

Part 2b – Collaboration – OneDrive

(Modern Work & Purview)

Contents

| | |
|---|-------------------------------------|
| Disclaimer..... | 1 |
| Document Scope..... | 2 |
| Out-of-Scope..... | 2 |
| Notes..... | 2 |
| Mapping Purview to OneDrive..... | 3 |
| Mostly done – Pre-data Creation – Links needed..... | Error! Bookmark not defined. |
| Mostly done – Create (data) – Links needed..... | Error! Bookmark not defined. |
| Mostly done – Use & Retain (data) – Links needed..... | Error! Bookmark not defined. |
| Mostly done - Destroy (data) – Links needed..... | Error! Bookmark not defined. |
| Next Steps..... | 11 |
| Not Done – Appendix and Links..... | Error! Bookmark not defined. |
| Blog Labels..... | Error! Bookmark not defined. |

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.

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

Notes

After each section of this blog, I will make a note of which of the 3 parts of the CIA Triad that Microsoft tool will help you meet. Here are a few examples.

Example #1 –  CIA component – Integrity & Availability

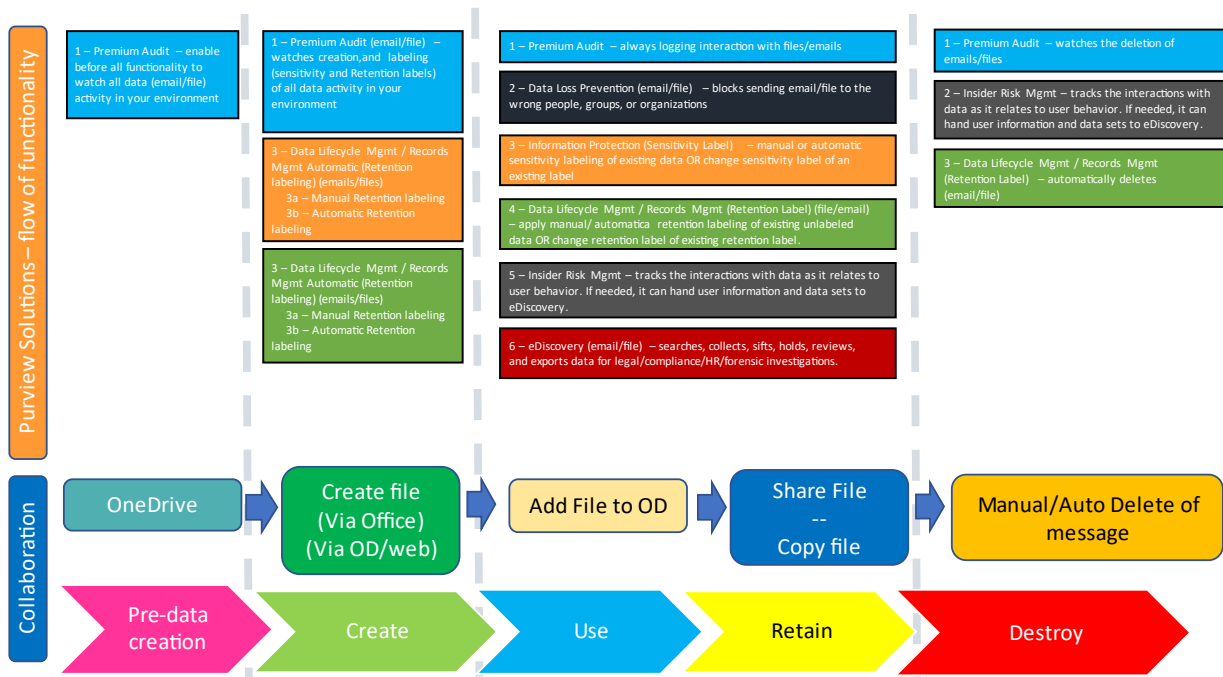
Example #2 –  CIA component – Confidentiality & Availability

Example #3 –  CIA component – Integrity

Mapping Purview to OneDrive

For this part of the blog, I have broken down the Purview workloads, mapped them to the OneDrive activity, and then mapped those to the corresponding stage of the Information Lifecycle.

Here is the high-level view of this mapping.



Please note I've added a new stage to the Information Lifecycle and called it Pre-data creation. This was done to help show that Microsoft Auditing is always enabled within your Microsoft tenant.

After each Purview workload, you will find a CIA triad "indicator" to show which part of the triad Purview is supported. In addition, you will also find assorted links to assorted Microsoft documents or blog postings that can help you enable that functionality in your environment, presuming you are appropriately licensed.

