



Securing Microsoft Teams

4 Tactics For Regulated Organizations



Microsoft
Partner



Gold Application Development
Gold Collaboration and Content
Gold Cloud Productivity
Gold Messaging
Gold Datacenter

Accessible content is available upon request.



Stephanie Donahue

Owner, PAIT Group

 @stephkdonahue

With over 20 years of experience in IT, Stephanie is a leader, an innovator, and skilled problem solver. She has a passion for technology and innovation that led her to co-found the PAIT Group.

Stephanie is also an active Microsoft RD & MVP, engaged in the community across the country where she speaks, writes, and podcasts (@Techsplaining).

Microsoft
Regional Director



John "Jay" Leask, PMP

Principal Solution Engineer

 @jayleask

Jay uses 20 years of IT experience to engage customers in designing digital collaboration solutions to increase efficiency of mission workers within their Microsoft investments.

Jay is also founder of the *On the Spot Network* with podcasts such as *This Week in Teams* and *Buzzkill* – where he not only discusses the technology but helps IT develop strategies to modernize IT with a focus on user experience and business/mission strategy.



The M365 Challenge for Regulated Industry and Government

TRADITIONAL DIVISIONAL FARMS



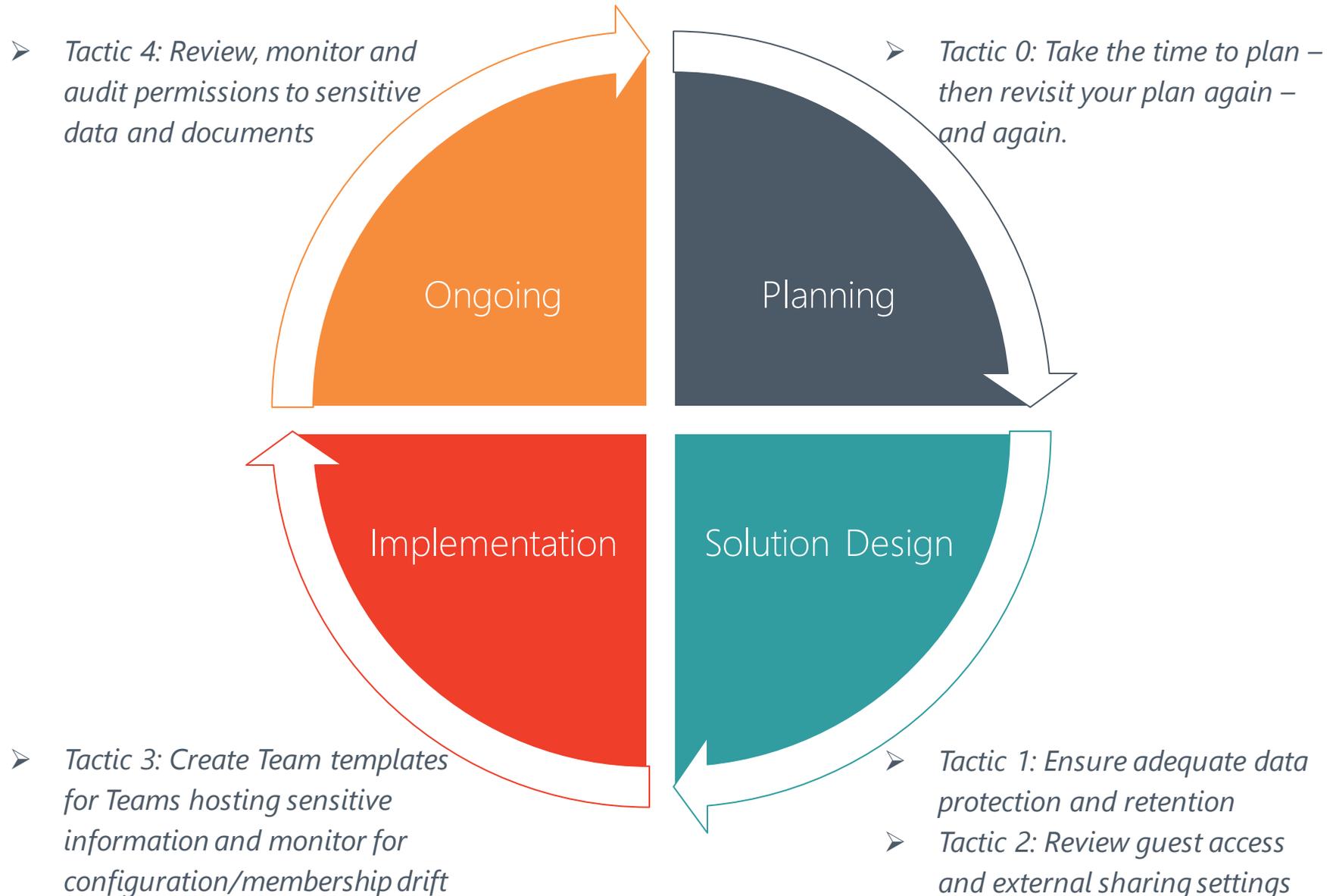
Regulated Industry M365 Adoption Blockers

Provisioning	How do you ensure Teams with specific criteria follow specific approval processes?
	Should a business owner have elevated privileges? Should we enforce multiple owners?
	Can we limit membership based on contract, citizenship, etc?
Ongoing management	How do we report ownership, purpose, sensitivity?
	How do we limit invitation of external users to a subset of users?
	What Teams belong to what divisions?
	We need to restrict and approve changes that effect policy such as security classification, ownership, etc.

Lifecycle	Require periodic review of permissions, membership, ownership etc.?
	What is the escalation process for orphan Teams? Lack of response? Inactivity?
	Can we enforce an approval process for deletions? Archive? Restoration?
	How do we restore something if the business purpose becomes relevant again?
Content Compliance	Process to assess ongoing business relevance?
	Content level classification and controls
	Retention/expiration and records declaration
	How do we identify sensitive data based on risk of exposure?

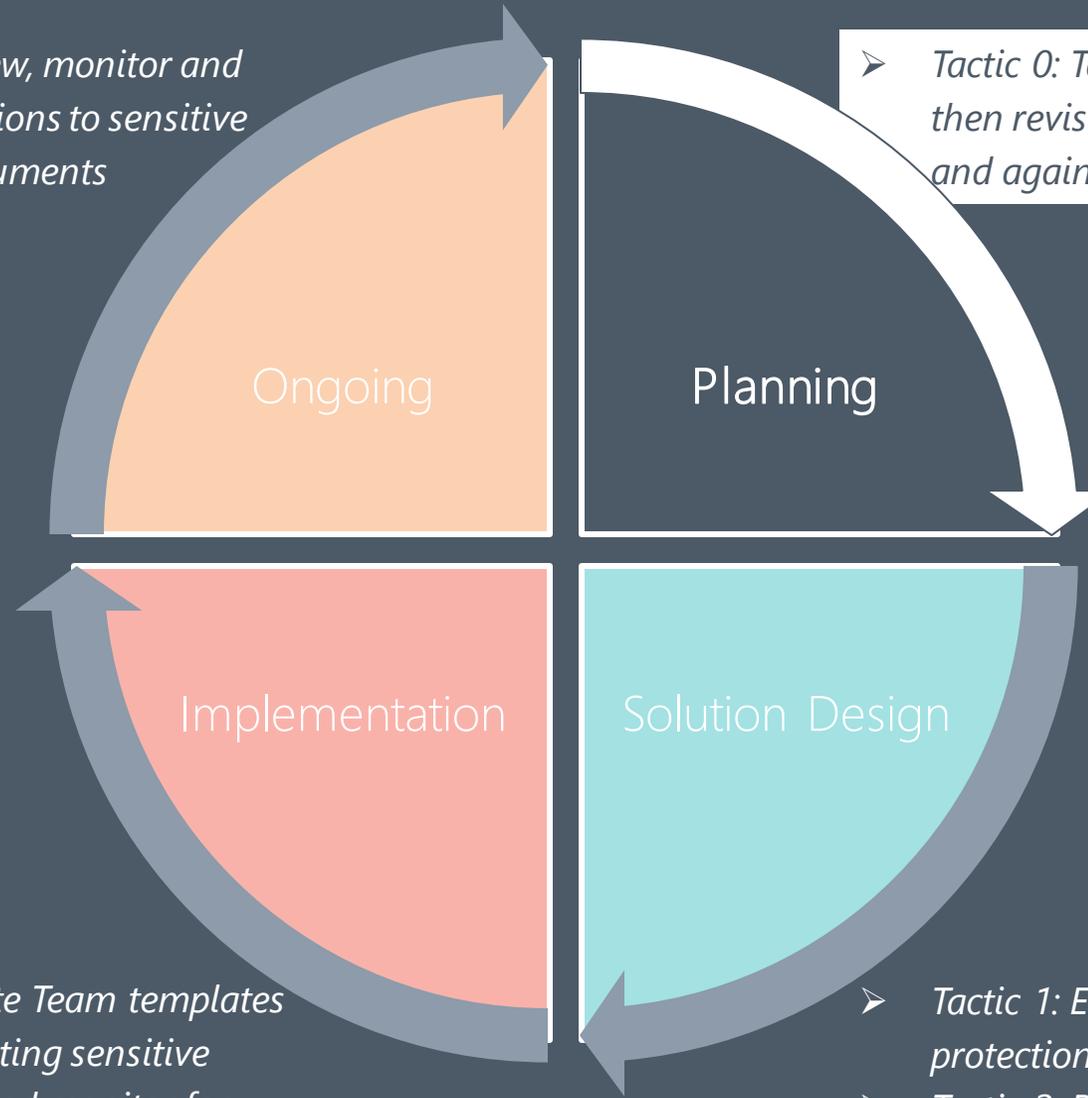
Resolving the Challenge

Native controls are designed for ease of collaboration, but regulated industries and government agencies and government must consider more security due to HIPAA, GDPR, state regulations, and more



- *Tactic 4: Review, monitor and audit permissions to sensitive data and documents*

- *Tactic 0: Take the time to plan – then revisit your plan again – and again.*



- *Tactic 3: Create Team templates for Teams hosting sensitive information and monitor for configuration/membership drift*

- *Tactic 1: Ensure adequate data protection and retention*
- *Tactic 2: Review guest access and external sharing settings*

Tactic 0: Take the time to plan – then revisit your plan again – and again.

Planning Round 1



- **Content:**
 - What goes into OneDrive vs SharePoint vs Teams
 - How do we split our content out across Teams – may be department driven at first
- **Security:**
 - Who needs access to that content?
 - Do we allow Guest Access?
- **Governance:**
 - Just create teams as requested
 - No archiving or Teams deletion
- **Apps and tools:**
 - No third-party integrations
- **Theme:**
 - Keep it locked down to control sprawl

Planning Round 2

- **Content:**
 - Migrate sensitive data like HR, R&D
- **Governance & Security:**
 - What additional layers of protection are needed?
 - Prevent print
 - Prevent external sharing
- **Retention:**
 - Archiving unused Teams
 - Archive vs Delete
- **Apps and Tools:**
 - Third-party integrations for critical business systems
 - Allow access to approved third-party apps
- **Theme:**
 - Continue to scale the environment and take advantage of more 365 features, without compromising security needs



Plan *with* the business, not *for* the business



Understand your collab scenarios

- What opportunities are there?
- What functional groups or departments are most likely to pick this up quickly ?
- Who should we wait on? (busy seasons, more complicated scenarios)
- ENGAGE the business in conversation

Governance Decision Points



Does your organization require a specific naming convention for teams?



Do you need to restrict the ability to add guests to teams on a per-team basis?

