

Part 1 – Overview

(Modern Work & Purview)

Contents

- Disclaimer..... 2
- Target Audience 2
- Document Scope 2
- Out-of-Scope 2
- Parts of this Blog series 3
- Here are the parts of the blog series: 3
- Mapping Purview tools to the CIA triad..... 4
- Mapping Purview tools to Information Lifecycle Management (ILM)..... 6
- Modern Work and Purview workloads 8
- Mapping Modern Work workloads to ILM 8
- Next Steps 9
- Appendix and Links 9

Before we start, please note that if you want to see a table of contents for all the sections of this blog, you can locate them at the following URL:

[Microsoft Purview and Modern Work \(Part 1\) - Overview](#)

Disclaimer

This document is not meant to replace any official documentation, including those found at docs.microsoft.com. Those documents are continually updated and maintained by Microsoft Corporation. If there is a discrepancy between this document and what you find in the Compliance User Interface (UI) or inside of a reference in docs.microsoft.com, you should always defer to that official documentation and contact your Microsoft Account team as needed. Links to the docs.microsoft.com data will be referenced both in the document steps as well as in the appendix.

All of the following steps should be done with test data, and where possible, testing should be performed in a test environment. Testing should never be performed against production data.

Target Audience

The Information Life Cycle Management section of this blog series is aimed at Security and Compliance and Modern Work officers who need to properly label data, encrypt it where needed.

Things to Consider (as relates to your role and/or organization)

Here are a few questions for you to consider before you read this blog series. If these questions or questions like them do not relate to your role or organization, then this blog series might not be meant for you.

- What are your data security goals?
- What are your Data Retention needs, either as an organization or within your industry?
- Do you have Data Leakage (accidental removal of data) concerns?
- Do you have Data Theft (removal of data on purpose) concerns?
- What are your organization's data security policies?
- What are your industry's data security policies?

Document Scope

This blog article is meant to help an IT administrator who is looking to secure their data throughout the lifecycle of the data.

It is presumed that you already have a basic understanding of the Purview tools and the Modern Work tools (including Exchange, Teams, SharePoint and OneDrive).

Out-of-Scope

This document does not cover configuring any of the below, ie. Holding your hand through the process of configuration", as that is covered via other blogs, official Microsoft documents, or through the aid of Microsoft implementation teams or Microsoft partners:

- Audit
- Communications Compliance
- Compliance Manager
- Data Classification (Sensitive Information Types)
- Data Classification (Exact Data Matching)
- Data Classification (Trainable Classifiers)
- Data Lifecycle Management (retention and disposal)
- Data Protection Loss (DLP) for Exchange, OneDrive, Devices, etc
- Information Barriers
- Information Protection (labeling, encrypting, watermarking, etc of files)
- Insider Risk Management
- Microsoft Defender for Cloud Apps (MDCA)
- Privacy Management (Priva)
- Records Management (retention and disposal)
- Standard or Premium eDiscovery

Parts of this Blog series

Here are the parts of the blog series:

Part 1 – [Overview of the blog series](#)

Part 2 – [Collaboration Overview](#)

Part 2a – [SharePoint Sites and Files](#)

Part 2b – [OneDrive Files](#)

Part 2c – [Teams Sites and Files](#)

Part 3 – [Communication Overview](#)

Part 3a – [Exchange Email Messaging](#)

Part 3b – [Teams Chats and Streams](#)

