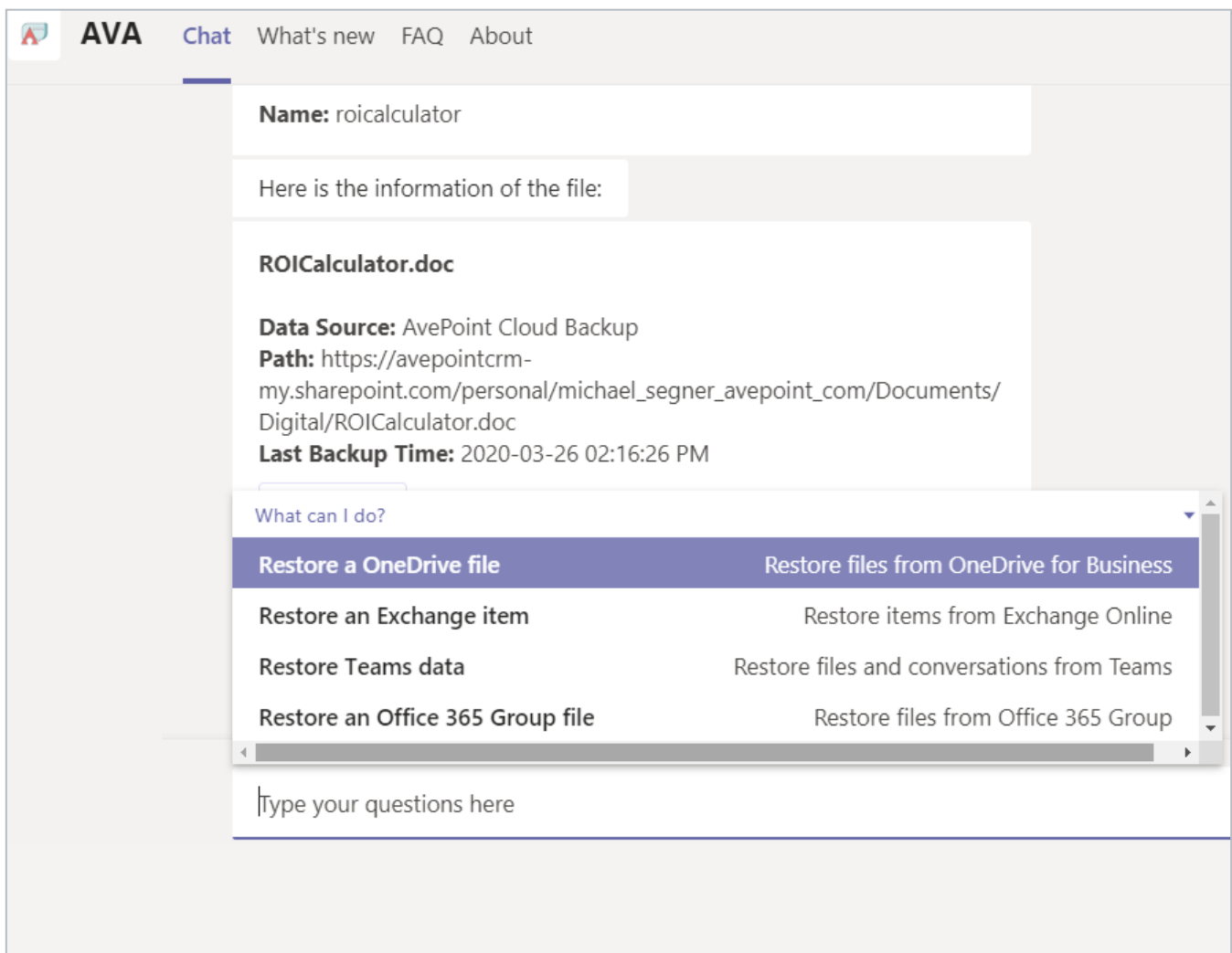
Note: There is a difference between Team apps, which we described above and organizational apps in Teams. Team administrators can download and “push” select apps so that they are pinned to the left-side rail of every users' Teams interface.

Chat and Meetings

Microsoft Teams is a fully-fledged chat, calling and meetings solution as well, taking over where Skype for Business used to play.

Users can hold one-to-one (and one-to-many) private chats with others, using text, voice and video; these chats are private to the participants and sit outside of a team workspace. Meetings with voice calling only, or voice and video, are supported within Teams, along with screen sharing of windows and applications.

There are also options for replacing legacy telephony approaches with Teams, including direct dial into Teams rather than a desk-based phone. AvePoint [has saved \\$400,000 a year by ditching desk-based phones.](#)





Chapter 3: Configuring Teams

As we have discussed, different departments have different requirements in organizational life, and these differences extend to how Microsoft Teams is used. This may affect provisioning, lifecycle, and access policies for how a Team should be used.

For example, while some departments commonly require the ability to collaborate with partners, vendors, and other users outside the corporate tenant in the normal course of day-to-day operations (e.g., vendor management or customer project teams), others require specific permissions or even have restrictions against that type of sharing (e.g., Human Resources or Finance).

Different departments are subject to different policies for configuration settings, some of which are imposed by external compliance regulations while others arise from internal policies designed to drive best practice.

However, the power balance within the native functionality between Team Owners (the administrative role within each specific Team), Microsoft 365 Administrators (across the entire Office 365 tenant), and end users can make achieving and maintaining desired settings and governance levels challenging.

Team Settings Configured By Owners

Each Team creates a primary security boundary separating and differentiating who has access rights to the information within a given team (and yes, as described above, private channels allow for a second level of security by creating a sub-group of users with specific access).

There are two types of memberships in Microsoft Teams (and the Microsoft 365 Group underpinning it): Owners and Members. Each time a Team is created, the person who created it automatically becomes the Owner; they then have the ability assign additional Owners and Members.

A Group Owner has a lot of power and responsibility to configure settings with the Team. By *default*, this includes but is not limited to:

- The ability to add or delete members;
- Grant owner-level permissions to members;

| | |
|---------------------------|--|
| Team Discovery | Make the team searchable and discoverable |
| Member permissions | Enable channel creation, adding apps, and more |
| Guest Permissions | Enable channel creation, adding apps, and more |
| @Mentions | Choose who can use @team and @channel mentions |
| Team code | Share this code so people can join the team directly — you won't get join requests |
| Fun stuff | Allow emoji, memes, GIFs, or stickers |
| Tags | Choose who can add tags |

- Naming and the picture icon of the Team;
- Set the privacy settings for the group (Public or Private);
- Enable guest user settings such as create, update, or delete channels (but not private channels – and only when guest users are enabled at the tenant);
- Add, delete and organize channels and private channels within the Team and determine if members can do the same;
- Add, delete and organize third-party apps within the Team and determine if members can do the same;
- Allow emoji, memes, GIFS and other fun items;
- And even delete the Group (and all data within despite any corporate data retention policies that may be in place);

While the Owner has a lot of power, it is unlikely they have been trained in your organization’s operational governance policies or think like a Microsoft 365 administrator.

For example, an Owner must decide whether to make the Team (and associated Group) public or private, without fully understanding what that means. Or they may not be aware of how private channels work and the impact of enabling them for the Team.

Organizations can turn-off the ability for users to create a Team and centralize this ability within IT (or other set of administrators). However, even if IT provisions all new Teams with the correct settings, there is no enforcement mechanism preventing Team Owners from changing them throughout the life of the workspace.

If the organization chooses to only let IT be Team Owners, you will not only frustrate your users and lose the dynamic nature of what makes Teams so effective, but it will be a tremendous burden to your IT team.

Team Settings Configured By Administrators

The good news is that Microsoft provides a lot of administration roles and tools to help configure Teams. That can also be bad news depending on your perspective, as it can make administering Teams a complex and demanding task.

For example, the way Teams works within your organization can be impacted by settings configured in at least five different admin locations— Azure AD, Microsoft 365 Admin Center, SharePoint Admin Center, OneDrive for Business Admin Center, and the Teams Admin Center. There are 37 different type of admin roles available in the Microsoft 365 Center and four levels of Teams specific administrators, each of which have [different types of access to settings and tools](#).

So while there are a near infinite number of ways for different types of admins to configure Teams, for the purposes of this eBook we will try to keep things simple and use the general term “admin” and cover some of the major settings to consider including:

- Provisioning;

Self-Service Creation of O365 Groups

“What options should I choose?”

- What do you want to call it?
- Why are you creating this group?
- Public? Private?

“Who should I add?”

- Members? Owners? What can they do?
- Who are they going to invite?

- External sharing and guest access;
- Expiration;
- Private channels;
- Naming Conventions; and
- Third-party apps.

