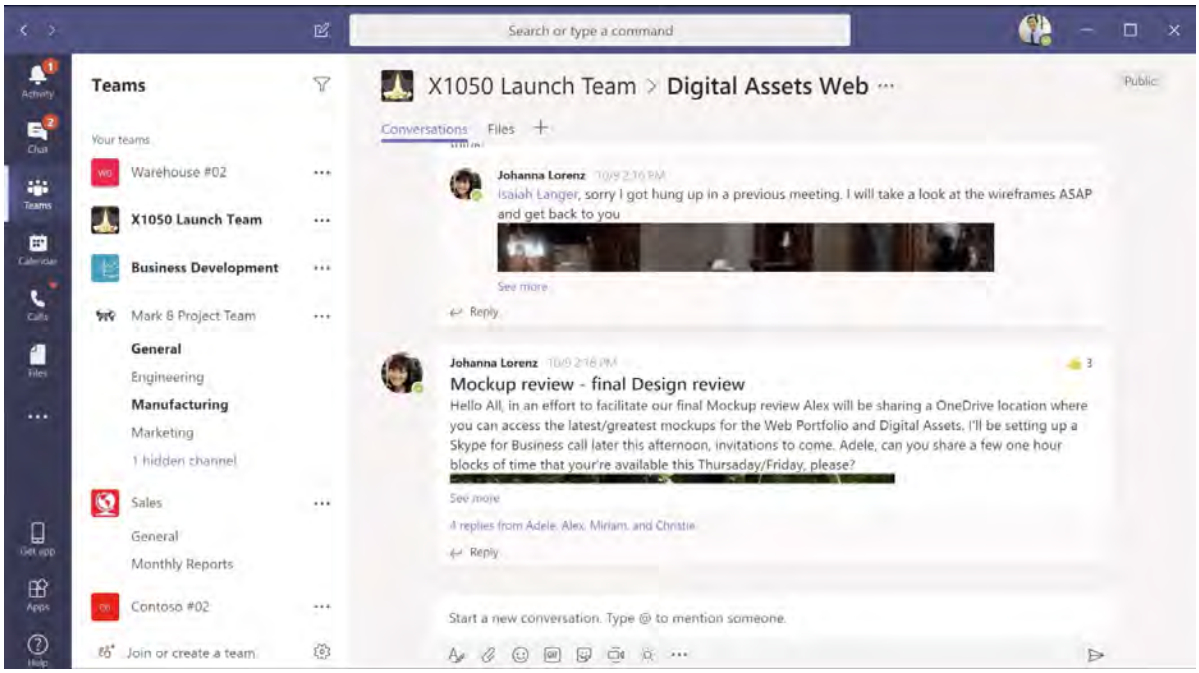
# Microsoft Teams: Guidance for Legal & Compliance Professionals

Many organizations are rapidly expanding their use of Microsoft Teams in response to COVID-19 directives on physical distancing and remote working. Implementation is primarily an administrator's job but there are numerous security, data privacy, and compliance features that are important for enterprise leaders and their legal and compliance advisors to consider.

This presentation is divided into three sections: An overview of Teams, Teams security & compliance controls, and Advanced Microsoft 365 security & compliance.

## Teams overview See page 3

Many of you may be new to Microsoft Teams—especially if it has been rapidly implemented within your organization in response to the current crisis. Even experienced users are discovering features that they didn't need before—when co-workers were just down the hall. Needless to say, Microsoft Teams is seeing unprecedented usage right now. The first section is, therefore, a quick overview of the features most teams use on a daily basis.