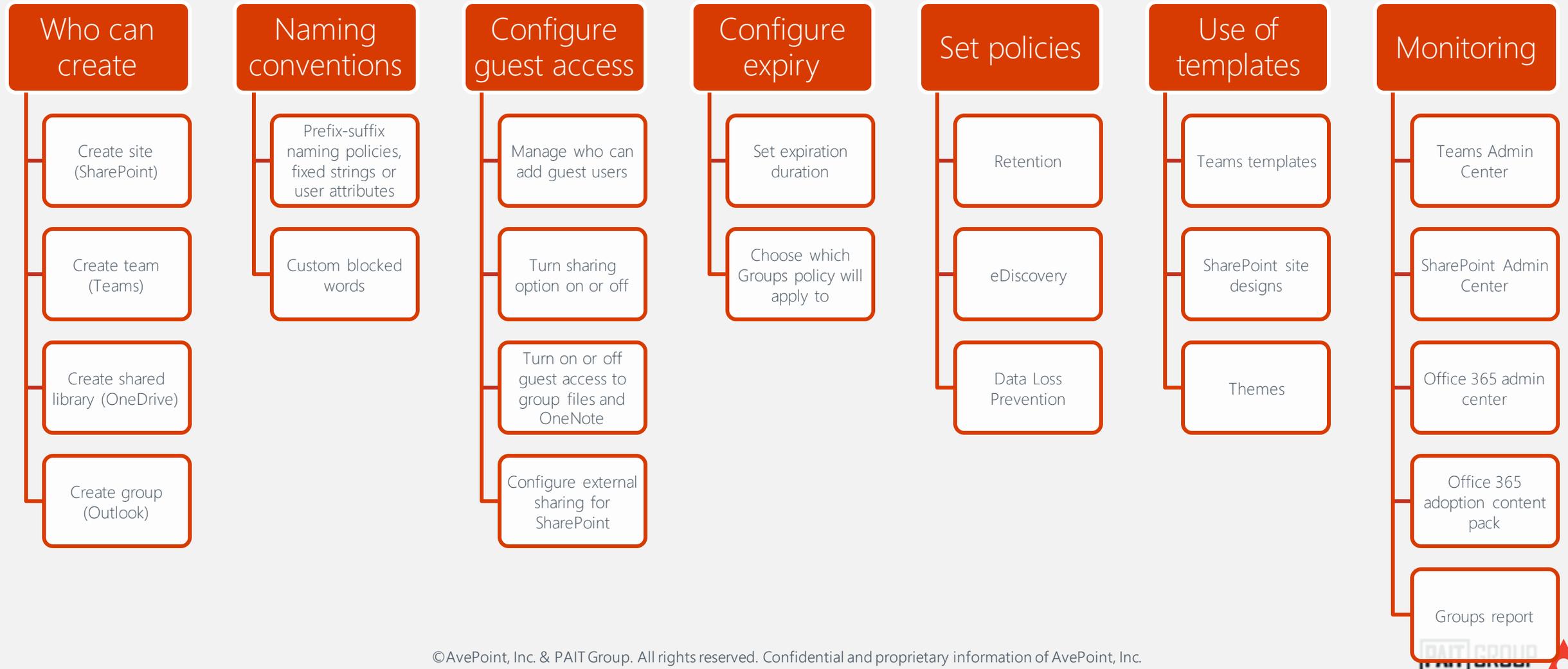


Do team creators need the ability to assign organization-specific classifications to teams?

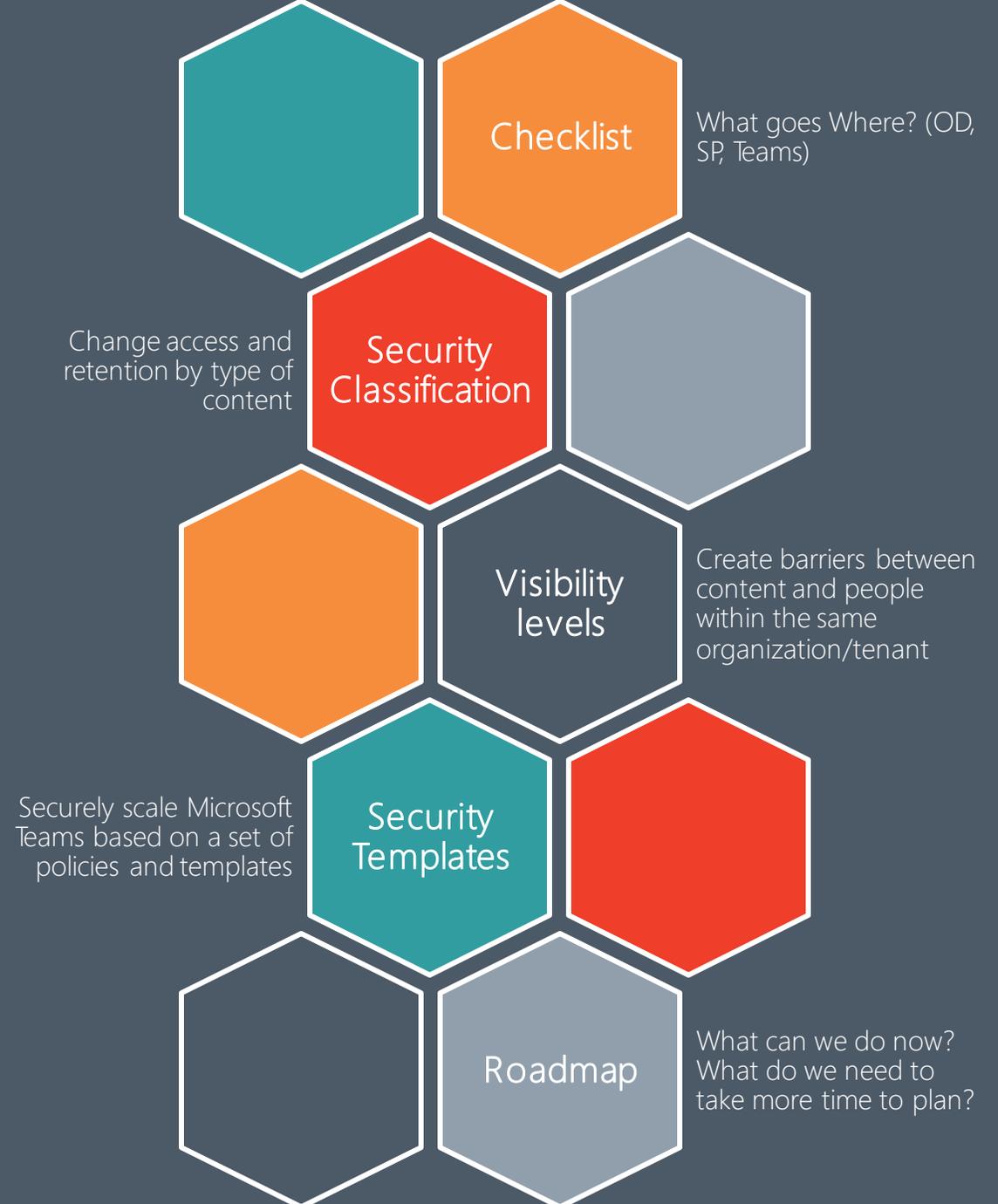


Does your organization require limiting who can create teams?

Control governance before day one

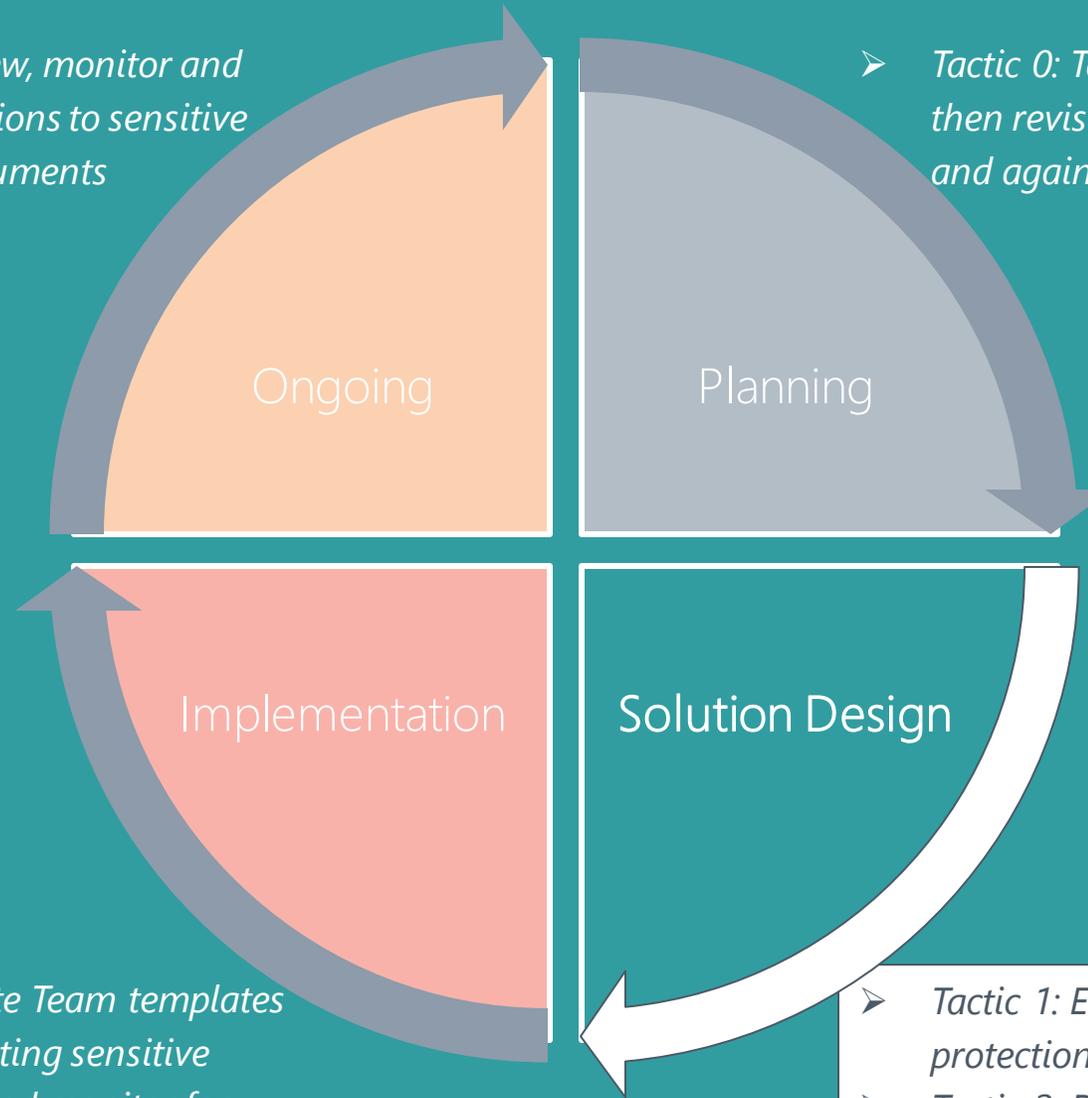


Planning Outcomes



- *Tactic 4: Review, monitor and audit permissions to sensitive data and documents*

- *Tactic 0: Take the time to plan – then revisit your plan again – and again.*



- *Tactic 3: Create Team templates for Teams hosting sensitive information and monitor for configuration/membership drift*

- *Tactic 1: Ensure adequate data protection and retention*
- *Tactic 2: Review guest access and external sharing settings*

Checklist – What goes where?