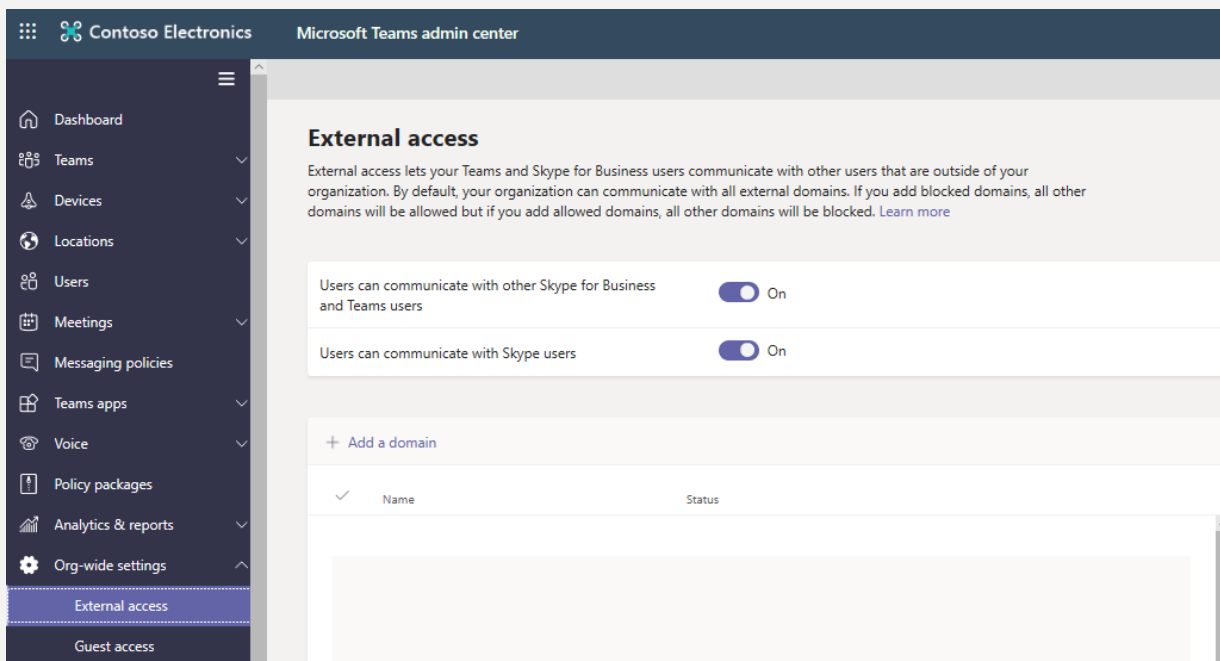
For a deeper dive on the impact of these settings, be sure to read our eBook on [Office 365 and Teams governance](#).

Provisioning: By default, any user can create a Team. Admins [have the ability to create up to five organization-wide Teams](#). Admins can restrict the ability for users to create Teams, but only with AD Premium or EDU license.

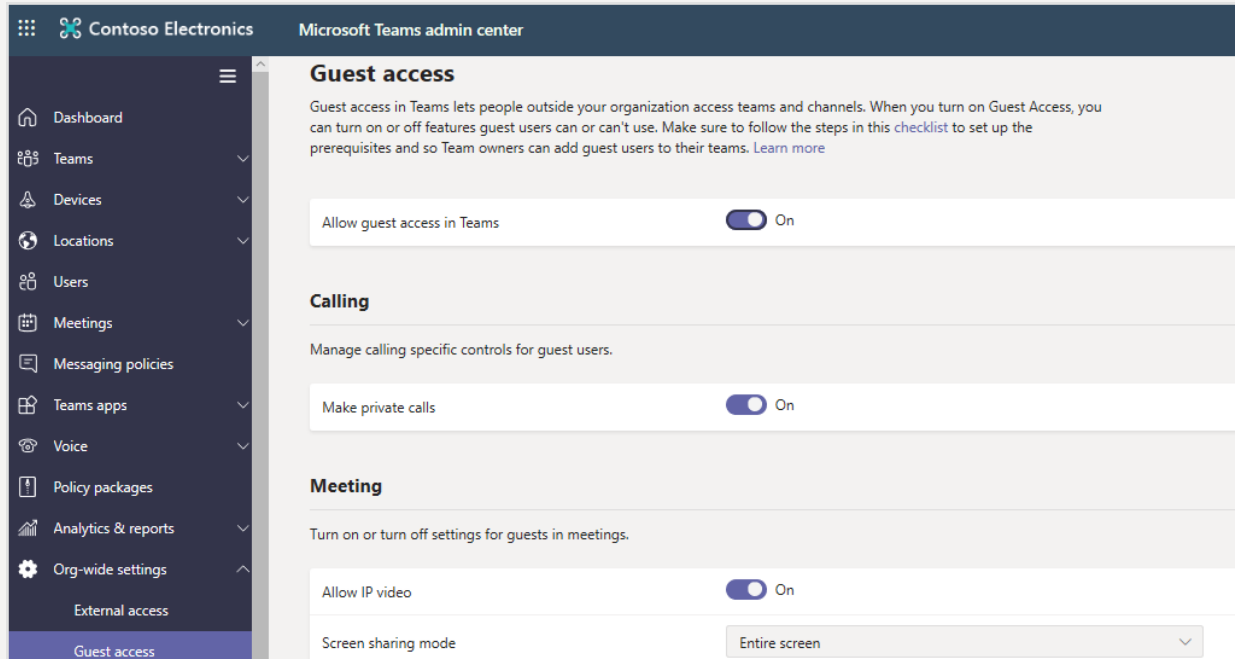
Natively, the only way to restrict users ability to create Teams is to restrict their ability to create Microsoft 365 Groups which also impacts users abilities to create workspaces in: Outlook, SharePoint, Yammer, Microsoft Teams, Microsoft Stream, StaffHub, Planner, and PowerBI.

Not only are you unable to change the provisioning settings for different Microsoft 365 apps or workspaces, you cannot tailor it by department: the provisioning setting is either on or off for the entire tenant.

External Users and Guest Access: It's important to note there is a difference between external users and guest access.



- *External users* can find, call, and chat with users in external domains but are not provided access to Team workspaces, channels, or the content within. It is a tenant level setting and on by default, but admins can turn it off or blacklist/whitelist certain domains. Blacklisting a domain means ALL domains except those may have external access for calls and chats; however, whitelisting a domain will turn off all domains EXCEPT those on the list.



- *Guest access:* Guest access provides access to the workspace components of Teams (really the Microsoft 365 Group) and is a tenant level setting turned on(!) by default. Settings can be modified through appropriate settings in multiple admin centers.

By default, Group members can invite guest users to a Microsoft 365 Group through Outlook on Web. Invitations are sent to the Group owner for approval. Once approved, the guest user is added to the directory and the Group.

Read more about the impact and decisions to make in our blog post on external sharing.

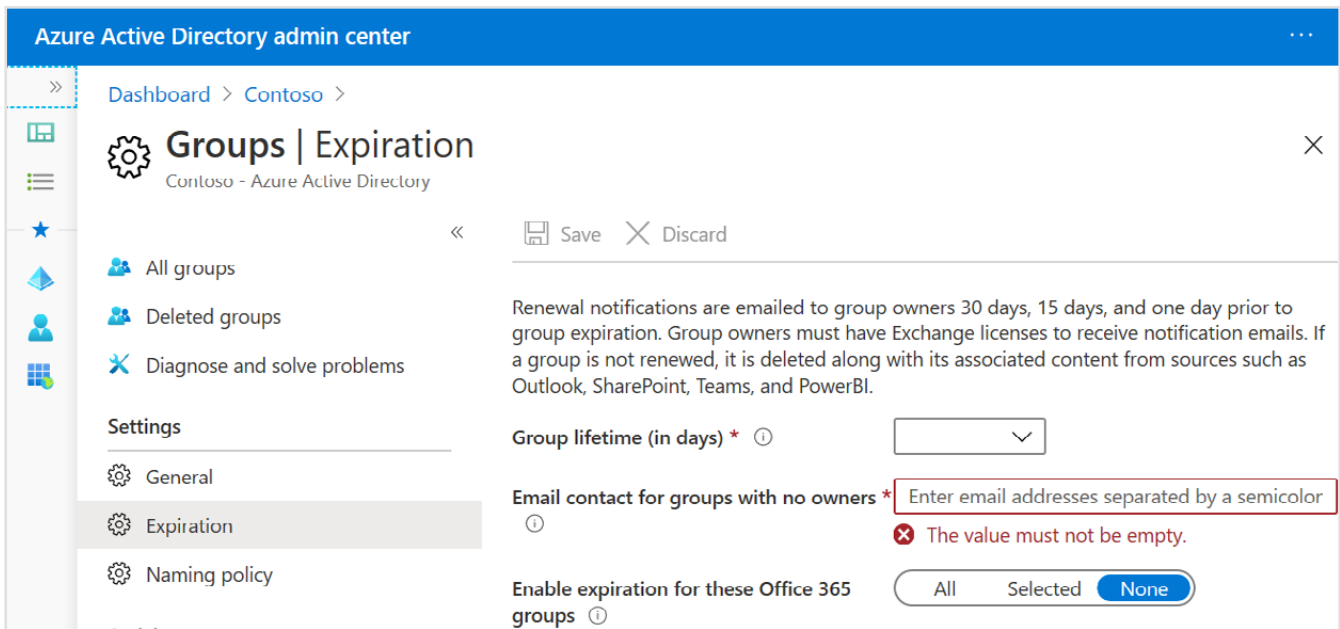
Admins can determine if Team Owners are able to add guests (or if guests can add other guests). Admins are also able to determine if guest users can have access to the Teams' File and Notes tabs through SharePoint Admin Center; if guest users are able to access the third-party applications and tabs within Teams; and how guest users are able to communicate through things like calls and chat.