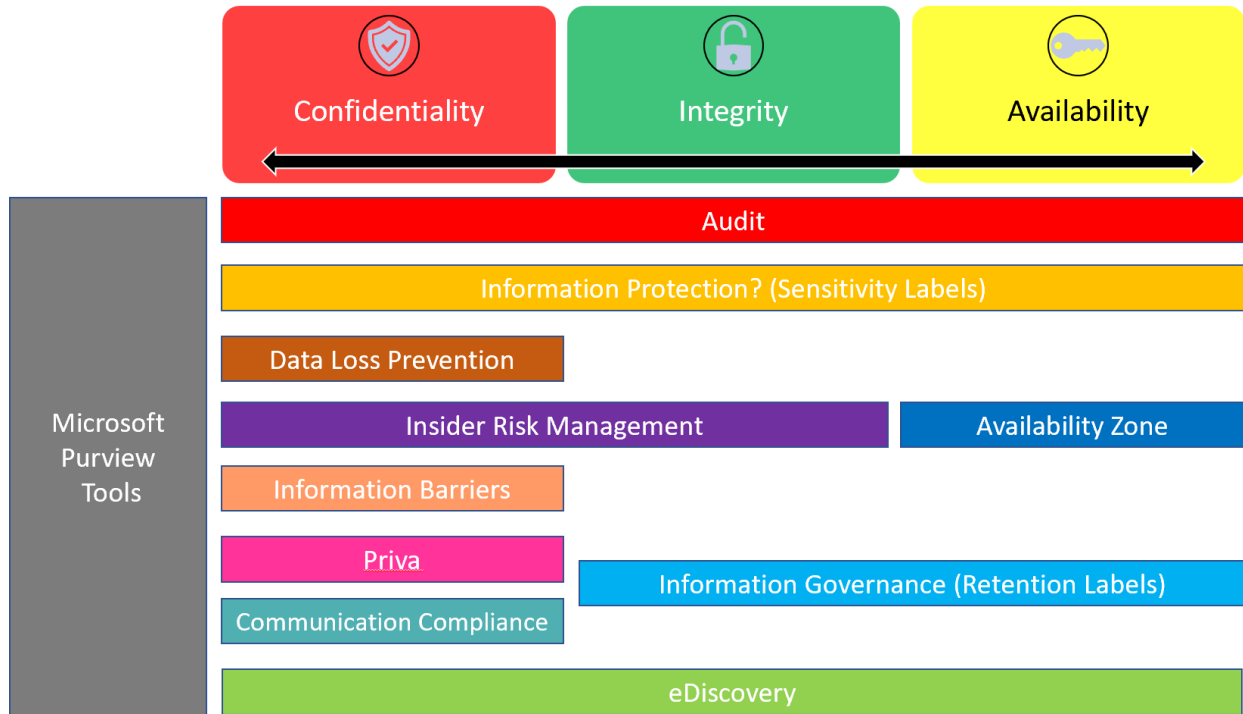
Mapping Purview tools to the CIA triad

If we want to measure have a tool to help quantify the security of our data, the CIA triad (Confidentiality, Integrity, Availability) is a good place to start. Our goal as an organization should be to get our data within the center of the triad.

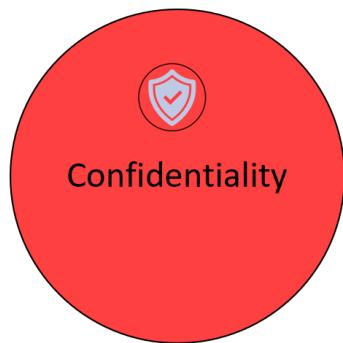


Let us take the CIA triad and map it to the various components of Microsoft Purview to the CIA triad. Here are two different “mappings” to try and help you visualize how the current Purview tools map to the CIA triad

Mapping Visualization #1



Mapping Visualization #2



Microsoft Purview Tools

- Audit
- Information Protection
- Insider Risk Management
- eDiscovery (HR and Legal)
- DLP
- Priva (out-of-scope of this blog)
- Information Barriers
- Communication Compliance
- Compliance Manager (out-of-scope of this blog)



Microsoft Purview Tools

- Audit
- Information Governance
- Information Protection
- Insider Risk Management
- eDiscovery (forensics)
- Compliance Manager (out-of-scope of this blog)



Microsoft Purview Tools

- Audit
- Information Governance
- Information Protection?
- Availability Zones
- Compliance Manager (out-of-scope of this blog)

Note – when it comes to Availability, backup tools should always be considered. However, Microsoft does protect the data inside of your tenant. Here are 2 links on this topic. There are more in the Appendix and Links section below.

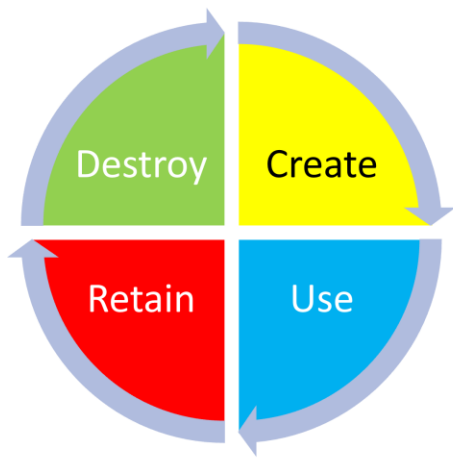
- [Microsoft 365 data locations - Microsoft 365 Enterprise | Microsoft Learn](#)
- [Data Resiliency in Microsoft 365 - Microsoft Service Assurance | Microsoft Learn](#)

As we dig into the different workloads around Collaboration and Communication, we will revisit the CIA triad so you can see how each tool helps protect your data during its Information Lifecycle. Now let us move to the next section and talk about how the Information Lifecycle maps to Purview Tools.