Classic sites

Modern Communication sites

Teams w/ Modern team site

contoso.sharepoint.com

Root (Publish)

News (Publish)

HR (Publish)

HR (Collab)

Project #1 (Collab)

Apps

Videos

News rollup

Corporate News

Blogs

Employee Spotlight

Benefits

Links

Policies & Procedures

HR News

Employee Reviews (SharePoint)

Salary Information (SharePoint)

Policy Drafts (SharePoint)

Tasks (Planner)

Task List (Planner)

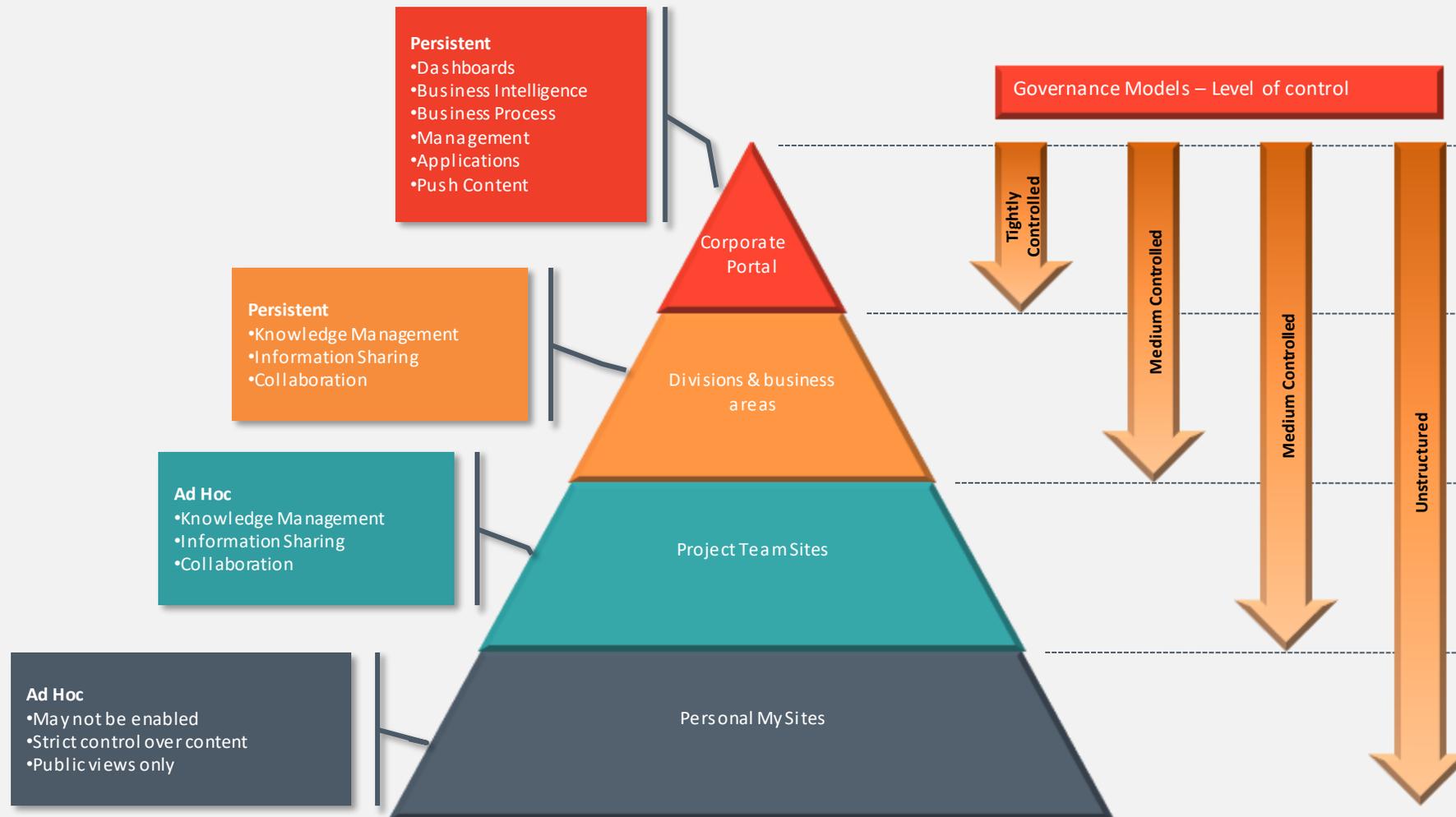
Files (SharePoint)

Notes (Wiki-OneNote)

Forms (PowerApps)

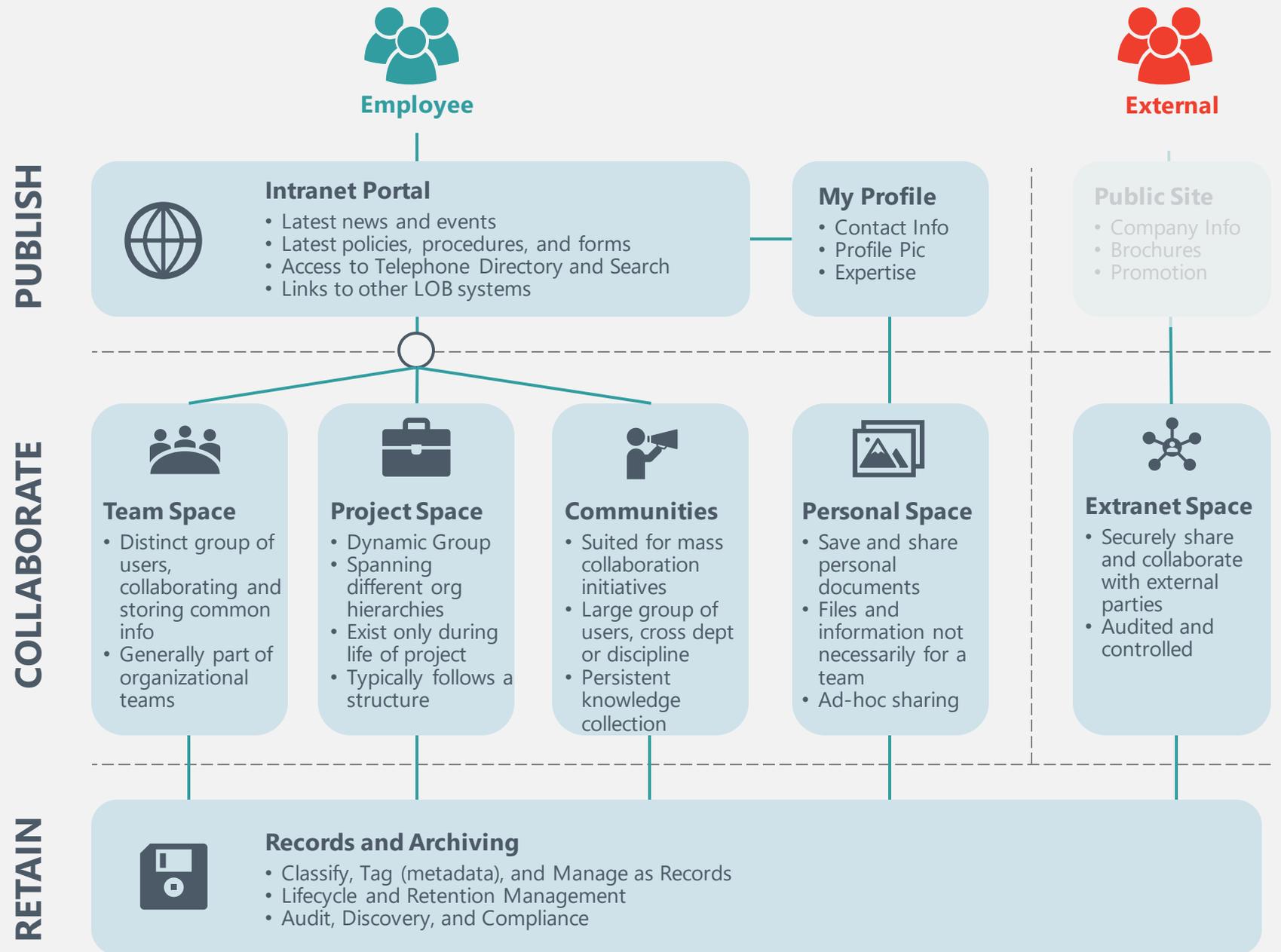
<https://www.paitgroup.com/blog/modernizing-your-approach-to-site-architecture-in-sharepoint-and-office-365>

Different Strategies for Different Information



A Best-Practice Approach to Information Architecture and Knowledge Management in Office 365

Don't try and organize your information by department... think about the information type instead.



Provisioning

How Teams are
Born

- Sprawl
- Duplication
- Appropriateness
- Convention
- Cataloging

Microsoft's native tooling to help govern Teams provisioning...

Restricting self-service creation

Can restrict creation to select group of users

Set group visibility

Options for public/private, hidden membership/group

Sensitivity Labels

Set a label at the Team level to manage access for

internal guest users

Usage Guidelines

Link to acceptable use policy etc.

Dynamic Membership

Set group membership by AAD attribute

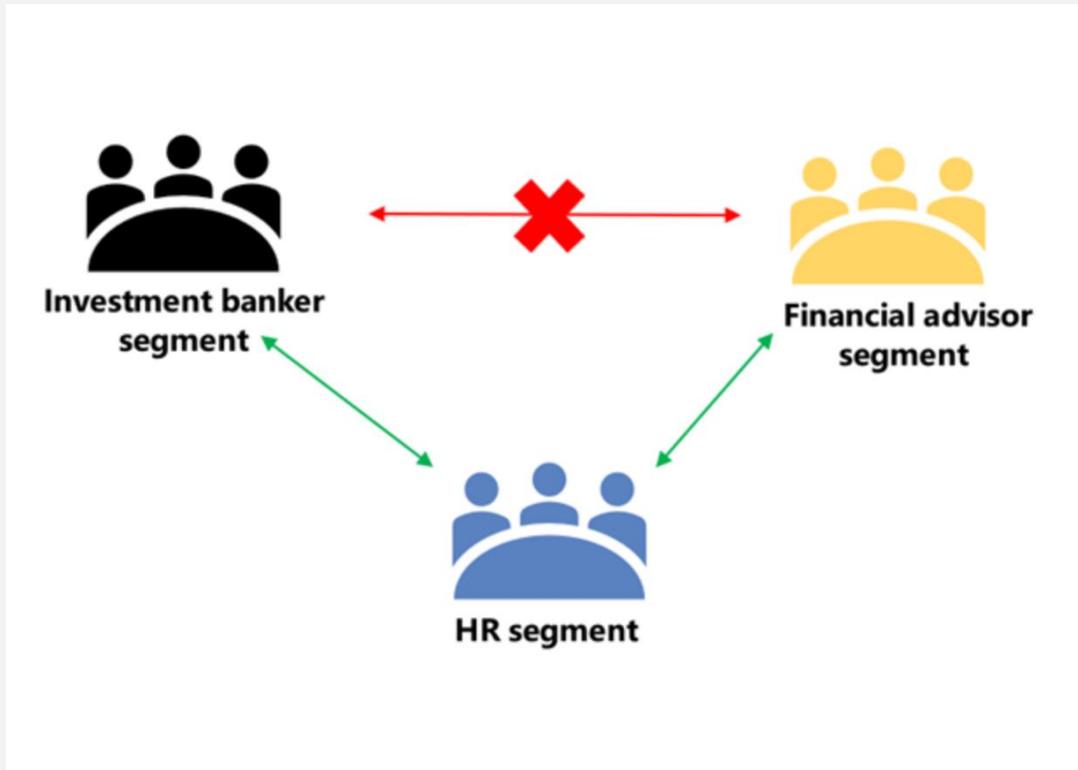
Naming rules

Prefix/Suffix, blocked words

<https://blogs.office.com/en-us/2017/04/06/whats-new-in-office-365-groups-for-april-2017>

Tactic 1: Ensure adequate data protection and retention

Naming Conventions & Scopes



Naming conventions (Azure AD Premium P1 for all users)

Adding a prefix or suffix

Helpful with M&A, companies with multiple companies under one umbrella (HR for different locations)

Microsoft Teams Scoped Directory Search (G5)

Creates a virtual boundary when searching for Teams

Your organization has multiple companies within its tenant that you want to keep separate.

Your school wants to limit chats between faculty and students.