With guest access turned on in Microsoft Teams, every Team will be able to allow guest users. Team Owner can determine if guest users can create, organize and delete channels (and the content within).

It is possible to have more granular guest access controls for individual Teams, but it can be very time-intensive for your IT team.

📌 SharePoint Online and OneDrive: There is an often-ignored third way to share content within a Team with users outside of your organization, and that is through SharePoint. Although the setting is not directly within the Teams interface, a Team Owner, who is by default automatically the SharePoint site collection owner, can utilize SharePoint's own external sharing capabilities which run independently of Teams.

These settings are configured in the Microsoft 365 Admin Center under SharePoint and allows a loop-hole in sharing — if guest access is off in Teams, but the owner turns it on in the SharePoint site associated with that Team, then all the channel files can be shared with outside users. The tenant-wide setting must be turned on, but once it is, the Owner can determine if it's appropriate Team by Team (and SharePoint site by SharePoint site).



Expiration: Expiration is a tenant level setting managed through Microsoft 365 Groups and is turned off by default.

In Azure Active Directory, admins can specify a time period (must be longer than 30 days) of inactivity, defined as visiting a Team channel, that will trigger a persistent notification in Teams asking the Owner to renew the Team. If the Team is not renewed, it will be soft-deleted, and then fully deleted after 30 days.

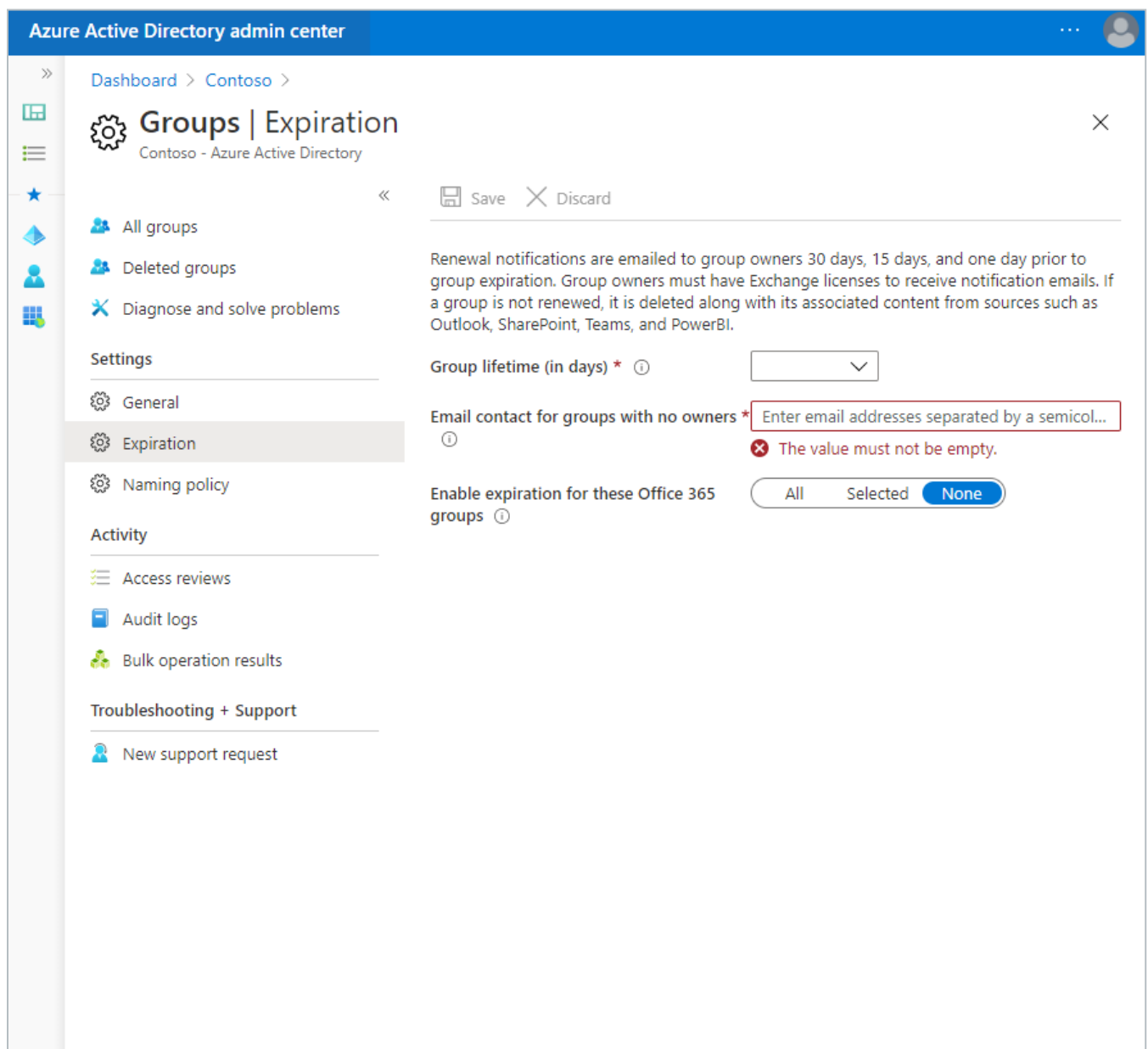
The expiration setting cannot be configured by workspace or by department. It can also be a limiting approach in that it only uses user activity levels to determine the lifecycle of a Team rather than a full re-certification process that ensures Team Owners re-attest the permissions, membership, and associated meta-data of the Team.

It's important to note that a Team Owner can delete a Team, and the content within that Team, at any time. The Team Owner can also choose whether members are able to add or delete channels and the information within. If your organization needs to comply with external or internal data retention regulations, this is a risk that needs to be mitigated.

- **Private Channels:** By default, private channels can be created by Team Owners and Team members, but not guests. They inherit the settings of the parent Team from which they are created. Admins can disable private channel creation organization-wide or enable specific users or workspaces to create Private Channels. If private channel creation is enabled, then Team Owners can determine if the members of their Team can create a Private Channel for that Team.

Naming Conventions: If users are allowed to self-provision Groups, then by default there are few restrictions on their ability to name a new Team. For example, any user could create the Team “IT Help Desk” or “C-Suite Strategy Discussions.”

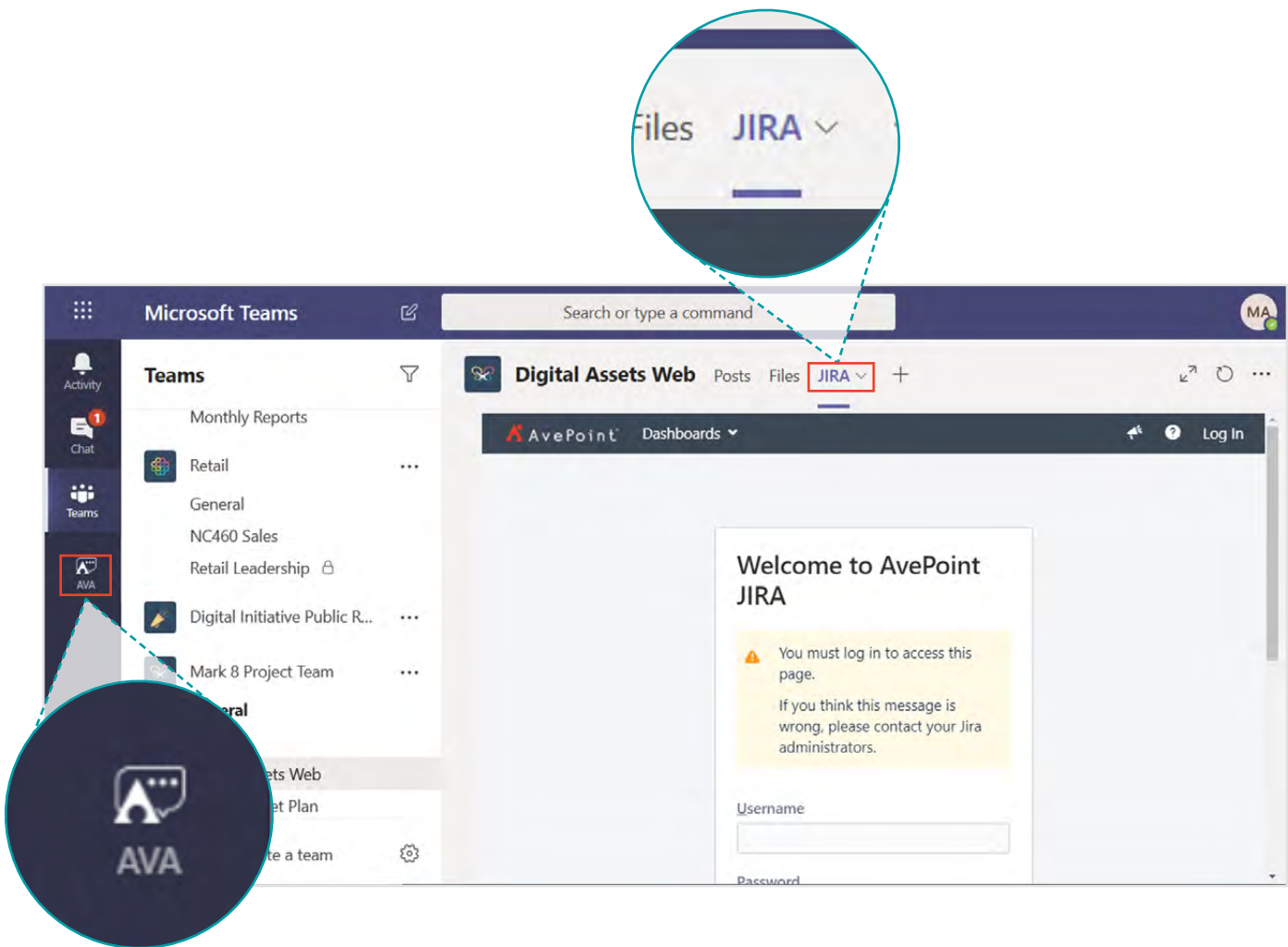
Admins can enforce a naming policy at the tenant level across Microsoft 365 Groups. This approach can block custom words from being used in a name and/or can add either a prefix, suffix (or both) to the name. These policies are applied across the entire Microsoft 365 tenant – meaning that all Teams (and all workspaces within Microsoft 365 that leverage Groups) in the organization are limited to having the same settings applied to them. 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.