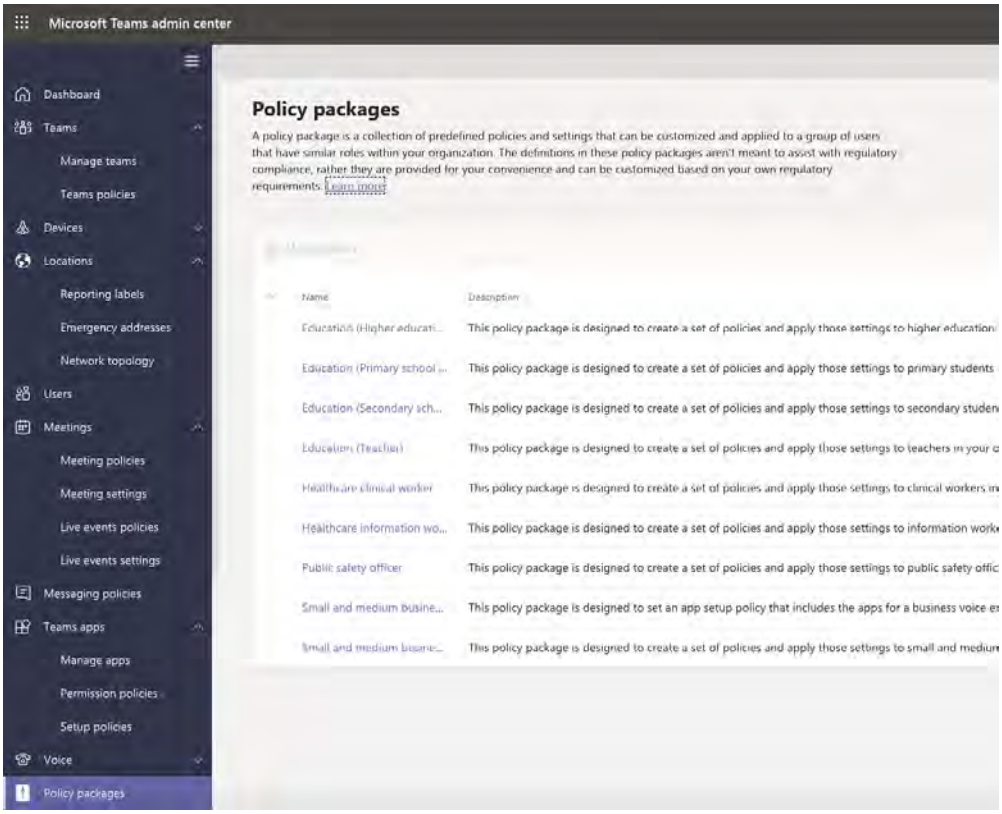


## Teams security & compliance controls See page 5

There are security and compliance-related controls for configuring the core experiences within Teams, including policies and organization-wide settings, such as guest access and more. You can implement these in the Microsoft Teams admin center.

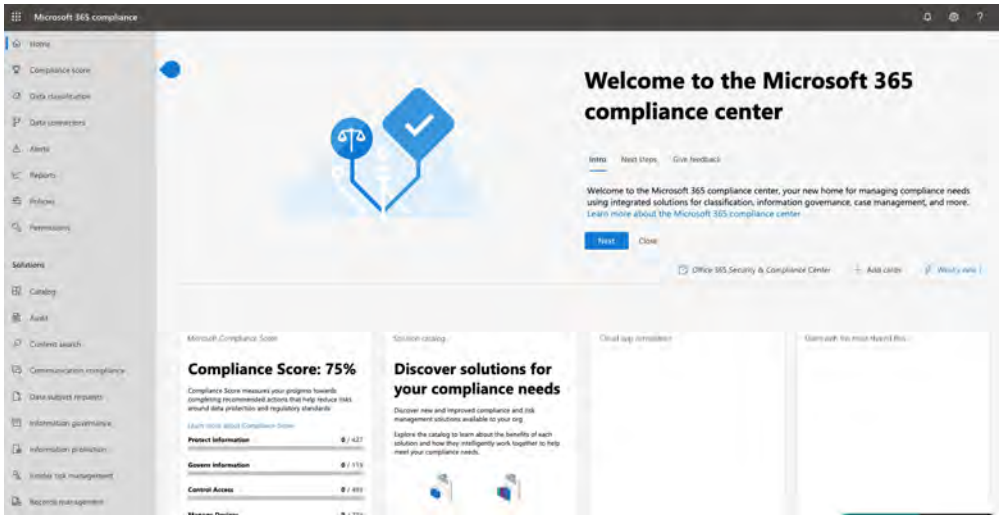
You'll find that even a default implementation of Teams meets most of your data protection, security, and compliance requirements. From there, you can build a comprehensive policy package tailored to your organization, or modify a pre-built package as a starting point.