Information Barrier Policies (G5)

Two-way restrictions

Prevents unauthorized communications in chat and channels

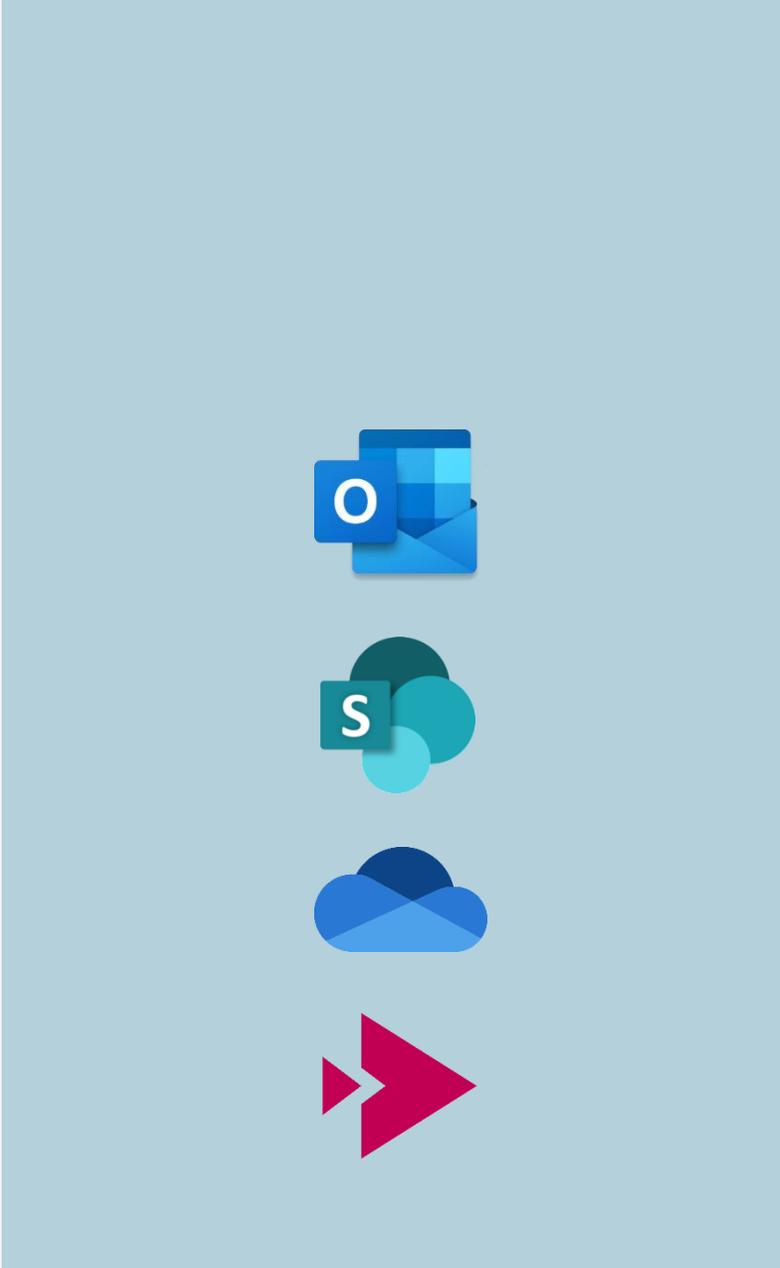
FINRA driven

Teams scoped directory search is just one example

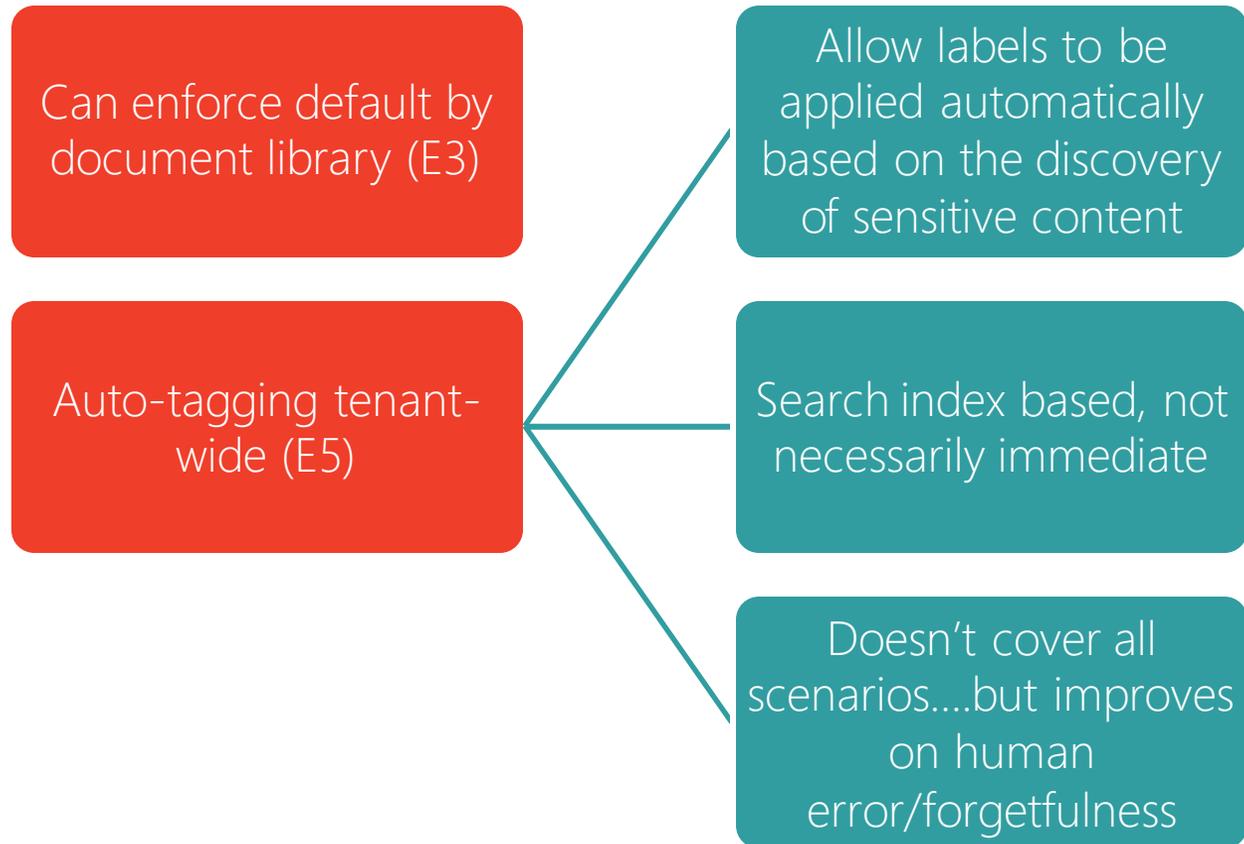
Unified Labels enable IM for your Teams data!



Sensitivity Label		Retention Label	
Confidential		Corporate Files- 30 Years	
PII	Trade Secret	Administrative	
Yes	Yes	Project File	15 Years



Auto-Tagging with Labels



Also consider...

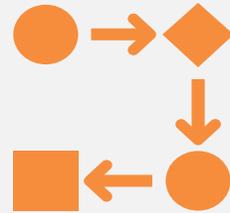


Additional PROVISIONING ideas from the field

- *Guidance to the user for what to use and when*
- *User/Division-level workflows*
- *Teams "Templates"*
- *Approval when necessary*
- *More flexible naming policies*
- *Setting guest access/external setting per team*
- *Metadata collection for cataloging your collab workspaces*
- *Named data owners*

Tactic 2: Review guest access and external sharing settings

Guest Access and Sharing



External Sharing

What types of content can be shared outside of the organization, if any?

Should those users be able to download or print that content?

Sharing links, anonymous access & expiration policies



Guest Access?

Are guests able to log into your Microsoft Teams?

What types of content can be shared when guests can log in?

How do we ensure secure information is not saved in Teams with guest access enabled?

Guest Access and Sharing

External Access



Guest Access

Access?

What types of content can be shared with external users?

Should those users be able to print that content?

Sharing links, anonymous access & expiration policies

Can users log into your Microsoft Teams?

What types of content can be shared when guests can log in?

How do you ensure secure information is not shared with guest access enabled?

External Sharing

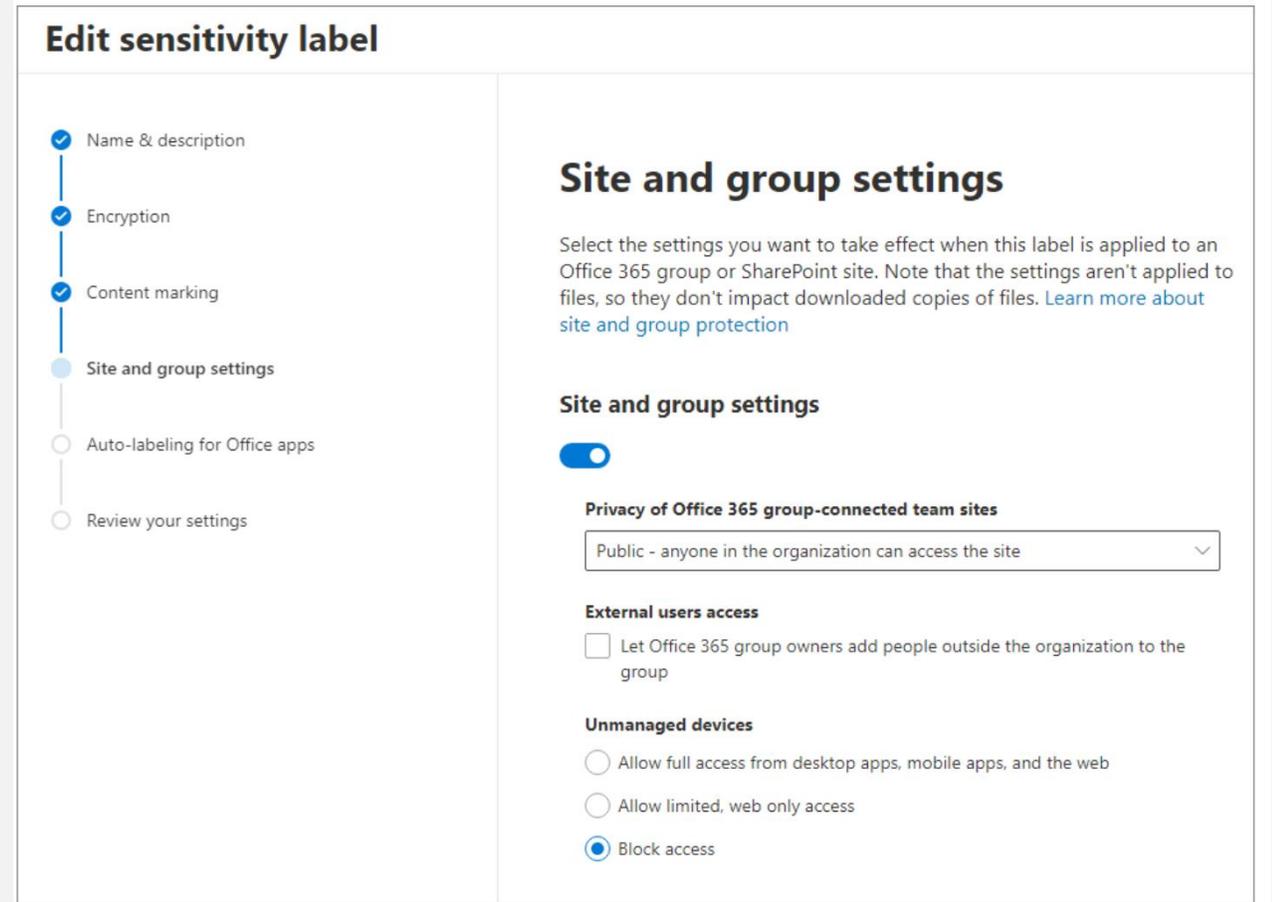
Labels for Containers (New!)