Third-Party Applications: All Microsoft apps, third-party apps, and tenant apps are on by default. Team owners can specify whether the members of their team can add or remove apps, tabs, and connectors. Admins can set global policies blocking all apps or they can whitelist/blacklist particular apps as well. Different Teams policies for apps can be created and applied to specific Groups or even users.

As you can see, some key Teams settings can only be configured at the tenant level, while some are dependent on Microsoft 365 Groups and apply across all virtual workspaces and others can be set to specific Teams or even users. Some settings are easily configured in the Teams Admin Center while others have multiple dependencies and interactions across many different interfaces within Microsoft 365 and Azure AD. With Microsoft 365's power and flexibility comes a great challenge in understanding what is happening where. The simple action of externally sharing a document isn't as simple as point and click.

As a result, while Teams is an incredibly extensible and powerful platform that can support many different use cases and ways of working, tailoring it can be a lot of work and in some cases its not even possible. This is where Team cloning and AvePoint's Cloud Governance tool can help.



Third party applications can be a tab in a team or pinned in the left hand sidebar

Chapter 4: Tailoring Teams for Productivity

Teams Cloning: The Copy and Paste of Teams

Microsoft Teams cloning is a native feature that allow users to create new Teams based on existing Teams. This can help your users or IT team replicate the desired “best practice” settings from one Team to others.

Teams cloning transfers the member permission settings configured by the Team Owner as well as the channel, tab and applications of the original Team. However, tabs and connectors need to be reconfigured. A tab (e.g., Planner) will show up in the new Team but it will need to be clicked on, set up, and authorized as new for the Team before it can be used.

Teams cloning *does not* transfer any content including messages and files (which can be easily moved using the SharePoint move feature, if needed). Team cloning also doesn't transfer membership—members must be selected by individual user or Group for the new Team. In addition, any type of policy (ie Team owners cannot create a SharePoint sub-site) cannot be included in a cloned Team. Think of it as simply the “shell” that can be replicated in a new space.

Cloning a Team can be done from Microsoft Teams client or programmatically using Microsoft Graph. [Watch this on-demand webinar](#) to learn how to clone Teams.

Cloning Teams allows organizations to create templates for different use cases and make it easier for users to tailor Teams to their communication needs.

The screenshot displays the Microsoft Teams 'Create your team' interface. At the top, it says 'Create your team' and provides a brief description: 'Collaborate closely with a group of people inside your organization based on project, initiative, or common interest. Watch a quick overview'. Below this are input fields for 'Team name' and 'Description', and a 'Privacy' dropdown menu set to 'Private - Only team owners can add members'. A red arrow points to the link 'Create a team using an existing team as a template'. Below this, a modal window titled 'Which team do you want to use as a template?' is shown, listing several existing teams: 'Solutions NA', 'US-Federal' (which is selected), 'Project_AvePoint Office 365', and 'SharePoint Conference North America'. A second modal window titled 'You are using "US-Federal" as a template for a new team' is also visible, showing the 'Team name' field with 'US-SLED' entered, a 'Description' field, and a section for 'Choose what you'd like to include from the original team'. This section includes checkboxes for 'Channels', 'Tabs', 'Team settings', 'Apps', and 'Members (35 people)', with the first four checked. A note states: 'Messages, files and content won't be copied. You'll need to set up tabs and connectors again.' At the bottom of this modal are 'Cancel' and 'Create' buttons.

However, there are limitations.

- Teams templates for cloning are tenant wide so each department will see every other department's templates.
- Cloning is not enforced.
- Cloning is unable to transfer other key settings that are configured at the Group or tenant level by administrators, which we will cover in the next section.

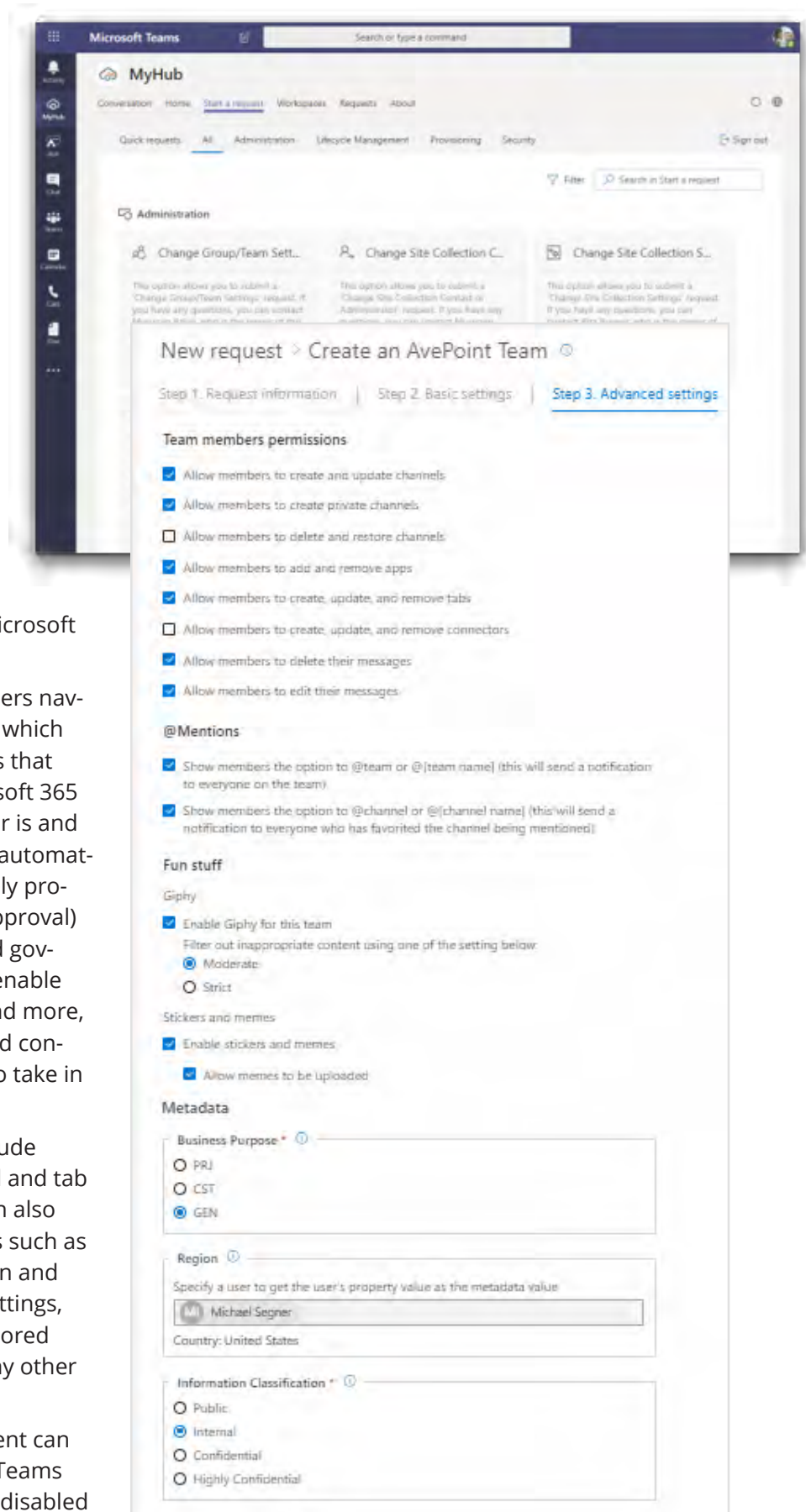
AvePoint Cloud Governance



[AvePoint's Cloud Governance](#) helps organizations find the right balance between collaboration and control in Microsoft Teams.