As a legal and compliance professional, this section should provide you with peace of mind as we explore what your organization can control from the Microsoft Teams admin center.




## Advanced security & compliance See page 6

If you are in a highly regulated field, such as Financial Services or Healthcare, or your organization sets stringent requirements on compliance and data protection, then you will want to know how Microsoft Teams benefits from the security and compliance foundation of Microsoft 365. As legal and compliance professionals, these are all familiar requirements, such as auditing & reporting, eDiscovery, legal hold, data loss prevention, data retention, etc. We cover these advanced topics and more in the third section.



# Teams overview

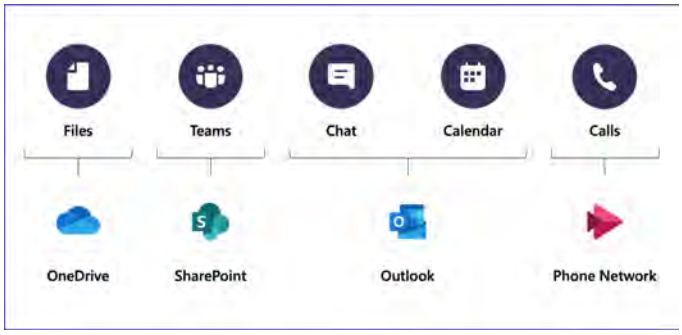
Microsoft Teams brings together everything a team needs: chat and threaded conversations, online meetings with video conferencing, and content collaboration.

## Teams is your hub for teamwork

In Microsoft Teams you can hold meetings, have team conversations, and share files. You can also initiate a private chat and make video or audio calls or schedule a meeting from the chat window. As people begin to work on projects across organizational boundaries, users can create their own teams. Meetings are made simpler with Teams. Besides online meetings, Teams has an integrated calendar synced with Outlook. Teams supports HD video and audio calls with multiple participants, screen sharing of files, whiteboard sharing, and meeting recording.
You can use Teams across all your devices. While we offer rich browser experiences, Teams also has clients for Windows and Mac, and Android and iOS mobile platforms.

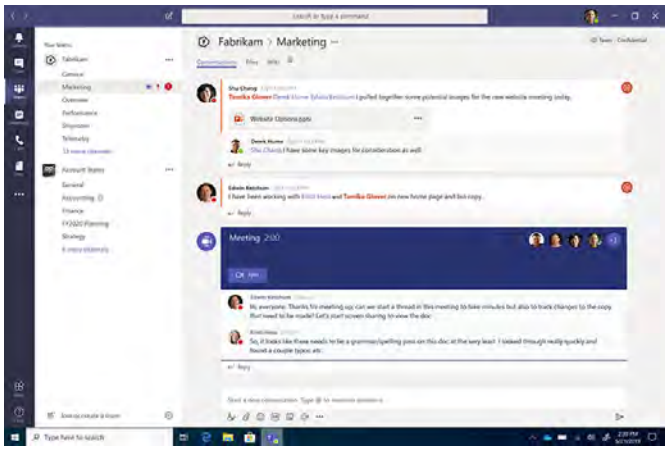
## Access management

Microsoft Teams integrates with your identity and access management system using Azure Active Directory. This allows you to control access and to take advantage of multi-factor authentication and intelligent conditional access. In fact, it gives you unified identity and access management, whether users sit inside or outside of your organization's domain.




## Teams architecture

Microsoft Teams is Your organization will have deployed OneDrive, SharePoint Online, and Exchange Online as part of Microsoft 365. To understand why, here's how this works architecturally. In Microsoft Teams, user folders and files are stored in OneDrive. As you create a team, we automatically create a dedicated Teams site in SharePoint for managing the team's files and content. Calendaring, chat, and contacts are integrated with Exchange Online and Outlook.