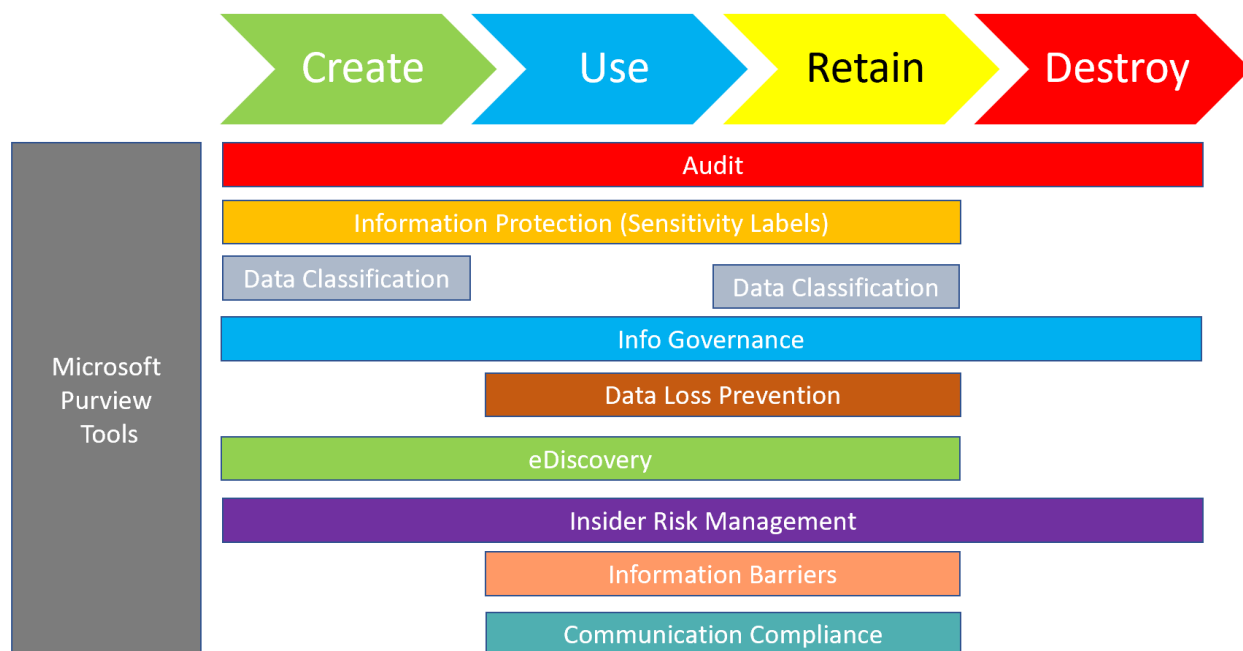
Mapping Purview tools to Information Lifecycle Management (ILM)

Information Lifecycle Management (ILM) is standard way of looking at data within an organization. The process as diagramed below, 1) starts with the creation of data, 2) use of data, 3) retention of data and 4) deletion of data. There are many government regulations (ex. HIPAA, SOX, GDPR, etc) that dictate how data is protected, retained, and disposed of. There are also internal, organizational regulations driven by HR and Legal teams that dictate how data is protected, retained, and disposed of.

1. Create – this is the creation of the file, site, chat, email, or folder.
2. Use – this is the modification or sharing of the data.
3. Retain – this is when the data has gone static/passive and is no longer being modified or shared by the end users.
4. Destroy – this is the elimination of the data from the organization to meet organization or government regulations/requirements.



Now let us map the Information Lifecycle to the components of Microsoft Purview (as noted above, this will not be an exhaustive list of components at this point in the blog).