Service Catalogue: With the solution, users navigate to an organizational app in Teams which presents a tailored catalogue of services that allow the creation of appropriate Microsoft 365 workspaces based on who the requestor is and what they need. The workspace is then automatically configured (and can be immediately provisioned or submitted for conditional approval) using the organization's pre-determined governance policies. The services can also enable changes to settings, content, security and more, providing the organization with balanced controls for almost any action users need to take in Microsoft 365.

Automation: This configuration can include member permissions as well as channel and tab set up similar to Team cloning, but it can also include operational governance settings such as external sharing, provisioning, expiration and more. These operational governance settings, even tenant-level settings(!)—can be tailored by department, Group, workspace or any other identifier in Azure AD.

In other words, the marketing department can be presented with the option to create Teams with external sharing whereas it can be disabled



| Department A | Department B | Department C |
|--|---|---|
| No external sharing | External Sharing In:  | External Sharing In:  |
| Expires After: 6 Months | Expires After: 12 Months | Expires After: 9 Months |
| Team Creation: Central IT | Team Creation: Dept IT | Team Creation: Users |
| Member Recertification: 3 Months | Member Recertification: 6 Months | Member Recertification: 12 Months |

for Teams requested by the legal department. Or perhaps external sharing can be disabled when the requestor indicates the Team will host sensitive data. Another example could be allowing marketing to provision new Teams immediately while the legal department requires approval from IT. Granular controls at the tenant level are limited at best, again excellent for deploying across an entire enterprise, but challenging when specific controls need to be established at an organizational level.

So not only are users getting exactly what they need, but the IT and administrative teams are saved from significant amounts of tedious configuration work across several admin centers.

In addition, Cloud Governance can also control access and configure dozen of settings in Microsoft 365 and Teams so that Team Owners only have access to the settings you want them to control.

Ongoing Governance Controls: Few governance processes are satisfied by a one-time action; most demand ongoing attention to ensure continued compliance. While the steps in such processes are often viewed as mundane, perfect adherence to the design and cadence of the process is critical to ongoing compliance with internal policies and external regulations.

In respect of Microsoft Teams, organizations require the ability to check the initial settings on a workspace are still valid, the workspace is still being used, and once the workspace is no longer needed, that appropriate end-of-life actions are taken.

From the Cloud Governance Service Catalog, Team Owners can re-certify the settings on their workspaces (including purpose, content, and users), secure an extended lease on a workspace when needed, and trigger the deprovisioning process for idle or end-of-life workplaces.

Team admins have a service catalogue of their own, which only gives access to the tasks that administrator can do in Microsoft Teams, scoping out of access the task sets that are irrelevant or inappropriate for a given administrator.

Such focus reduces display noise, eliminates the risk of inappropriate tasks being executed, and simplifies the overall experience of managing Microsoft Teams. The service catalogue also provides centralized management for permissions and configuration tasks, so that administrators don't have to learn to use multiple administrative interfaces.



Step 1: Bob logs into Cloud Governance and requests a new site. Once the request is approved by his manager, the new site is created based on the associated policy that automatically sets the site quota, lease, and retention duration.



Step 2: Through content management services, Bob has folders with documents relevant to the project moved to the new site. He archives the rest.



Step 3: To make sure the right people have access to this new site, Bob receives a recertification to prompt to review permissions.



Step 4: Cloud Governance notifies Bob that the lease for the old site has expired. Since the site is no longer used, Bob chooses to move the site and its content to more cost-effective storage.

Automated Policy Enforcement: Once a workspace has been created—along with the associated Microsoft 365 Group for membership and SharePoint site collection for file sharing—ensuring the correct settings remain enforced is essential.

Cloud Governance can be set up to ensure drift doesn't happen, where Team Owner, Team membership, and SharePoint site settings are changed inadvertently or deliberately away from what these settings should be.

This adds a layer of protection by tracking all changes to membership and SharePoint site settings, and if configured to do so, will automatically revert any out-of-scope changes.



Step 1: For the last two quarters, your employees have been utilizing a collaboration space provisioned by Cloud Governance.



Step 2: Based on your organization's information governance policy, a scheduled permissions recertification event is initialized by Cloud Governance.



Step 3: Bob, the accountable business owner, is assigned a tasks to review and certify that all user permissions within the space are accurate and still relevant.

User: Bill

Permission: Contribute

User: Charles

Permission: Read Only

User: Suzy

Permission: Full Control



Step 4: Cloud Governance assigns the new permissions structure automatically, without having to burden your IT staff.

Tailoring Teams Examples: Legal and Marketing Departments

Let's take a moment to meet two users at Contoso and determine how we could tailor Teams to their needs using native functionality and with AvePoint Cloud Governance.

Robert Smith Jr. Esq., Senior Legal Council:

Let's get to brass tacks. Before I came to Contoso I was billing \$600 an hour and time is money. You asked about how my department needs to collaborate and I'll tell you we handle some of the most sensitive information at the company — security is paramount. We do need to share files with our outside council from time to time but its typically around specific cases that contain important records. Oh, we use Dropbox for that why do you ask? Anyway, we also employ an army of paralegals that turn over quite frequently.



Finn, Associate Social Media Maven:



I'm glad we could take a minute to chat collab strat. Collab is essential to marketing, typically a doc will be touched by 5 or more of us before its donezo. We must move fast, time to market is essential. We use a few key external vendors for our events, but they are like an extension of our family. We like Teams, but its hard to keep track of all of 'em. We spin up a Team for every industry event we support and we have separate parallel Teams on billing which is a drag, you know? Sorry, gotta jet, a killer Tweet just started trending.

Native Approach

Both the marketing and legal departments have reoccurring Teams that are created around events and cases respectively. A member of the IT team could work with both departments to get a better understanding of the types of conversations and tools each department uses and create two Teams templates for cloning optimized for these use cases.

For example, for the marketing events clone you might have member private channel creation enabled and have their SaaS social media scheduler and a master event tracker Excel sheet integrated as tabs. Channels could include event announcements, lead routing, speaker support, and social media.

For the legal department, you might have their SaaS contract management software integrated as a tab with channels on discovery, records, case notes, depositions, and pleadings. For member permissions, you might disable the ability for members to add third-party apps to help mitigate risks around sensitive content and block the use of GIFs, emojis and stickers to keep the tone of conversations aligned with departmental culture.

External sharing would take some hustle. You could set a global Team policy to disable guests from being able to join Teams, while adding the outside legal council to the Microsoft 365 tenant with access to one SharePoint site designed for external collaboration of legal files. You could then create a separate Team policy for the marketing department and apply those workspaces to it.

There would be challenges and compromises made across expiration, recertification, and provisioning—and this doesn't even consider the needs of other departments!

For example, the marketing department wants to declutter their environment and get rid of old Team event sites but setting an activity expiration date would be a disaster for the legal records in the legal case-based Teams. Legal would want a tightly controlled provisioning process with approvals, especially considering the number of paralegals employed, while marketing would want quick self-service.



AvePoint Cloud Governance

With AvePoint Cloud Governance, the same Team cloning process could be leveraged but with an additional layer of custom settings for provisioning, expiration and recertification. Cloning could also be done based on department, project and external access classifications with the appropriate governance policies.

Additionally, the experience for both users and admins would be much more streamlined. A member of the legal department would navigate to the MyHub app in Teams and be presented with tailored workspaces aligned with the organizational

governance policy. A form would ensure that they requested the right type of workspace for their needs and also provide key information for the IT team to monitor and make decisions on this workspace throughout its lifecycle.