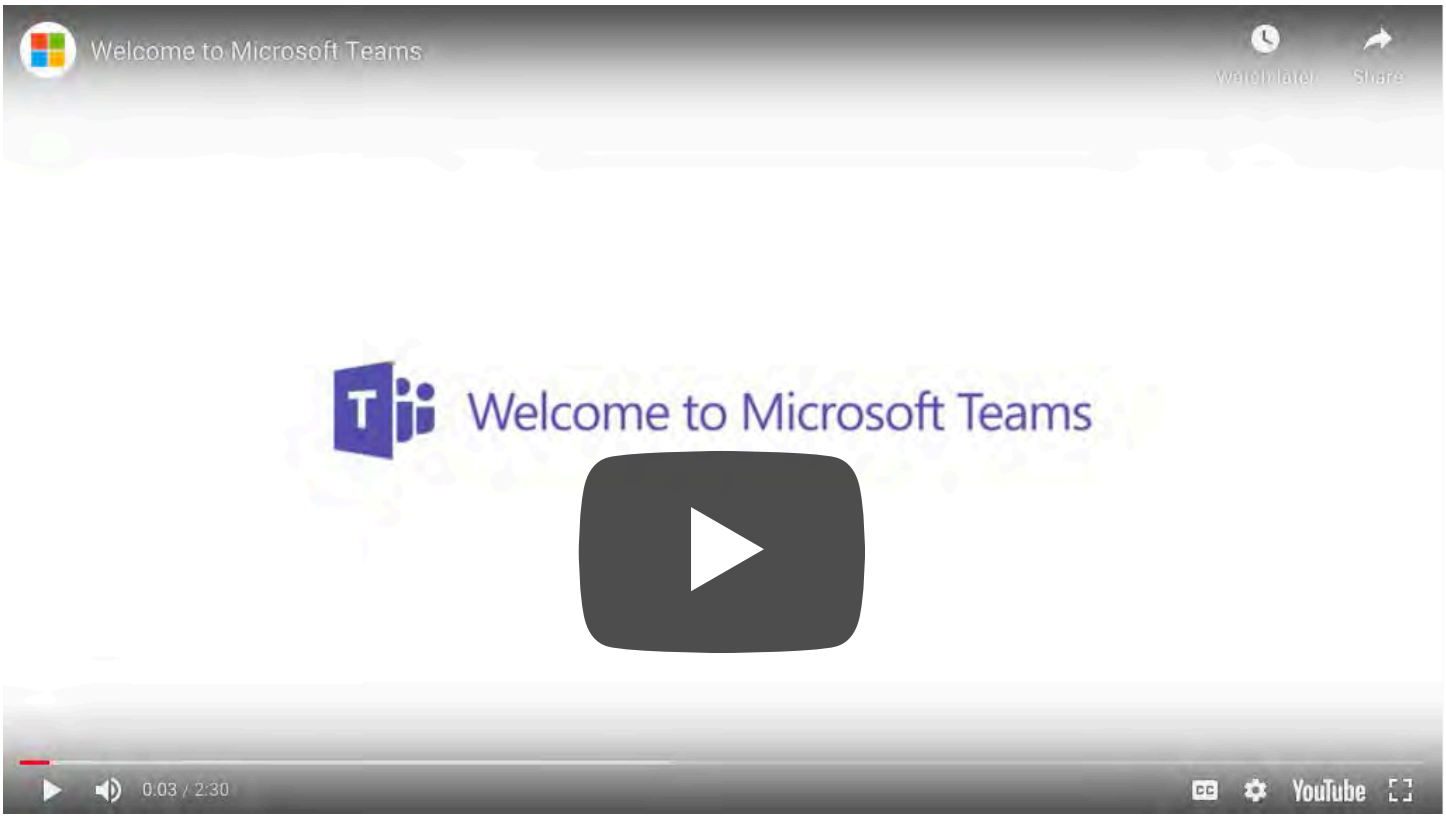

## Data security

Microsoft Teams is built on the Microsoft 365 hyper-scale, enterprise-grade cloud, delivering the advanced security and compliance capabilities our customers expect. As is the case with Microsoft 365, Microsoft Teams is Tier-C compliant, which means it adheres to several national and international security standards, including ISO 27001, ISO 27018, SOC 1 and SOC2, HIPAA, GDPR, and several others. This is important as many consumer-oriented data-sharing, chat, and video conferencing applications do not.

Teams data is encrypted in transit and at rest. Files are stored in SharePoint and are backed by SharePoint encryption. Notes are stored in OneNote and are backed by OneNote encryption. Audio and video calls from within Teams are encrypted in transit too.