Modern Work and Purview workloads

These are the Modern Work workloads we will cover in this blog series

1. Collaboration
2. Communications

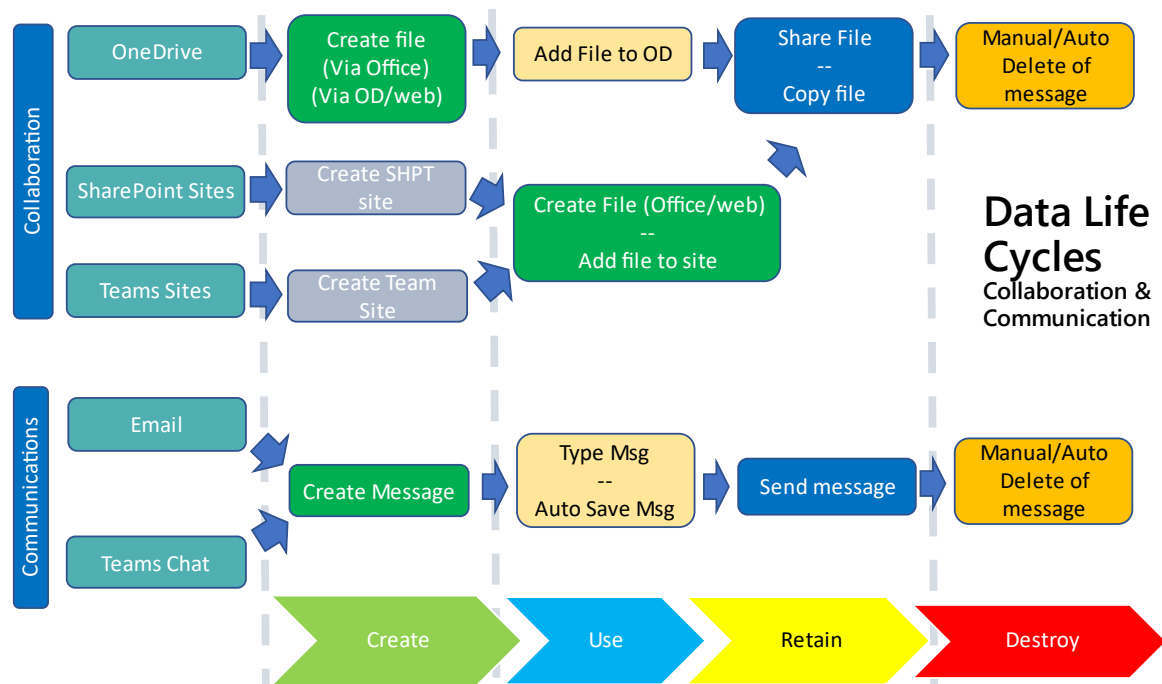
Inside of these 2 workloads are technology-based applications.

1. Collaboration –this involves data sharing (ie. Files, folders, SharePoint sites, OneDrive data, Teams sites, etc). For this blog, I will focus on the following 3 items:
 - a. SharePoint sites and files
 - b. OneDrive files
 - c. Teams’ sites and files
2. Communications – This means things such as Teams chats and Exchange email messages. For this blog, I will focus on the following:
 - a. Exchange Email Messaging
 - b. Teams Chats and Streams

Mapping Modern Work workloads to ILM

When looking at the lifecycle of data (Create – Use – Retain – Destroy) we need to map it, at least at a high level, to the Microsoft Collaboration and Communication tools and the data they generate.

Here is a visual map to get you thinking about this.



Next Steps

Now that we have mapped Lifecycle Management to the Microsoft Collaboration and Communications, we can map Purview tools and workloads to specific Modern Work data flows. We cover these in more depth Parts 2 and 3 of this blog series.

Appendix and Links

- [Microsoft Purview compliance documentation - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Microsoft Purview risk and compliance solutions - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Introduction to Azure security | Microsoft Learn](#)
- [Azure's Well-Architected Framework | Pillar 5: Security - US Partner Community Blog - Microsoft](#)
- [Talk:CIA triad - Wikipedia](#)
- [Application lifecycle management - Wikipedia](#)

- [Learn about Microsoft Purview Data Lifecycle Management - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Microsoft Purview Data Lifecycle Management | Microsoft Security](#)
- [Use Microsoft Teams for collaboration - Microsoft 365 Business Premium | Microsoft Learn](#)
- [What is OneDrive? \(work or school\) - Microsoft Support](#)
- [Welcome to Microsoft Teams - Microsoft Teams | Microsoft Learn](#)
- [Overview of teams and channels in Microsoft Teams - Microsoft Teams | Microsoft Learn](#)
- [Overview of Exchange services on Exchange servers | Microsoft Learn](#)
- [Introduction to SharePoint and OneDrive - SharePoint in Microsoft 365 | Microsoft Learn](#)
- [Should I Backup My Microsoft 365 data? - Microsoft Community](#)
- [Cloud Data Integrity at its Finest | Microsoft Trust Center](#)
- [Microsoft 365 data locations - Microsoft 365 Enterprise | Microsoft Learn](#)
- [Data Resiliency in Microsoft 365 - Microsoft Service Assurance | Microsoft Learn](#)
- [Exchange Online Data Resiliency in Microsoft 365 - Microsoft Service Assurance | Microsoft Learn](#)
- [SharePoint and OneDrive data resiliency in Microsoft 365 - Microsoft Service Assurance | Microsoft Learn](#)