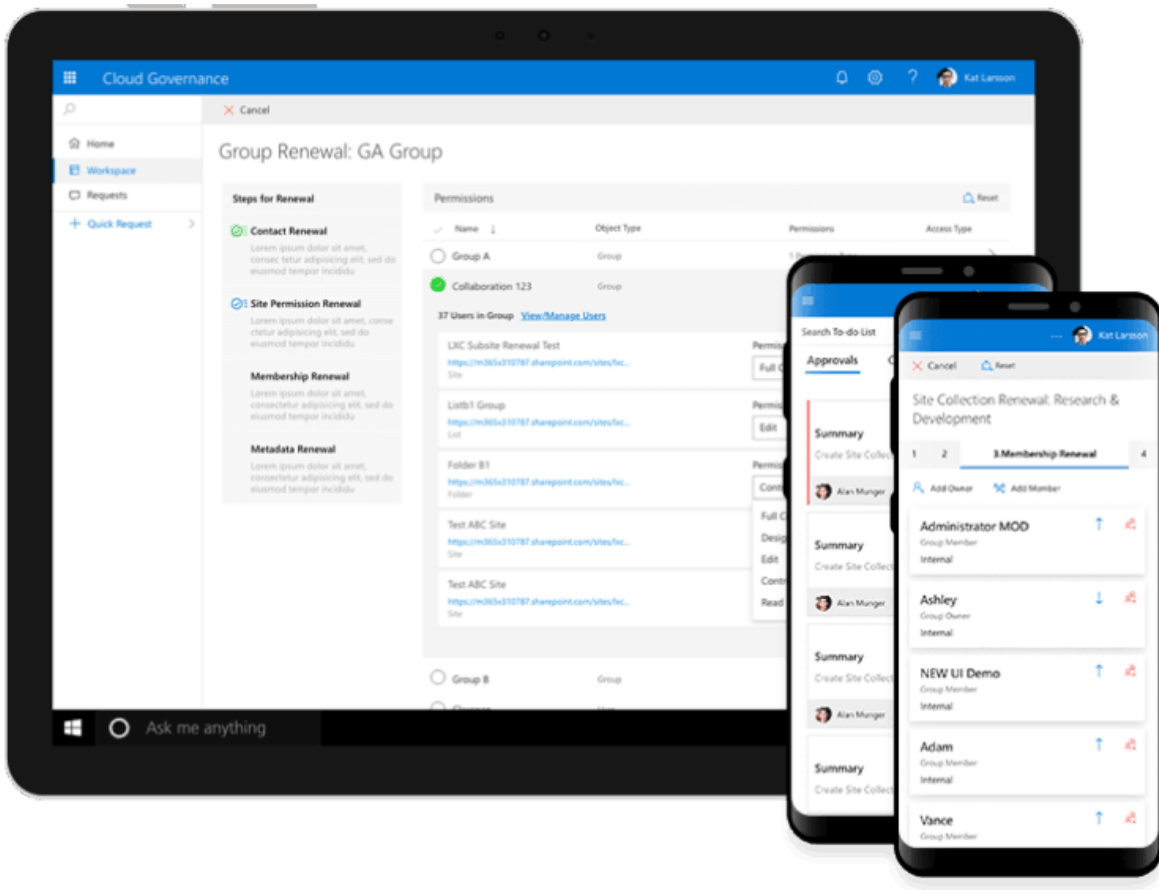
Did you notice the difference in time and energy required from the IT team?


Use of the catalogue by end users offloads the burden from IT administrators for carrying out day-to-day tasks. Business users are empowered to carry out essential tasks, without waiting for overburdened IT staff to complete essential but mundane step-by-step activities. In turn, IT staff are able to focus on higher value tasks aligned with the organization's digital transformation agenda.

Not only would time be saved during the provisioning process, but Cloud Governance would also kick-off a recertification process after the pre-determined amount of time to make it easy for IT to recertify that Teams have the appropriate, membership, content sensitivity and activity levels.

This can add up to a significant amount of time saved for users and admins. In fact, we have created a [web-based calculator](#) that can help you estimate the amount of time and resources saved based on your number of users.

Based on previous experience, we estimate the number of Microsoft 365 workspaces your organization has and the minutes per workspace per year it takes for users and IT to communicate on tasks related to the provisioning, management and end of lifecycle of those workspaces.





Chapter 5: Taking Teams to the Next Level

Optimizing and Delegating Administrator Access

Microsoft's original design for Microsoft 365 of one tenant per organization hit roadblocks fairly quickly, because multi-national and global organizations were unable to embrace this design due to widely different compliance mandates across the world for which a single tenant was unable to deliver.

Recent years have seen Microsoft introducing the new [Multi-Geo option](#) to divide a single global tenant into multiple logical components, and also other innovations to enable a tenant to be divided into smaller groups for eDiscovery (e.g., Compliance

Boundaries) and to meet ethical wall requirements (e.g., Information Barriers for Microsoft Teams).

What hasn't changed, however, is the inability to divide administrator controls below the level of a workload—such as SharePoint Online or Exchange Online—in order to provide delegated administration within the tenant.

For example in the past, an IT manager that may have been charged with just administering SharePoint 2016 for the North American marketing department of Contoso is suddenly given access to the company's entire SharePoint Online environment including its Japanese, German and other divisions; there's no role below SharePoint administrator built into Microsoft 365.

Faced with this issue, organizations leveraging Microsoft 365 typically have two options: 1) Reduce the number of global admins, or 2) Accept the potential risk that comes with giving admins too much power.

Both options have their faults; lowering your admin count means fewer people to manage your data while having competent people on the sidelines, and excessive, unmanaged risk is also unacceptable.

For organizations that deal with sensitive information or deal with ITAR or similar stringent regulations, the second path may not even be an option.

AvePoint's delegated administration capabilities in Cloud Management for Microsoft 365 provides the answer, and as with users, makes it easy for administrators to do the right thing.

Imagine being able to take your central Microsoft 365 tenant and carve it up into separate, more

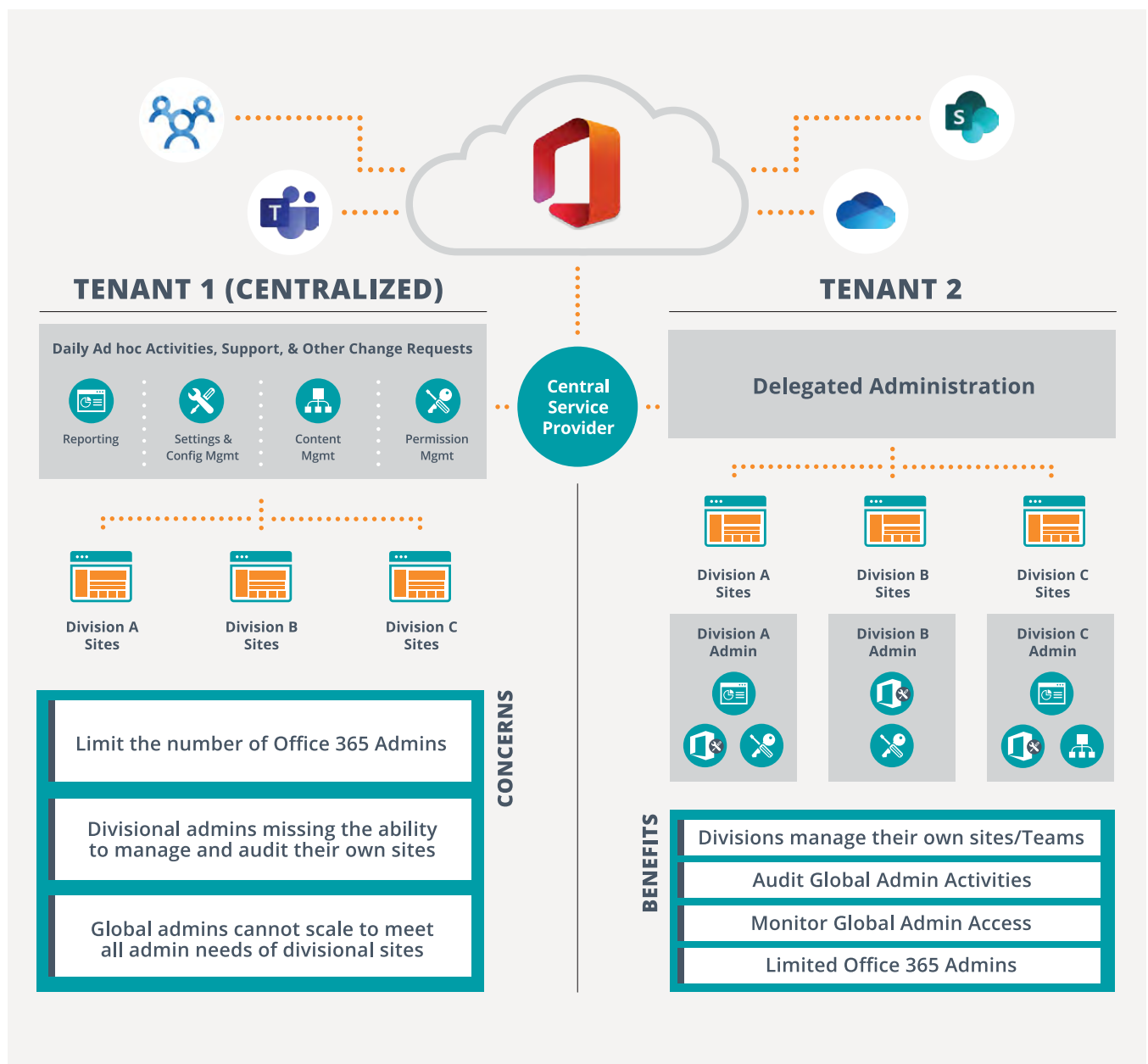


manageable containers that can be administered at the division level without giving up access to the entire tenant. It provides the structure and security of isolated tenants but still allows you to leverage Microsoft 365's collaboration capabilities to the fullest.