Pre-data Creation

1. Premium Audit (email/file) – It is recommended that this be enable before all functionality to watch all data activity in your environment.



CIA component – Confidentiality & Integrity

1 – Premium Audit – enable before all functionality to watch all data (email/file) activity in your environment

Create (data)

1. Premium Audit (email/file) – This watches the creation, user, searching, labeling (sensitivity and Retention labels), etc. of all data in your tenant.



CIA component – Confidentiality & Integrity

2. Information Protection (Sensitivity Label) (email/file/site) – This tool applies encryption, watermarking, access, editing, etc. based on a user's credentials either in your tenant or associated with your tenant. There are two ways that this tool can apply labels:
 - a. Automatic Sensitivity labeling – This is done by the tool reasoning over data that exists or being created and applies a sensitivity label based on what it finds.
 - b. Manual Sensitivity labeling – This is done by the user who applies a sensitivity label based what they see or have placed in that file/email.



CIA component – Confidentiality & Integrity

3. Data Lifecycle Management / Records Management (Retention Label) (email/file) – This tool applies retention based on what is inside of an email/file. There are two ways that this tool can apply labels:
 - a. Automatic Retention labeling - This is done by the tool reasoning over data that exists or being created and applies a retention label based on what it finds.
 - b. Manual Retention labeling – This is done by the user who applies a retention label based what they see or have placed in that file/email.

[Learn about Microsoft Purview Data Lifecycle Management - Microsoft Purview \(compliance\) | Microsoft Learn](#)

[Records management for documents and emails in Microsoft 365 - Microsoft Purview \(compliance\) | Microsoft Learn](#)

[Microsoft Purview - Paint By Numbers Series \(Part 4\) - Records Management - Microsoft Community Hub](#)



CIA component – Integrity

1 – Premium Audit (email/file) – watches creation, and labeling (sensitivity and Retention labels) of all data activity in your environment

3 – Data Lifecycle Mgmt / Records Mgmt Automatic (Retention labeling) (emails/files)
3a – Manual Retention labeling
3b – Automatic Retention labeling

3 – Data Lifecycle Mgmt / Records Mgmt Automatic (Retention labeling) (emails/files)
3a – Manual Retention labeling
3b – Automatic Retention labeling

Use & Retain (data)

1. Premium Audit (email/file) – This is always logging interactions with files/emails.

[Microsoft Purview Audit \(Premium\) - Microsoft Purview \(compliance\) | Microsoft Learn](#)



CIA component – Confidentiality & Integrity

2. Data Loss Prevention (email/file) – This blocks sending emails/chats/data/files to the wrong individuals or organizations.
 - a. Example - your organization and your organization’s primary competitor.

[Learn about data loss prevention - Microsoft Purview \(compliance\) | Microsoft Learn](#)

[Microsoft Purview - Paint By Numbers Series \(Part 3\) - Data Loss Protection for Exchange - Microsoft Community Hub](#)



CIA component – Confidentiality & Integrity

3. Information Protection (Sensitivity Labels) – This allows for manual/automatic sensitivity labeling of existing data OR changing sensitivity label of an existing label.
 - a. An example of this would be encrypting files so only your Business partners can read the files using a user profile associated with your Azure Active Directory. All other credentials, personal, competitor, etc. would be blocked from accessing the data.

[Learn about sensitivity labels - Microsoft Purview \(compliance\) | Microsoft Learn](#)

[Microsoft Purview- Paint By Numbers Series \(Part 2\)- Information Protection - Microsoft Community Hub](#)



CIA component – Confidentiality & Integrity

4. Data Lifecycle Management / Records Management (Retention label) (file/email) – These tools provide for either manual or automatic retention labeling of existing unlabeled data OR change the retention label of existing labels.
 - a. Examples include applying a 7 year retention to PHI for HIPAA regulations, or changing a 7 year retention label to a 3 year retention when data within a file has been changed.

[Learn about Microsoft Purview Data Lifecycle Management - Microsoft Purview \(compliance\) | Microsoft Learn](#)

[Records management for documents and emails in Microsoft 365 - Microsoft Purview \(compliance\) | Microsoft Learn](#)

[Microsoft Purview - Paint By Numbers Series \(Part 4\) - Records Management - Microsoft Community Hub](#)



CIA component – Integrity

5. Insider Risk Management (email/file) – This tool tracks data movement, deletion, changes in labels, exfiltration, etc and maps it to user behavior. If needed, this tool can hand collected information (emails, files, users name, etc) to eDiscovery as a case.
 - a. An example of this would be a user tendering their resignation, and you see a sudden spike in their downloading corporate data to a USB stick.