Privacy (public or private) of Microsoft 365 group-connected teams sites

External users access

Access from unmanaged devices

<https://www.youtube.com/watch?v=SEyUce9UsIU>



Edit sensitivity label

- Name & description
- Encryption
- Content marking
- Site and group settings
- Auto-labeling for Office apps
- Review your settings

Site and group settings

Select the settings you want to take effect when this label is applied to an Office 365 group or SharePoint site. Note that the settings aren't applied to files, so they don't impact downloaded copies of files. [Learn more about site and group protection](#)

Site and group settings

Privacy of Office 365 group-connected team sites

Public - anyone in the organization can access the site

External users access

Let Office 365 group owners add people outside the organization to the group

Unmanaged devices

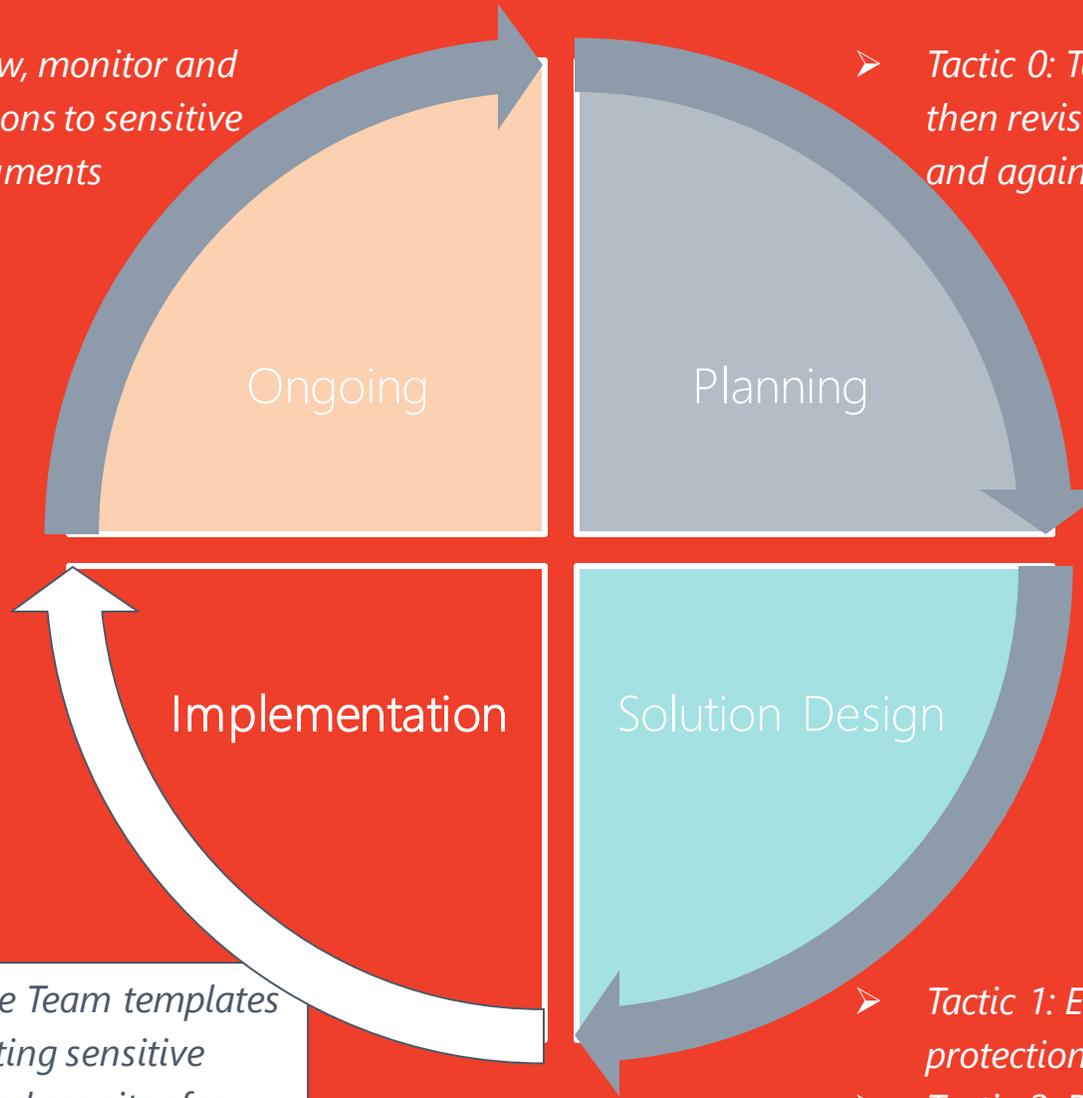
Allow full access from desktop apps, mobile apps, and the web

Allow limited, web only access

Block access

- *Tactic 4: Review, monitor and audit permissions to sensitive data and documents*

- *Tactic 0: Take the time to plan – then revisit your plan again – and again.*



- *Tactic 3: Create Team templates for Teams hosting sensitive information and monitor for configuration/membership drift*

- *Tactic 1: Ensure adequate data protection and retention*
- *Tactic 2: Review guest access and external sharing settings*

Management

Ongoing Operations

- Day to day administration of Teams
- Monitor for Group Usage and Adoption
- Ensure users aren't doing what they shouldn't
- You're old friend hasn't gone anywhere...

Why Training Alone is Not Working



Non-Contextual

Unclear Roles

Generational Gap

What's In It For Me?

User Adoption

- **Train** users on not just the HOW but the WHY
- **Prioritize Ongoing Support and Education** to ensure users can take advantage of new features and adapt to changing needs in your organization
- **Keep it simple** – lengthy governance documents are rarely effective. Share checklists and one-pagers to keep users on track!
- **User Acceptance Testing** will help you determine if your approach is effective and easy to understand
- **Use templates and automation** where possible to help prevent human error and increase user confidence in the security of Microsoft Teams

Tactic 3: Create Team templates for Teams hosting sensitive information and monitor for configuration/membership drift

Create from existing Team

You are using "Stephanie Demo Team" as a template for a new team ×

Stephanie Demo Team [copy] ✓

Description

Let people know what this team is all about

Privacy

Private - Only team owners can add members ▾

Choose what you'd like to include from the original team

Messages, files and content won't be copied. You'll need to set up tabs and connectors again.

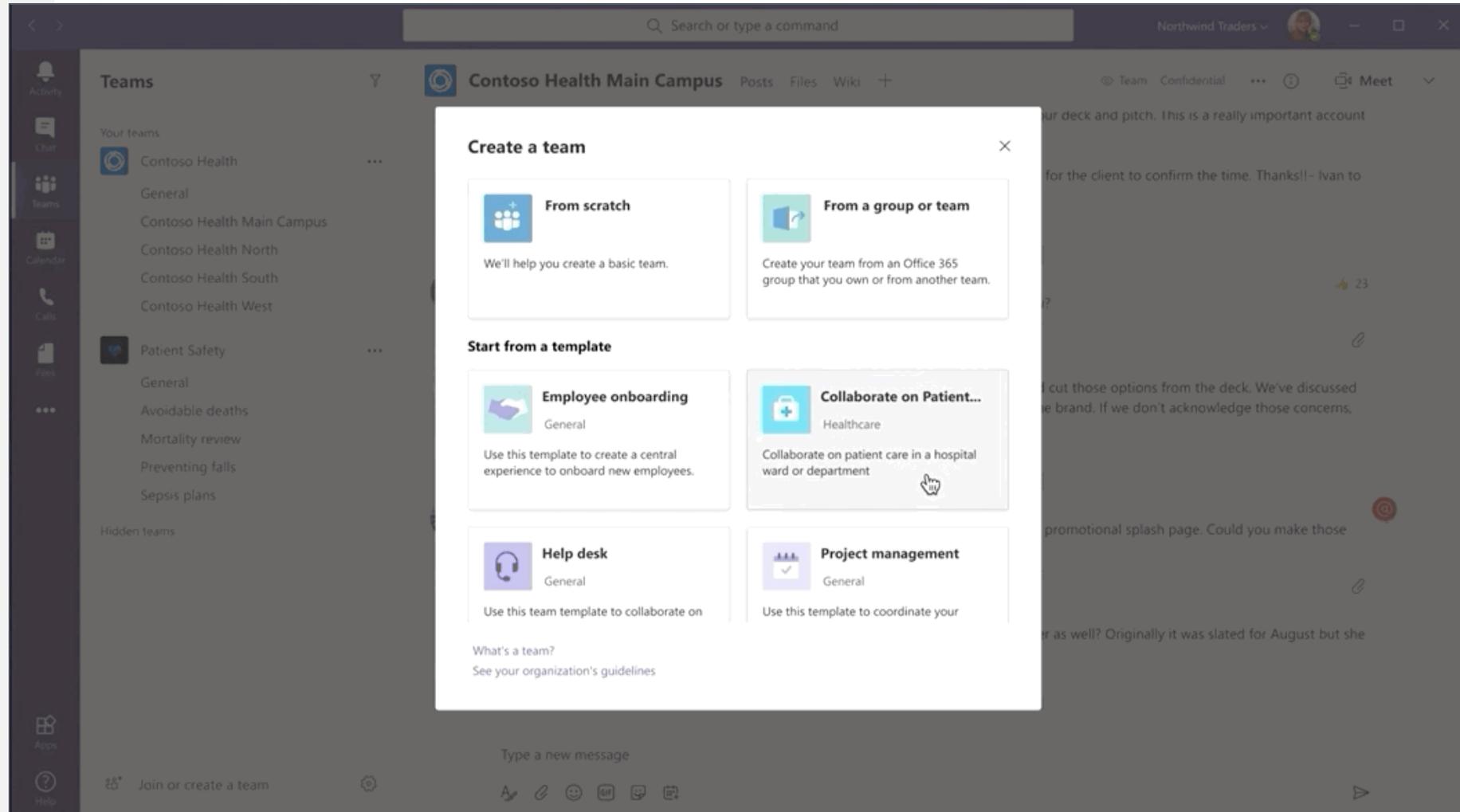
Channels Apps

Tabs Members (5 people)

Team settings

< Back Create

Teams Templates *In development*



<https://docs.microsoft.com/en-us/MicrosoftTeams/get-started-with-teams-templates-in-the-admin-console>

Teams Templates *In development*

The screenshot displays the Microsoft Teams admin center interface. The left-hand navigation pane is dark blue and contains the following items: Dashboard, Teams (with a sub-menu for Manage teams and Teams policies), Team templates (highlighted with a dashed border), Devices, Locations, Users, Meetings, Messaging policies, Teams apps (with sub-menus for Manage apps, Permission policies, and Setup policies), Voice, and Policy packages. The main content area is titled "Team templates" and includes a descriptive paragraph: "Team templates are pre-built definitions of a team's structure designed around a business need or project. You can create a template using the Teams client, then upload and manage the templates stored in your organization. These templates can be assigned to a specific groups using team policies." Below this text is a table with columns for Name and Description. The table contains several entries, with "Adopt Office 365" selected. At the top of the table are action buttons for Add, Edit, Duplicate, and Delete, along with a search bar.

	Name	Description
<input type="checkbox"/>	Demo Team	Demo Team
<input checked="" type="checkbox"/>	Adopt Office 365	Help build, grow, and sustain your Champions community rollout by evangelizing and helping your peers
<input type="checkbox"/>	Manage a Project	Manage tasks, share documents, conduct project meetings and document risks and decisions with this te
<input type="checkbox"/>	Manage an Event	Manage tasks, documents and collaborate on everything you need to deliver a compelling event. Invite g
<input type="checkbox"/>	Onboard Employees	Improve your culture and streamline your employee onboarding with this central team for resources, que
<input type="checkbox"/>	Organize Help Desk	Collaborate on documentation, policy and processes that support your helpdesk. Integrate your existing
<input type="checkbox"/>	Collaborate on Patient Care	Streamline healthcare communication and collaboration within a ward, pod, or department. The template
<input type="checkbox"/>	Collaborate on a Global Crisis or Event	Centralize collaboration for your crisis team across business units and help create business continuity pla

“Templates” are more than a rubber stamp structure

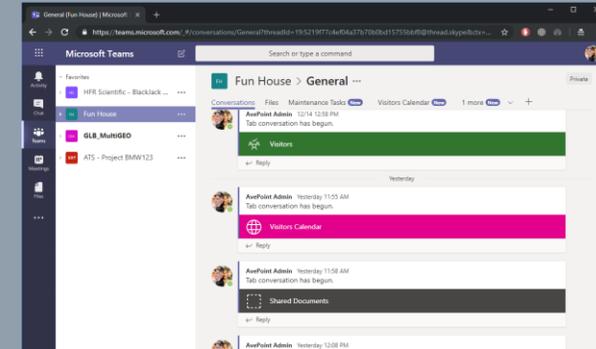
They should include lifecycle components & policy enforcement

- Pre-set Channels, Tab recommendations, and site structure are great for helping contextualize Teams and SharePoint sites for business users.
- AvePoint’s approach accounts for the Operational Governance and lifecycle to ensure “templates” are not ONLY provisioned correctly (and compliant with IT policy) but also managed securely

Special Project



TEMPLATE DEFINITION: Recommended for secure collaboration by Embassy Security. It includes pre-configured topical channels with real-time chat and automated policy enforcement on membership and guest membership restrictions.