This can be extremely helpful for government agencies or large organizations who can now allow IT users closer to the business or mission to help with permissions management, content management, and reporting for their division.

So for example, while the state government of California may be under a single Microsoft 365 tenant, they could then create Microsoft 365 admins in the Department of Transportation who just have access to those workspaces and data.

Objects such as mailboxes, OneDrive repositories, Microsoft 365 Groups and more can be divided into separate logical groupings, based on properties or combinations of properties. For example, all objects with the departmental property of "sales" and the geography property of "United States" can be



automatically allocated to a “US Sales” container, to which an IT administrator can be assigned.

He or she can carry out the administrative tasks for all objects in the container, but not for any objects outside of the container.

Alternatively, all Exchange mailboxes with a custom property of “executive” can be assigned to an “Executives” container, and only the assigned administrator is able to provide administrative support to the executives of the organization.

This prevents just any administrator with the Exchange Administrator role in Microsoft 365—which gives access to all mailboxes by design—from accessing the mailboxes of executives which will contain sensitive, confidential and secret business information.

Information Management In Teams

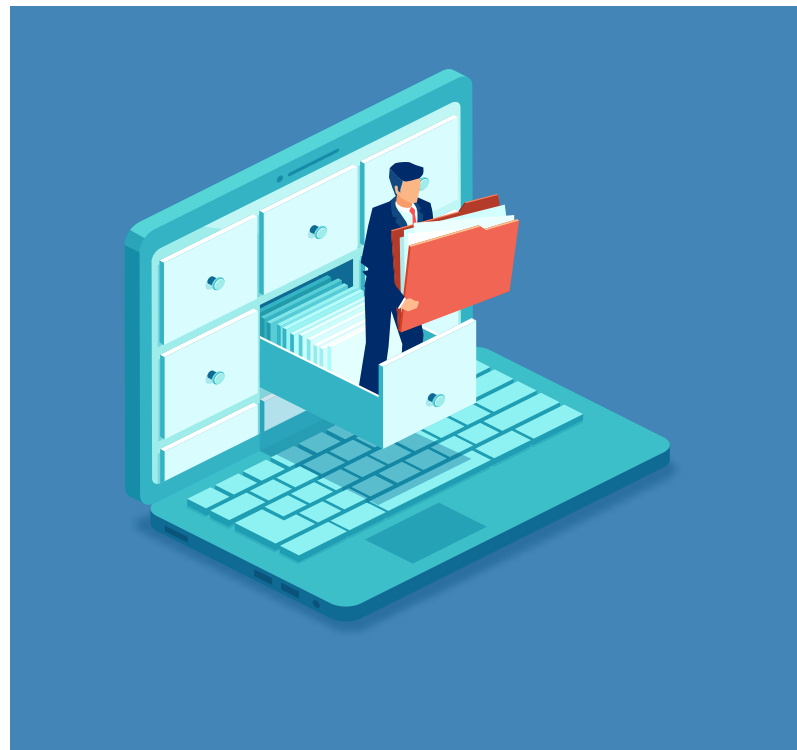
Optimizing the use of Microsoft Teams in your organization includes having capabilities to address information management responsibilities, such as backup, records retention, and access to sensitive data stored in workspaces.

AvePoint’s solutions support best practice information management approaches and delegated administration, for optimization across the lifecycle of Teams usage.

Creating and Accessing Backups

Backups are an essential part of a disaster recovery scenario, but also have less dramatic uses in recovering a lost email, document or other digital artifact. Once created, however, backups need to be secured just as relentlessly as live data, to ensure backup data is not changed, compromised in a data breach, or accessed by unauthorized people.

AvePoint Cloud Governance helps in two ways: default backup settings, and backup scopes. Default backup settings can be included in the definition of each clone used by different departments, so that new workspaces are automatically added to backup processes.



In terms of backup scopes, these reduce the risk surface in creating and accessing backups through automated controls over which administrators can backup certain mailboxes, Microsoft 365 Groups, and Teams workspaces.

For example, because the spaces used by executives are likely to contain highly confidential and secret business data, a special backup scope can prevent anyone other than nominated administrators from creating and accessing backup data for these executive objects in Microsoft 365.

Assuring Backup Completeness

Microsoft 365 is a complex set of interconnected services, meaning that the backup task for Microsoft Teams is much greater than any single workload. As the hub for teamwork in Microsoft 365, Teams by design stores data in SharePoint sites (the newly-introduced Private Channels makes this task even more complex, due to the introduction of a separate SharePoint site collection for each private channel), a group mailbox in Exchange Online, Planner and more, not to mention the channel and chat data created in Microsoft Teams itself.

Being able to backup everything related to a Teams workspace is essential, as is being able to restore

individual items to the right place when required. [AvePoint's Cloud Backup](#) is the only solution available today that can backup and restore channel conversations in a Teams workspace.

Records

While no two teams, projects or communities of interest and practice are exactly the same, each type shares common attributes and characteristics.

Dividing new workspaces into the appropriate type enables the specification of default labels on the data created in the workplace, which then triggers automated lifecycle processes for retention and deletion that are aligned with the different types.

For example, a team space for the Finance team will have different records requirements than a project space for the end-of-year Christmas Party, and while Microsoft Teams can be used for both, different records requirements will be in place. [AvePoint Records](#) can be used to enhance the records management process in Microsoft 365.

Sensitive Data

The questionnaire used for requesting a new workspace can include prompts around types of sensitive data that are likely to be included in the workspace.

Pre-declaration of inclusion intent enables the appropriate tagging to be configured for controlling sensitive data, offering automated classification rather than relying on end users to correctly classify each item separately.

Complementary AvePoint tools—such as [Compliance Guardian](#)—can also be used to scan for sensitive data- inside content- across all workspaces, ensuring that non-declared sensitive data is quickly identified and appropriately protected.

In addition, scoped access for delegated administration over objects such as Teams workspaces reduces the risk that administrators will inadvertently access sensitive data they should not see.

An Exciting Time

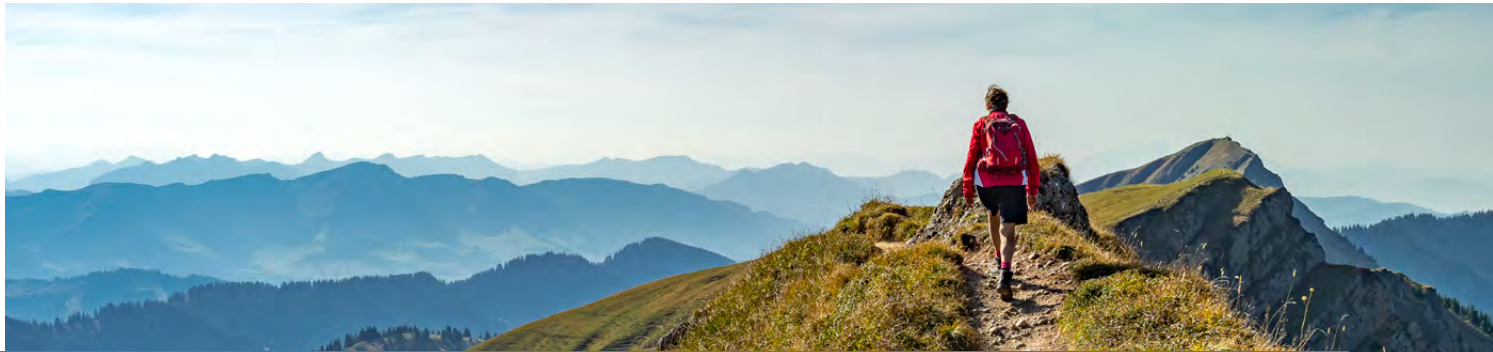
It is an exciting time for teams and organizations with the emergence of Microsoft Teams as an innovative way to support and enable the new culture of teamwork. While the early usage trajectory has been impressive, there's much more to come, as long as organizations have the ability to optimize and tailor Teams for the real-world requirements they face.

While Microsoft's tools in Microsoft 365 offer good access and security controls, these can be extended for larger organizations or those with sophisticated internal or external requirements. Creating appropriate scopes of control—for users, departments and IT administrators—is essential to seeing ongoing value from Microsoft Teams.





Chapter 6: Case Studies



Customer Profile:

Intrepid Travel

Founded by two bearded backpackers, a typewriter and a kitchen table, Intrepid Travel eventually grew into the world's largest small-group adventure tour company. With more than 2,300 staff and leaders based around the world and over 1,000 different trips across every continent, they seek to provide responsible travel and very big adventures.

The Challenge

For an international travel agency headquartered in Melbourne, Australia, moving to the cloud meant the ability to reduce latency, foster more collaboration, and scale with growth.

Originally adopting Office 365 for Outlook Online and Skype for Business, Intrepid Travel quickly began to adopt SharePoint Online and Microsoft Teams. When Intrepid decided to roll out Microsoft Teams across their organization, the rapid rate of adoption was a surprise.