# Teams intro video

This short, three-minute video is a good introduction to Teams. This video and dozens more are available from the Help menu within Teams.




## The Teams admin center

As a legal and compliance professional, very likely you won't have Global Admin access to edit settings. However, your Teams administrator can assign you what is called a "Global Reader" role whereby you have read-only access to admin centers. This is a great way to familiarize yourself with the specific security and compliance controls for configuring the core experiences within Teams, including meeting policies and organization-wide settings, such as guest access and more. These are implemented in the Microsoft Teams admin center. The Teams admin center is located here: admin.teams.microsoft.com.

## Team policies

Once you have Global Reader access, you can familiarize yourself with the various controls shown in the left panel of the Teams admin center. We won't cover all the areas listed—only a few that you will want to go over with your Teams administrator. Teams and channel policies are used to control what settings or features are available to users when they are using teams and channels. You can use the Global (Org-wide default) policy and customize it or create one or more custom policies for those people that are members of a team or a channel within your organization.

## Organization-wide configuration settings

Based on your security and compliance needs, organizational culture, or type of industry you're in, you need to think through the org-wide configuration settings that you want to implement. For example, based on regulatory or security needs you can specify the domains of other organizations to either block or allow communication between their users and yours. Likewise, guest access to teams and channels can be configured to provide the right level of sharing and control. For example, you can limit screen sharing to protect sensitive information. Additionally, you can configure which cloud file-sharing services, in addition to OneDrive, you want to allow so that you can make them available in the Teams Files tab.

## Core business apps

Next, think about the core apps running in your business. These can be line-of-business apps such as your expense tool or HR systems or other external apps, like GitHub or Trello. You can customize the Teams experience and policies for your organization and even specific teams by choosing which apps and cloud services can be integrated.

## Communication policies

Beyond apps, you also need to think about the style of communication in your company. Teams offers a rich set of communication policies so that you can configure the user experience in alignment with your corporate standards and organizational culture. You can automate membership to teams so users know where to land. Then, as people begin to work on projects across organizational boundaries, users can create their own teams.

## Managing teams

As adoption takes off, you can manage Teams with visibility into usage across channel and chat messages, calls and meetings, drill down into metrics by user, and get more granular reports with Power BI. Additionally, to help your organization to manage Teams over time, we give you lifecycle management controls. For example, you can edit teams, archive them, or delete them. You can also modify the privacy settings of an active team if needed.

## Extending Teams to partners

Most organizations these days have trusted partners, suppliers, and external contractors. Traditionally, this has been an area of weakness for ensuring security and data integrity. Microsoft Teams offers a robust method of extending Guest access to your partners and tailoring that access to exactly meet your data protection and compliance standards.

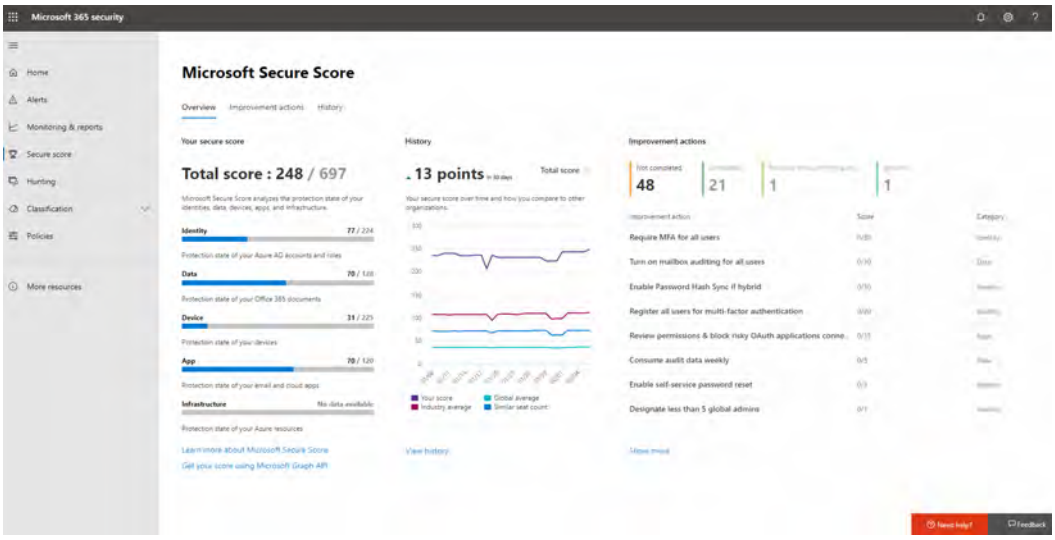
# Advanced security & compliance

Because Teams is part of Microsoft 365, the best approach is to consider Microsoft Teams as another endpoint in your security and compliance strategy.