EXTERNAL SHARING	 No external sharing
EXPIRATION/RETENTION	3 Months after last accessed
WHO CAN CREATE	All requests through Central IT
RECERTIFY MEMBERS	after 1 Month

Targeted, Policy Enforcement by Division or Purpose

AvePoint's Delegation Solution

AvePoint Online Services (AOS) provides agencies with the ability to create a series of centralized core services that are deployed across the entire tenant.

Then, Division by Division (or other unique specifiers) policies and services can be deployed enabling each to meet their unique needs.

Additionally, AOS combines service/role-based permissions (SharePoint Admin, Exchange Report, RBAC, etc) with content scope to enable elevated privilege, where required, without providing tenant-wide access to services such as SharePoint.

Tenant Wide General Services

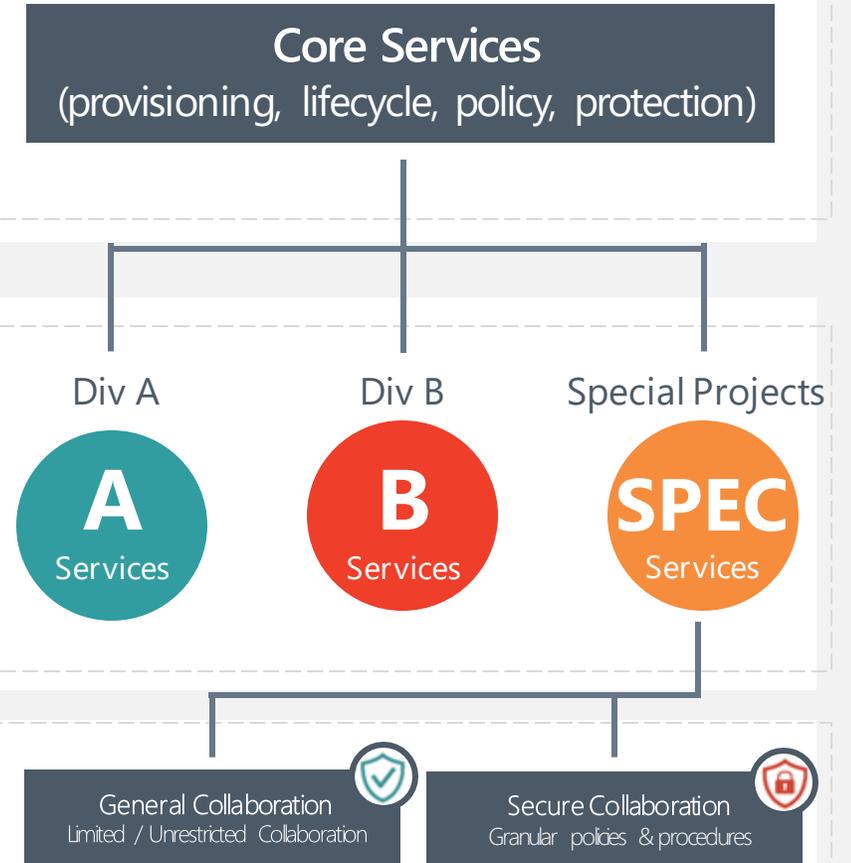
- Available to all/most users
- Address general productivity, security, compliance needs
- Remove burden from centralized IT

Address Unique Needs of Specific Offices

- Division and Unit specific configurations
- Enable more/less control and restrictions
- E.g.,: allow external sharing separately for each SharePoint & Teams office-by-office

Specialized Services Smaller Groups

- Unique needs can be addressed
- Pilots of future services



AvePoint MyHub

Permission-Trimmed Service Catalog

The screenshot displays the Microsoft Teams interface for the 'MyHub Insider' application. The top navigation bar includes 'Microsoft Teams', a search bar, and a user profile icon. The main content area is divided into sections: 'Change Management' and 'Create'. Under 'Change Management', there is a 'Manage Workspaces' card with a description: 'If you are not sure where to start, you can use this questionnaire to guide you to the appropriate service request.' Under 'Create', there are three cards: 'Create Private Team' (describing a request to create a group/team/community and mentioning Barriemore Barlow), 'Guest User Request' (describing a request to invite a new guest user and mentioning Ian Anderson), and 'New Workspace Request' (describing a questionnaire for workspace requests).

AvePoint MyHub

End-user Services
with Policy-informed
templates & controls

The screenshot displays the Microsoft Teams interface for a team named "MyHub Insider". The left sidebar contains navigation options: Activity, Chat (with a notification badge), AVA, Teams, Calendar, Files, MyHub Insider (highlighted), and a menu icon. The top navigation bar includes "Microsoft Teams", a search bar, and a user profile icon. Below the navigation bar, there are tabs for "Home", "Hubs", "Workspaces", "Requests", and a "Create a workspace" button. The main content area is titled "Team members permissions" and lists several settings:

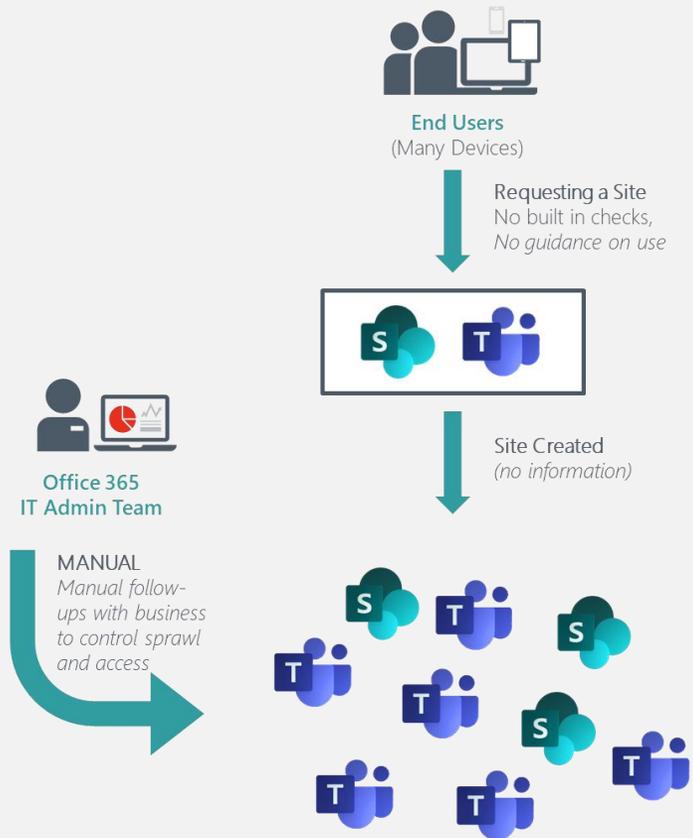
- Allow members to create and update channels
- Allow members to create private channels
- Allow members to delete and restore channels
- Allow members to add and remove apps
- Allow members to create, update, and remove tabs
- Allow members to create, update, and remove connectors
- Allow members to delete their messages
- Allow members to edit their messages

Below the permissions section is the "Additional Information" section, which includes several dropdown menus and radio buttons:

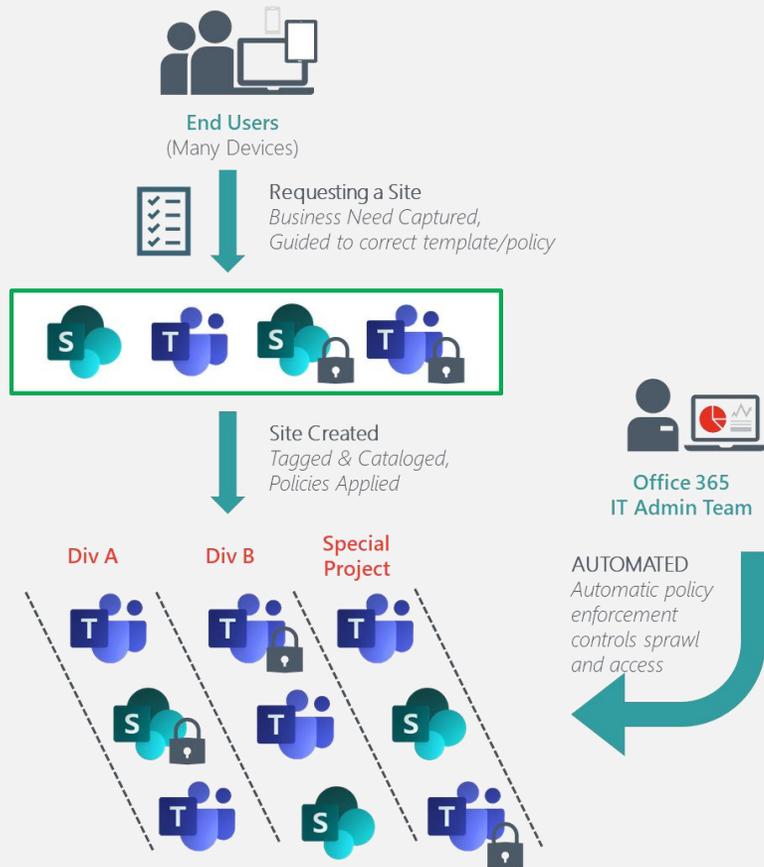
- Purpose**: Collaboration
- Region ***: US
- Access Level**: Internal
- Object Type**: Team
- Critical Business Application ***: No

Auto-Enforcement with AvePoint

UNRESTRICTED CREATION



WITH AUTOMATED GOVERNANCE



Automated Governance gathers information during provisioning and recertification to enable business-driven enforcement of IT policies.

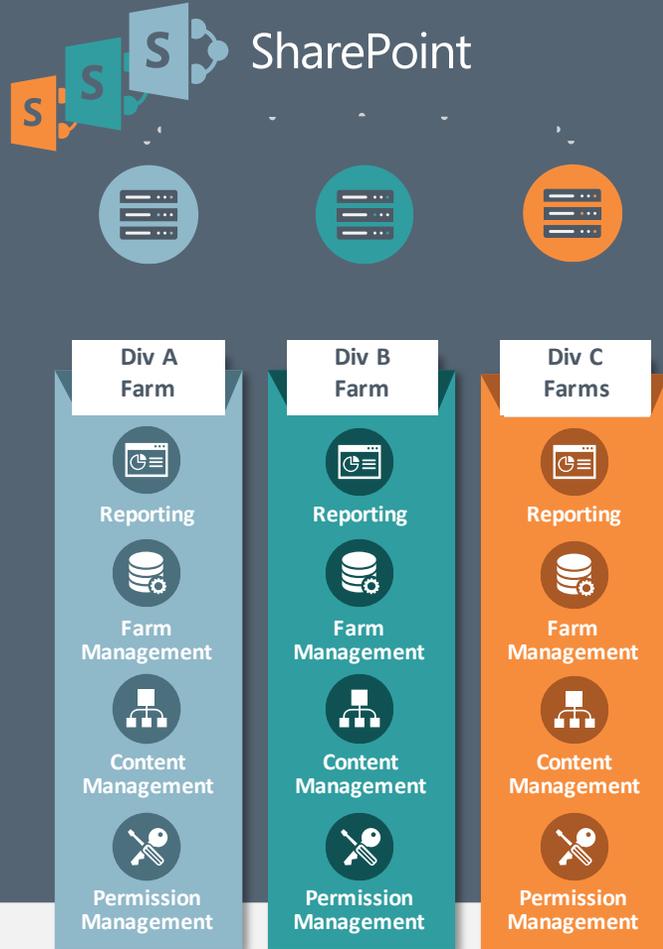
Workspaces are categorized to drive granular, bureau-by-bureau policy enforcement.

End users are only granted privileges desired by IT, allowing full management through AvePoint's service catalog.

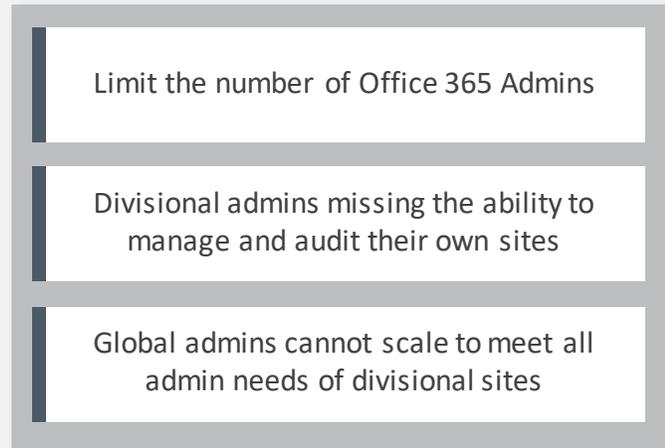
Landscape reporting across each bureau allows shared cost management and identifies inappropriate usage of the system.