“We never forced anyone in the organization to adopt or use Teams, we just turned it on and quietly migrated over from Skype. One employee would talk to another who was using Teams – and before we knew it, the majority of our employees were already on it,” explained Gavan Meyer, SharePoint Architect, Intrepid Travel.

Three specific challenges arose as quickly as the adoption rate.

“Sprawl, lack of consistency, and security issues,” said Meyer. “Anyone can create a SharePoint site and a Teams site. Being in many different countries, each office functions differently in their own way.”

Workspace duplication and ongoing permissions management were particularly tricky issues to navigate.

“Usually it was just simple naming inconsistencies that lead to multiple Teams named almost exactly the same,” said Meyer. “On top of that, when people didn’t understand internal security, they would either give everybody access, or nobody.”

The AvePoint Solution

Intrepid did their due diligence by researching other available solutions in the market before investing in AvePoint.

“We dug through the market and did all of our research. We ended up sticking with AvePoint because your solution made sense and worked,” explained Meyer. “It was a good experience and didn’t make my head hurt. We don’t have time for a complicated solution.”

Using Cloud Governance for the provisioning of Microsoft Teams, Office 365 Groups, and SharePoint Online, Intrepid is fostering sustainable collaboration and adoption.

“We’re [managing] sprawl by requiring fields during the provisioning [process] like; business, department, and location. We also get notifications for which sites haven’t been used in a while,” said Meyer.

Cloud Governance enhanced the Intrepid IT team’s control over naming and ownership, which enhanced consistency across their environment.

“With Cloud Governance, we have consistency because of the questionnaire that people have to complete before requesting a site or Team. This allowed us to give our users guidance and direction,” said Meyer.

When considering the security of their Office 365 environment, Intrepid found it paramount that they maintain control and accurate ownership.

“It sets the owners and administrators by default, giving us a single account to manage everything, and also giving us notifications when the sites run out of space,” explained Meyer.

The Bottom Line

AvePoint’s Cloud Governance has already shown a tangible value to Intrepid’s IT team, reducing their burden.

“It’s definitely a time-saver. Last month we created 58 new sites in SharePoint. On average, that would’ve taken about 40 hours of IT hassle. This doesn’t even include training the service desk,” said Meyer. “So overall, Cloud Governance is saving us about 3 months of work each year. On top of that, we got control over our environment.”

Overall, Intrepid is very satisfied with the performance of Cloud Governance.

“In over two years, I haven’t logged more than two calls with your Technical Support. The tool was easy to understand, it worked well, and it’s easy. It’s literally that simple,” said Meyer.



Customer Profile:

Prudential Financial

United States, Asia, Europe, and Latin America, Prudential Financial provides customers with a variety of products and services, including life insurance, annuities, retirement-related services, mutual funds and investment management.

As a Fortune Global 500 company, Prudential has experienced extensive growth since their arrival in Microsoft 365 in 2017. They maintain about 63,000 Microsoft 365 seats with five terabytes of data in their SharePoint Online environment and 17 terabytes in OneDrive for Business.

The Challenge

Before executing their migration to Microsoft 365, Prudential's on-premises environment – approximately 400 sites collections – was quickly becoming unmanageable. Once in the cloud, the sprawl of their environment accelerated and began to impede adoption of Microsoft 365.

"We were receiving at least 25 Teams and about 10 SharePoint Online site requests every week, which quickly resulted in a lot of work for our IT team," said Robert Young, IT Engineer at Prudential.

As a result, Prudential began a very comprehensive and deliberate search for a governance solution to help control workspace provisioning and assist with reporting.

"We tried about four other companies with a whole proof of concept and analysis. AvePoint just simply made more sense," said Young. "We knew we needed help with multiple things – reporting, governance, management, etc. – and AvePoint was the only provider to really cover it all."

The AvePoint Solution

Cloud Governance can automate almost any policy or procedure in an Microsoft 365 environment, like Microsoft Teams, by guiding the Group creation process through a self-serving form-based website.

"Every new team or SharePoint site is managed by Cloud Governance. When someone needs help from my team, we now have a ticketing system. Now they simply fill out a form, and the provisioning system will control the creation and approval for us," said Young.

Cloud Governance has the functionality to automatically enforce critical governance components of a team or site such as naming conventions, lifecycle,

permissions, ownership and much more.

Prudential has started with a simple implementation of Cloud Governance to realize immediate value, but is planning to leverage the tool further to enforce more granular governance policies.

"We haven't gotten too complex, but definitely plan on it. Right now, all our sites have been deemed internal with no PII (personally identifiable information) or sensitive information... We are planning on looking into different policies based on the level of sensitivity," said Young. "Currently, we have a single team provisioning process. Everyone can request the same team with a 50-gigabyte limit. However, we have set it up on the back end to automatically be approved for directors and above."

Additionally, Prudential is planning on leveraging Cloud Governance to securely enable external collaboration.



"We will also be opening external sites to collaborate with vendors on work, which will need heavy management. We currently block all users from adding any external users to anything. They have to come through IT and management directly," said Young.

Prudential has also decided to force and create a sense of ownership for sites and teams through automating a renewal policy.

Young explains, "We set up Cloud Governance policies to put a renewal profile against sites and teams. We are getting more requests asking which sites belong to which users. This policy and easy reporting have helped us understand and create ownership."

Prudential's North American tenant has been so successful with Cloud Governance, the company plans to integrate it globally.

"Our Japanese tenant is a completely different entity. They are rolling everything out in Microsoft 365, but will also be using Cloud Governance by following our North American strategy," said Young.

The Bottom Line

Since Prudential's implementation of Cloud Governance, they have been able to quickly adopt Microsoft Teams and save IT management time.

"Cloud Governance has definitely given us more confidence... it has made us comfortable rolling out Teams and it actually happened very quickly," said Young. "Technical Support has also been really great. We get great customer services and are constantly shown status updates."



Customer Profile:

Cambridge Consultants

Cambridge Consultants is a global product development and technology consultancy firm with a headquarters in the UK providing outsourced research and development services.

Cambridge has 900 employees in seven offices around the world. The company has been around for over 60 years and tackles an average of more than 400 projects each year. Their engineers, designers, scientists, and consultants work on projects that contain sensitive information, and access to the project data is on a strict need-to-know basis.

The Challenge

During the adoption process of Microsoft Teams, Cambridge Consultants were looking for a governance tool to sync membership with Active Directory Security Groups and enforce consistent access across all their systems.

“For many years we have had a custom solution that allows our project managers to update Active Directory security groups with authorized project team members,” explained Julie Peck, enterprise applications architect at Cambridge Consultants. “The security groups are then used by all of our applications that store project data. It was really important to us that Teams followed the same model.”

To ensure strong end-user adoption, Cambridge Consultants wanted to enable users to self-create Teams while also controlling risks to sprawl, and unauthorized access to content.

Cambridge Consultants also sought tools to monitor their employee’s usage of the application, ensure Teams are compliant and the employee access was valid.

Governing the full information lifecycle and determining when data is no longer in use and should be disposed was also a key criteria.

The AvePoint Solution

At Cambridge Consultants, all current Microsoft Team’s team creation requests go through their IT Department.

The department then separates the teams requests into two different types, Project and Public.

For Public Teams, there is only one configuration. For Project Teams, they are further separated depending on if they are client-facing or internal.

For the different types of Teams, the IT Department will send a corresponding form for the user to fill

out for their Team to be provisioned and configured according to the company's governance policy.

"When filling out the form to request a Team the user can name a primary or secondary contact for the Team and also create a name with the enforced naming conventions for Project Teams," explained Joel Sutherland, IT applications analyst at Cambridge Consultants.

As the organization continues with its Teams deployment, they plan to allow users to fill out their own Teams creation questionnaire via SharePoint.

Cambridge Consultants also has services set up to edit Microsoft 365 Group names, change Group details, and remove users from a Group.

"AvePoint's Cloud Governance allows you to specify your Microsoft 365 Groups for Team membership, which has been quite useful for us," said Sutherland.

Guided self-provisioning is enabled for SharePoint sites at Cambridge Consultants.

Users complete a questionnaire from the Workspace Catalogue on the company's SharePoint site. After the questionnaire is filled out it is sent to the user's manager for approval.

Once approved the request is automatically sent into the workflow to create the Group with the proper configuration. The user then gets an email to let them know their space is now available.

The Bottom Line

Cambridge Consultants is very pleased with the adoption and success of Teams. Of their 900 employees, there are 851 active users of Teams. In 28 days, there were over 12,000 Teams channel messages and 121,316 chat messages.

They were also pleased with the amount of control they had over Teams creation. "Using AvePoint Cloud Governance, we were able to avoid any initial sprawl and monitor the appropriateness of Teams," stated Sutherland.



Chapter 5

Additional 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](#)





525 Washington Blvd, Ste 1400 | Jersey City, NJ 07310

P: +1.201.793.1111 | E: sales@avepoint.com | www.avepoint.com