[Learn about insider risk management - Microsoft Purview \(compliance\) | Microsoft Learn](#)

[Microsoft Purview - Paint By Numbers Series \(Part 6\) – Insider Risk Management - Overview - Microsoft Community Hub](#)



CIA component – Confidentiality

6. eDiscovery (email/file) – With this tool you can search, collect, sift, hold, review, and export data for legal/compliance/HR/forensics investigations.

[Microsoft Purview eDiscovery solutions - Microsoft Purview \(compliance\) | Microsoft Learn](#)

[Microsoft Purview - Paint By Numbers Series \(Part 5\) - Advanced eDiscovery - Microsoft Community Hub](#)



CIA component – Integrity

1 – Premium Audit – always logging interaction with files/emails

2 – Data Loss Prevention (email/file) – blocks sending email/file to the wrong people, groups, or organizations

3 – Information Protection (Sensitivity Label) – manual or automatic sensitivity labeling of existing data OR change sensitivity label of an existing label

4 – Data Lifecycle Mgmt / Records Mgmt (Retention Label) (file/email) – apply manual/automatic retention labeling of existing unlabeled data OR change retention label of existing retention label.

5 – Insider Risk Mgmt – tracks the interactions with data as it relates to user behavior. If needed, it can hand user information and data sets to eDiscovery.

6 – eDiscovery (email/file) – searches, collects, sifts, holds, reviews, and exports data for legal/compliance/HR/forensic investigations.

Destroy (data)

1. Premium Audit (email/file) – This watches the deletion of emails/files.

[Microsoft Purview Audit \(Premium\) - Microsoft Purview \(compliance\) | Microsoft Learn](#)



CIA component – Confidentiality & Integrity

2. Insider Risk Management (email/file) – This tool tracks data movement, deletion, changes in labels, exfiltration, etc. and maps it to user behavior. If needed, this tool can hand collected information (emails, files, users name, etc) to eDiscovery as a case.

[Learn about insider risk management - Microsoft Purview \(compliance\) | Microsoft Learn](#)



CIA component – Confidentiality

3. Data Lifecycle Management / Records Management (Retention label) (file/email) – These tools provide for either manual or automatic retention labeling of existing unlabeled data OR change the retention label of existing labels.

[Learn about Microsoft Purview Data Lifecycle Management - Microsoft Purview \(compliance\) | Microsoft Learn](#)

[Records management for documents and emails in Microsoft 365 - Microsoft Purview \(compliance\) | Microsoft Learn](#)

[Microsoft Purview - Paint By Numbers Series \(Part 4\) - Records Management - Microsoft Community Hub](#)



CIA component – Integrity

1 – Premium Audit – watches the deletion of emails/files

2 – Insider Risk Mgmt – tracks the interactions with data as it relates to user behavior. If needed, it can hand user information and data sets to eDiscovery.

3 – Data Lifecycle Mgmt / Records Mgmt (Retention Label) – automatically deletes (email/file)

Next Steps

We will now move to look at Teams and specific Purview workloads that can be mapped to data within that platform.

Appendix and Links

- [Learn about insider risk management - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Learn about communication compliance - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Learn about data loss prevention - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Microsoft Purview Compliance Manager - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Microsoft Purview eDiscovery solutions - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Microsoft Purview Audit \(Premium\) - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Learn about Microsoft Purview Data Lifecycle Management - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Records management for documents and emails in Microsoft 365 - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Learn about information barriers - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Learn about sensitivity labels - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Learn about Microsoft Priva - Microsoft Priva | Microsoft Learn](#)
- [Microsoft Purview- Paint By Numbers Series \(Part 2\)- Information Protection - Microsoft Community Hub](#)
- [Microsoft Purview - Paint By Numbers Series \(Part 3\) - Data Loss Protection for Exchange - Microsoft Community Hub](#)
- [Microsoft Purview - Paint By Numbers Series \(Part 6\) – Insider Risk Management - Overview - Microsoft Community Hub](#)
- [Microsoft Purview - Paint By Numbers Series \(Part 4\) - Records Management - Microsoft Community Hub](#)

- [Microsoft Purview - Paint By Numbers Series \(Part 5\) - Advanced eDiscovery - Microsoft Community Hub](#)
- [Microsoft Purview - Paint By Numbers Series \(Part 8a\) - Information Barriers and Team Chat - Microsoft Community Hub](#)
- [Microsoft Purview- Paint By Numbers Series \(Part 0\) - Overview - Microsoft Community Hub](#)