## Secure Score

Microsoft Teams benefits from the security and compliance foundation of SharePoint, OneDrive, and Exchange, so for the most part, your organization just needs to extend these to your Teams environment. A good place to start is with Secure Score, found in the Microsoft 365 security center. Under "Improvement actions" you will find a list of recommendations in order of importance to improve the security of your environment. We will point out a few that are relevant to Teams.

In a standard installation, the Microsoft 365 security center is located here: security.microsoft.com.




***"When it comes to multi-factor authentication: 100 percent of your employees, 100 percent of the time. The single best thing you can do to improve security for employees working from home is to turn on MFA."***

Ann Johnson, Corporate VP

Cybersecurity Solutions Group

## Multi-factor authentication (MFA)

MFA is probably the most important 'improvement action' you can take, if you haven't already. It can reduce the risk of phishing attacks, including impersonation, by around 99.9%. With MFA, you can require a second form of authentication before a user gets access to Teams, such as a phone call, a text message, or the Microsoft Authentication app on a mobile device. Enabling multi-factor authentication is done in Azure Active Directory.

## Safe links

Back in Secure Score, another great recommendation is configuring Safe Links. This can help you protect your users from impersonation and phishing attacks from weaponized links. This can be configured across Office 365 experiences in the Office 365 Security & Compliance center, under Threat Management policy. Additionally, we have a capability called Safe attachments which, like Safe Links, is part of Office 365 Advanced Threat Protection. You will need to proactively enable this for Teams.

## Data loss prevention

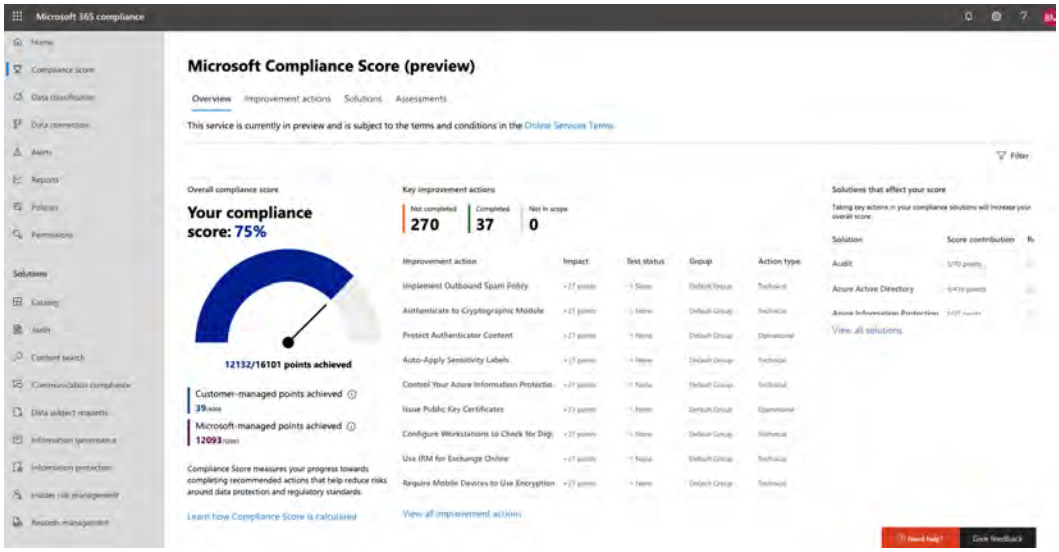
Then, beyond threat protection, another capability that you will see recommended by Secure Score is data loss prevention or DLP. This is central to how we approach information protection across Microsoft 365 including the classification of your data for compliance.