The M365 Challenge for Regulated Industry and Government

TRADITIONAL DIVISIONAL FARMS



CENTRALIZED ORGANIZATIONAL TENANT



CONCERNS

Example 90 Day Roadmap

Month 1

- Identify 3 use cases for Yammer and 3 use cases for Teams
- Engage leadership and secure buy-in
- Develop rules of engagement and how-to resources

Month 2

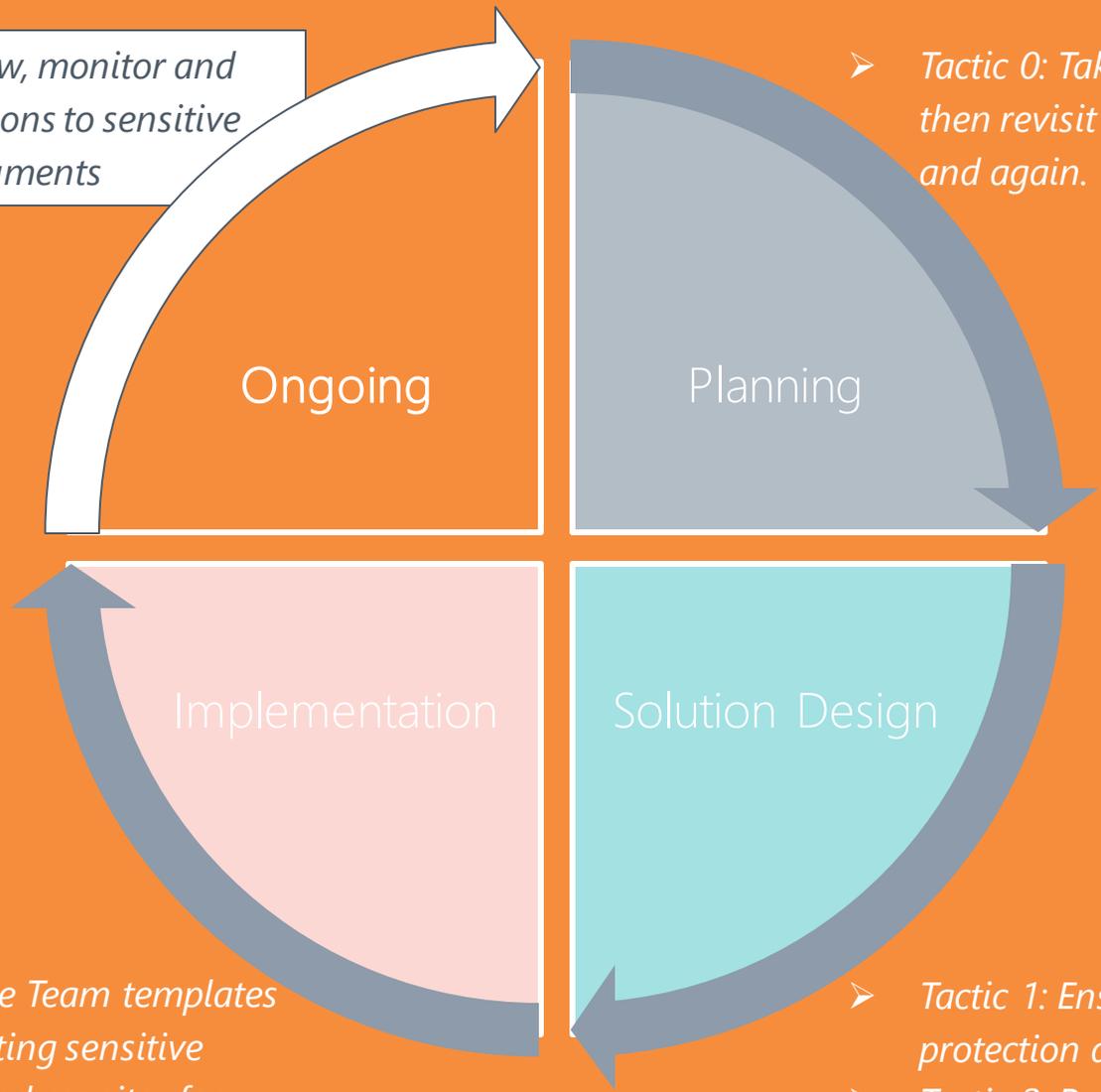
- Engage 3 departments/groups to pilot Yammer and Teams use cases
- Identify what works and what doesn't with use cases then modify
- Configure Yammer and Teams to support use cases for company wide deployment

Month 3

- Launch use cases company wide
- Encourage leadership to consistently promote and adopt the use cases
- Showcase and highlight wins of adopting Yammer and Teams

➤ *Tactic 4: Review, monitor and audit permissions to sensitive data and documents*

➤ *Tactic 0: Take the time to plan – then revisit your plan again – and again.*



➤ *Tactic 3: Create Team templates for Teams hosting sensitive information and monitor for configuration/membership drift*

➤ *Tactic 1: Ensure adequate data protection and retention*
➤ *Tactic 2: Review guest access and external sharing settings*

Lifecycle

Retention,
Expiration and
Disposition

- How do I know when a Group should be expired
- How do I get rid of it “safely”
- How do I make sure information management policies are enforced?

Microsoft native tooling to help govern Teams lifecycle...

Team "Archiving"

- Removes Team from user's lists of active Teams
- Puts Team conversations and files into "read only"
- Can be reversed by a Team owner

Soft Delete

- Recover deleted Teams and Groups

Group Expiration

- Require owners to confirm their Group is still active and relevant periodically

Retention and expiration of content

- Records management and content compliance policies

Archiving

Show/Hide functionality

Archive Teams in the Teams admin panel

- When you archive a team, all activity for that team ceases.
- Archiving a team also archives private channels in the team and their associated site collections.
- However, you can still add or remove members and update roles and you can still view all the team activity in standard and private channels, files, and chats.

When you delete a team, team activity in standard and private channels (and associated site collections), files, and chats is also deleted.

On that note about retention....

https://www.theregister.com/2020/08/24/kpmg_microsoft_teams/

Also consider...



Additional LIFECYCLE ideas from the field

- Periodic Renewal/Recertification
- Managed de-provisioning workflows
- Offline Archiving
- Data Export

AvePoint MyHub

Periodic Teams lease
renewals & member
recertifications

Microsoft Teams

Search

MyHub Insider Chat Home About

Home Hubs Workspaces Requests ...

Cancel

Team renewal: Q2 Outing

Renewal steps	Additional Information renewal
<p><input checked="" type="checkbox"/> Contact renewal</p> <p>Confirm that the primary and secondary contacts are still correct. If necessary, you can assign the roles to other users.</p>	<p>Critical Business Application *</p> <p><input type="radio"/> Yes <input checked="" type="radio"/> No</p>
<p><input checked="" type="checkbox"/> Permission renewal</p> <p>Confirm that the group team site permissions for users and groups are still correct. If necessary, you can update the permissions.</p>	<p>Purpose *</p> <p>Collaboration</p>
<p><input checked="" type="checkbox"/> Membership renewal</p> <p>Confirm that the owners and members are still correct. If necessary, you can update the membership.</p>	<p>Region *</p> <p>Canada</p>
<p><input checked="" type="checkbox"/> Additional Information renewal</p> <p>Confirm that the metadata is still correct. If necessary, you can update the metadata values.</p>	<p>Line of Service</p> <p>Corporate Communications (COM)</p>

Back Submit

Tactic 4: Review, monitor and audit permissions to sensitive data and documents

Microsoft native tooling to help govern Teams management...

Teams Admin Center

Day to day management of the Teams service with policies and settings

Usage Reporting

Track and monitor usage and adoption

Audit Reporting

Report on user activity within Microsoft Teams

<https://blogs.office.com/en-us/2017/04/06/whats-new-in-office-365-groups-for-april-2017>

Compliance Manager (new!)

Microsoft 365 compliance

Compliance Manager

Overview | Improvement actions | Solutions | Assessments | Assessment templates

Compliance Manager measures your progress in completing actions that help reduce risks around data protection and regulatory standards. [Find guidance and documentation](#)

Filter

Overall compliance score

Your compliance score: 75%

12093/16101 points achieved

Solutions that affect your score

Taking key actions in your compliance solutions will increase your overall score.

Solution	Score contribution	Remaining actions
Audit	0/54 points	10
Azure Active Directory	0/379 points	23
Azure Information Protection	0/27 points	1

[View all solutions](#)

Your points achieved 0/4008

Microsoft managed points achieved

Compliance Manager Assessments

Key improvement actions

None Not assessed Passed Failed low risk Failed medium risk Failed high risk Out of scope To be detected
Could not be detected Partially tested

Improvement action

- Implement account lockout
- Protect authenticators commensurate with us
- Refresh authenticators

Create assessment

Impact Test status

Select a template

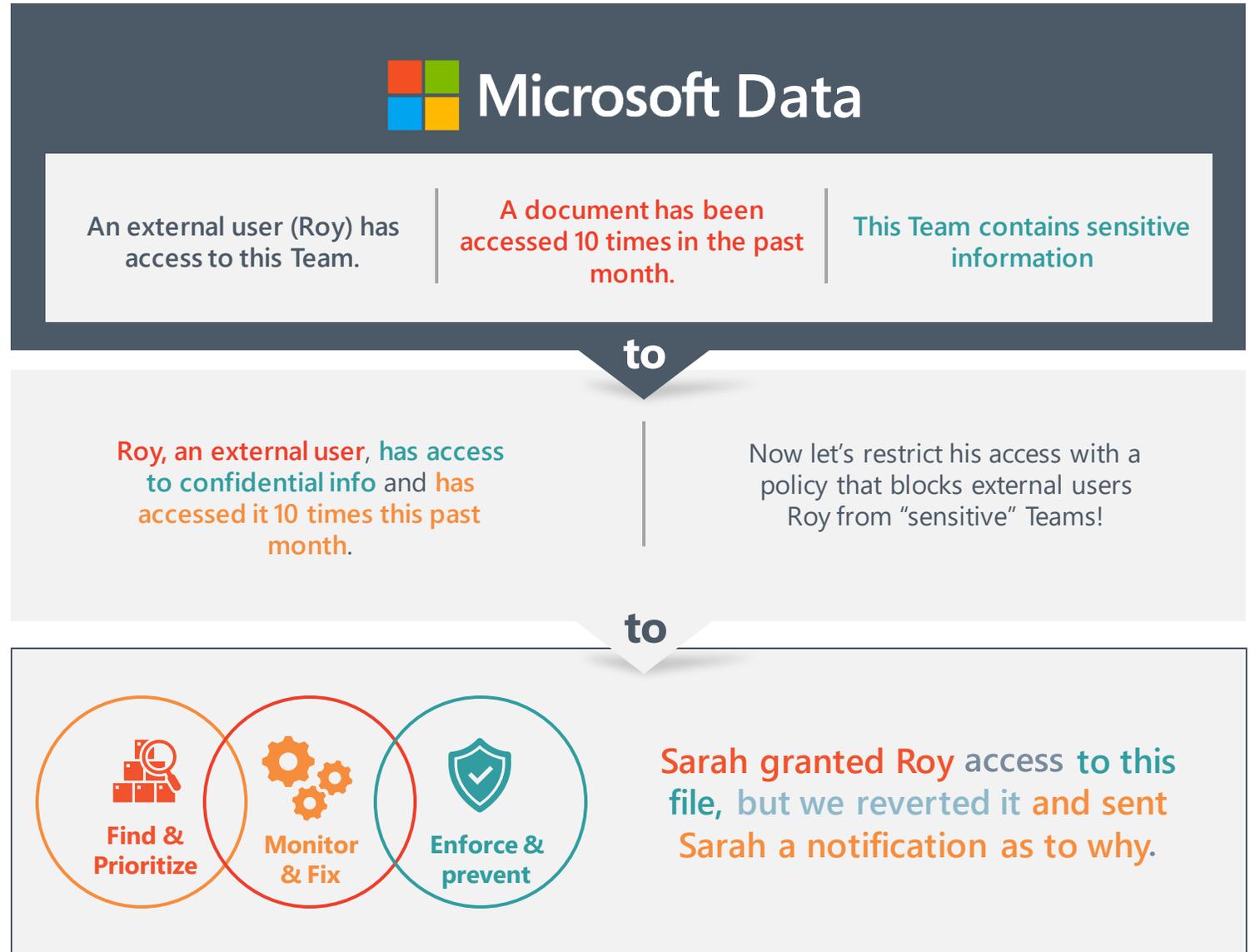
Choose a template as the basis for your assessment. Learn more about [Compliance Manager templates](#).

① Access to premium templates will be subject to new licensing terms in the near future. [Learn more](#)

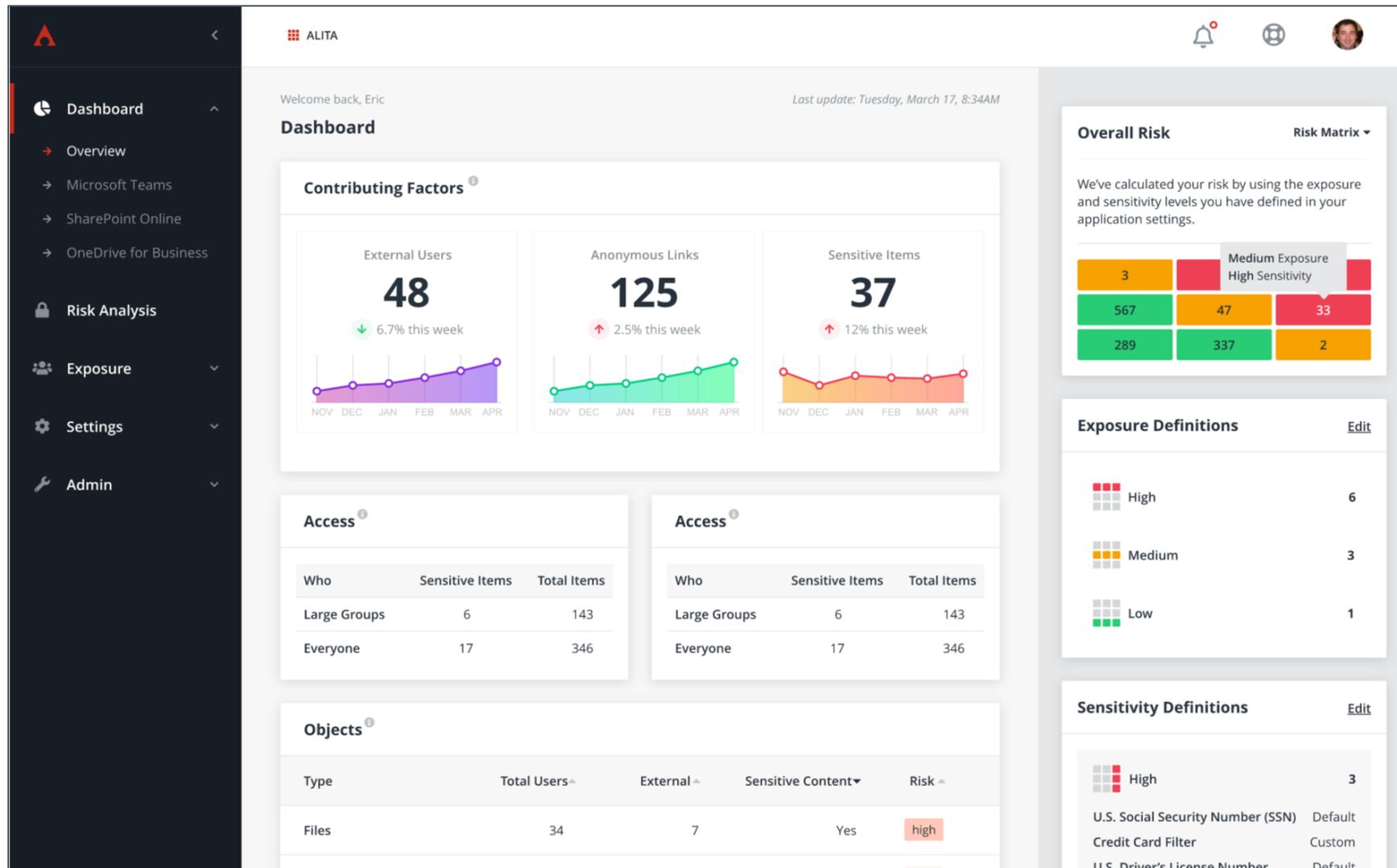
1 of 180 selected Search

Template	Availability
<input checked="" type="checkbox"/> FedRAMP Moderate	Premium
<input type="checkbox"/> FedRAMP SSP High Baseline	Premium
<input type="checkbox"/> Federal Financial Institution...	Premium
<input type="checkbox"/> France - Act 78-17 Of 6 Jan...	Premium
<input type="checkbox"/> Freedom of Information Ac...	Premium
<input type="checkbox"/> Generally Accepted Record...	Premium

Piece together the data Microsoft provides to see the full story of sharing and risk



Insight into who is
accessing what and
what risk that poses



ALITA

Welcome back, Eric Last update: Tuesday, March 17, 8:34AM

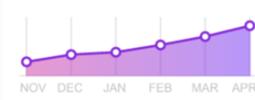
Dashboard

Contributing Factors

External Users

48

↓ 6.7% this week



Anonymous Links

125

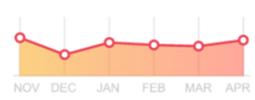
↑ 2.5% this week



Sensitive Items

37

↑ 12% this week



Access

Who	Sensitive Items	Total Items
Large Groups	6	143
Everyone	17	346

Access

Who	Sensitive Items	Total Items
Large Groups	6	143
Everyone	17	346

Objects

Type	Total Users	External	Sensitive Content	Risk
Files	34	7	Yes	high

Overall Risk

Risk Matrix

We've calculated your risk by using the exposure and sensitivity levels you have defined in your application settings.

3	Medium Exposure	
567	High Sensitivity	33
289		2

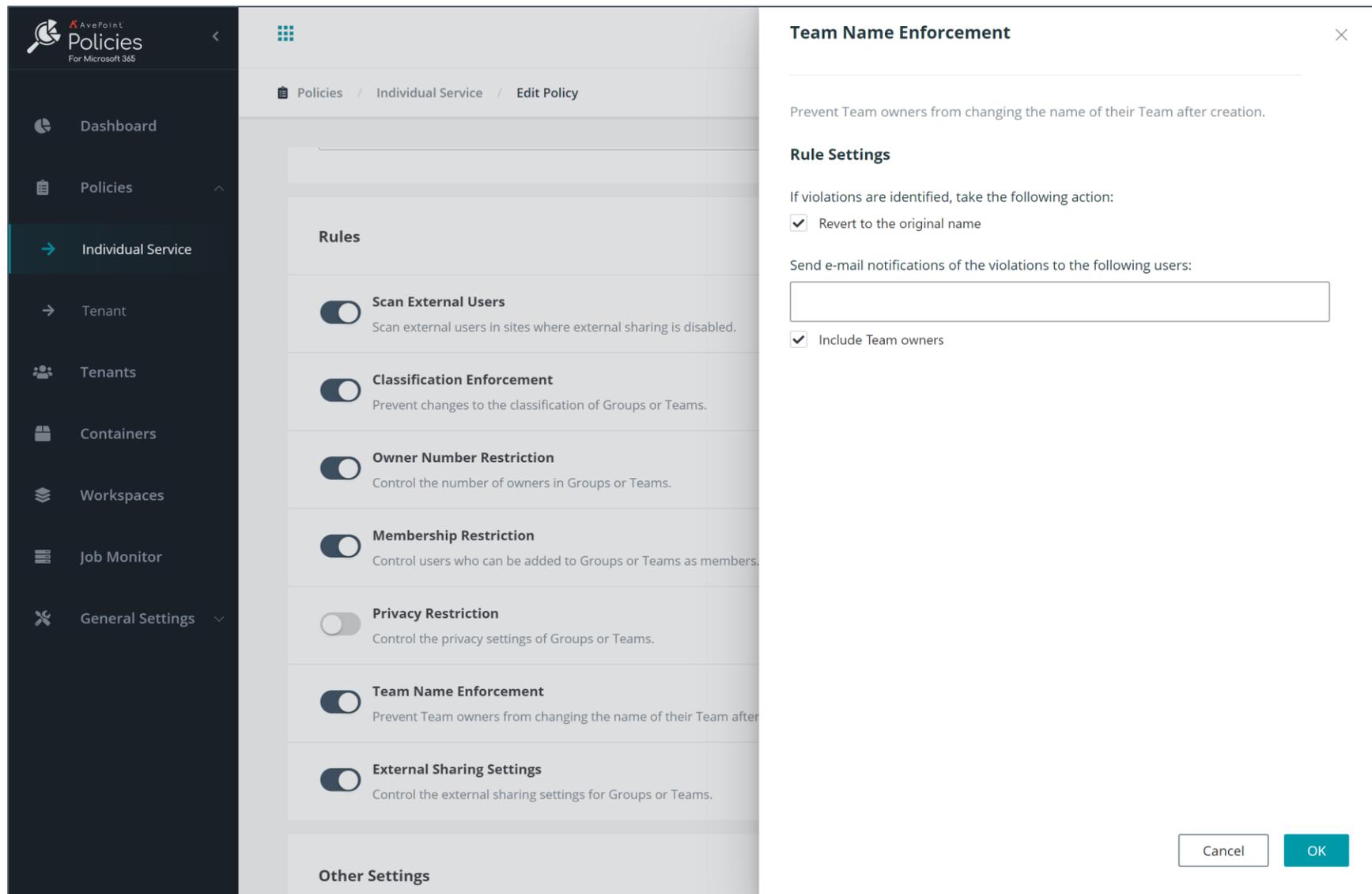
Exposure Definitions

High	6
Medium	3
Low	1

Sensitivity Definitions

High	3
U.S. Social Security Number (SSN)	Default
Credit Card Filter	Custom
U.S. Driver's License Number	Default

Automatic policy enforcement across Teams, OneDrive, and SharePoint



The screenshot displays the AvePoint Policies & Insights interface for Microsoft 365. The left sidebar contains navigation options: Dashboard, Policies, Individual Service (selected), Tenant, Tenants, Containers, Workspaces, Job Monitor, and General Settings. The main content area shows the 'Edit Policy' configuration for 'Individual Service'. Under the 'Rules' section, several policies are listed with toggle switches: Scan External Users, Classification Enforcement, Owner Number Restriction, Membership Restriction, Privacy Restriction, Team Name Enforcement (which is currently turned on), and External Sharing Settings. A modal window titled 'Team Name Enforcement' is open on the right, providing details for the selected policy. The modal includes a description: 'Prevent Team owners from changing the name of their Team after creation.' It also features 'Rule Settings' with a checkbox for 'Revert to the original name' (checked) and a section for 'Send e-mail notifications of the violations to the following users:' with an empty text input field and a checked checkbox for 'Include Team owners'. At the bottom right of the modal are 'Cancel' and 'OK' buttons.

Wrap-Up

- Tactic 1: Review guest access and external sharing settings
- Tactic 2: Ensure adequate data protection and retention
- Tactic 3: Create Team templates for Teams hosting sensitive information and monitor for configuration/membership drift
- Tactic 4: Review, monitor and audit permissions to sensitive data and documents

thank you

Gracias

ευχαριστώ

Danke

Grazie

благодаря

Hvala

Obrigado

Kiitos

شكراً

Tak

Ahsante

Teşekkürler

متشكراً

Salamat Po

감사합니다

Cám ơn

شكريه

Terima Kasih

Dank u Wel

Děkuji

நன்றி

Köszönöm

ありがとう
ございます

ขอขอบคุณครับ

Dziękuję

谢谢

Tack

Mulțumesc

спасибо

Merci

תודה

多謝晒

дядкую

Ďakujem