In the case of Teams, with DLP, you can scan chat messages and channel conversations to block the sharing of sensitive data, whereas files in Teams are covered by DLP policies applied to SharePoint. From Secure Score, you get a direct link to enable DLP policies for Teams.

## Compliance Score

Compliance Score is a dashboard within the Microsoft 365 compliance center that provides your overall compliance score and a summary of your data protection and compliance posture. It also includes recommendations to improve data protection and compliance. This is a recommendation; it is up to you to evaluate and validate the effectiveness of customer controls to meet your particular regulatory environment.

In a standard installation, the Microsoft 365 compliance center is located here: compliance.microsoft.com.




## Information Classification

Let's take a look at the top compliance configurations. The first step is to understand the type of information that is in your environment. The new data Classification tab in the Microsoft 365 Compliance Center takes you to an overview page that shows you the volume of sensitive data across your digital estate in Microsoft 365. This can help you streamline the process of figuring out the types of information protection rules you need to apply with DLP. Additionally, Microsoft Teams also honors sensitivity labels created for Office files, OneDrive, and SharePoint.

## Compliance content search

Beyond proactively using DLP and information classification to protect your data and stay compliant, we also give you the ability to reactively search for specific content and understand when it was last accessed and by whom, for regulatory and legal reasons. Using content search, you can filter down to Microsoft Teams only content, such as Chat and Channel Messages, Meetings, and Calls, if necessary.

## eDiscovery

From the Microsoft 365 compliance center, you can set up eDiscovery capabilities. You create your search criteria in the same manner as Content Search and you can select specific locations, such as mailboxes and sites. eDiscovery can be initiated for both private channels and Team channels.

## Retention

Beyond keeping your data for legal reasons, you also need to be able to set the right retention policies to reduce your compliance risk. You can create retention policies in the Microsoft 365 compliance center. Your administrator can set up two types of policies; preservation, which allows you to retain data for a given period of time, even if a user deletes the information from Teams, and deletion.

## Information barriers & communication compliance

Now let's talk about how to manage and monitor the flow of communication in your organization. There are two capabilities that can help you with this; information barriers and communication compliance.

Information barriers help you avoid conflicts of interest, such as insider trading, within your organization by limiting which individuals can communicate and collaborate with each other in Microsoft Teams.

Next, communication compliance in Microsoft 365 helps you minimize communication risks by helping you detect, capture, and take remediation actions for inappropriate messages in your organization.

## Auditing and reporting

Audit log search plugs right into the Microsoft 365 compliance center and gives you the ability to set alerts, as well as report on audit events, by allowing the export of workload-specific or generic event sets for admin use and investigation across an unlimited auditing timeline.

# Wrap-up

This has been a brief introduction to security, data privacy, and compliance controls in Microsoft Teams. As you can see, it is a complex subject that you and your Teams administrator will want to discuss when time permits during or after the current COVID-19 crisis. Our intent is to provide you with some talking points for guiding that discussion and to leave you feeling confident that Microsoft Teams can address your organization's unique security and compliance concerns.

## Sources

Multi-factor authentication: https://aka.ms/mfa
Data Loss Protection: https://aka.ms/DLP
Information Classification: https://aka.ms/infoclassification
eDiscovery: https://aka.ms/M365eDiscovery
Information barriers: https://aka.ms/informationbarriers


Welcome to Microsoft Teams

Security and compliance in Microsoft Teams

Manage teams in the Microsoft Teams admin center

FAQ: Support your remote workforce

Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios

Security and Microsoft Teams

Protect user and device access

Manage app setup policies in Microsoft Teams

Welcome to Microsoft Teams (short video)

Get started with Microsoft Teams (hour-long video)

Security & Compliance in Microsoft Teams: Cloud App Security and Azure Active Directory (video)

## Admin center links

Once logged in as either a Global Admin or Global Reader, here are the links to the various admin centers. Note that they may not all be available to you, depending on your particular Microsoft license.

Microsoft Teams admin center https://admin.teams.microsoft.com/

Microsoft 365 admin center https://admin.microsoft.com/

Microsoft 365 compliance center https://compliance.microsoft.com/

Microsoft 365 security center https://security.microsoft.com/