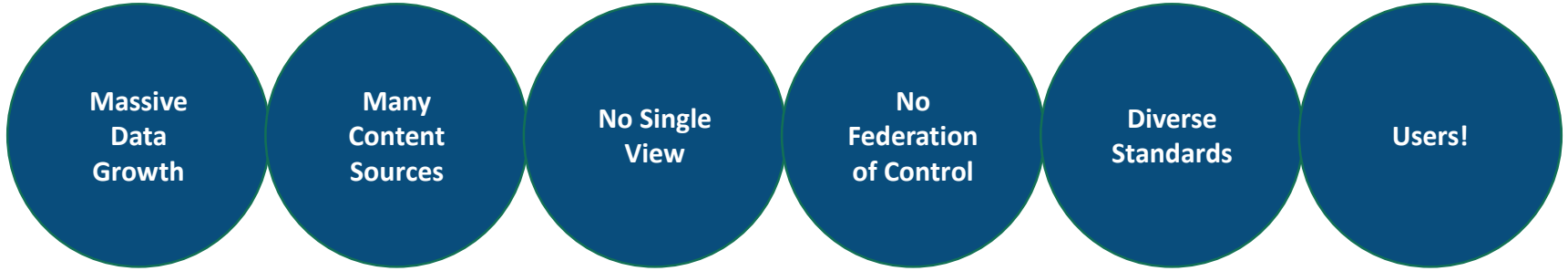
Understanding Compliance in Office 365

Introduction to Records Management & Retention

WaTech
Washington Technology Solutions

The Compliance Problem



"My data is scattered across many sources and growing fast"

"It's impossible to know what I have, let alone apply policy"

"My users aren't interested in compliance"

"How can I identify and protect sensitive information?"

"I want policy to be universal, automatic, and based on content"

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Records Principles

EASY

- Reduce complexity for record creators
- Employees are not compliance experts
- Seamlessly manage content across multiple repositories
- In-place records management across cloud and on-prem

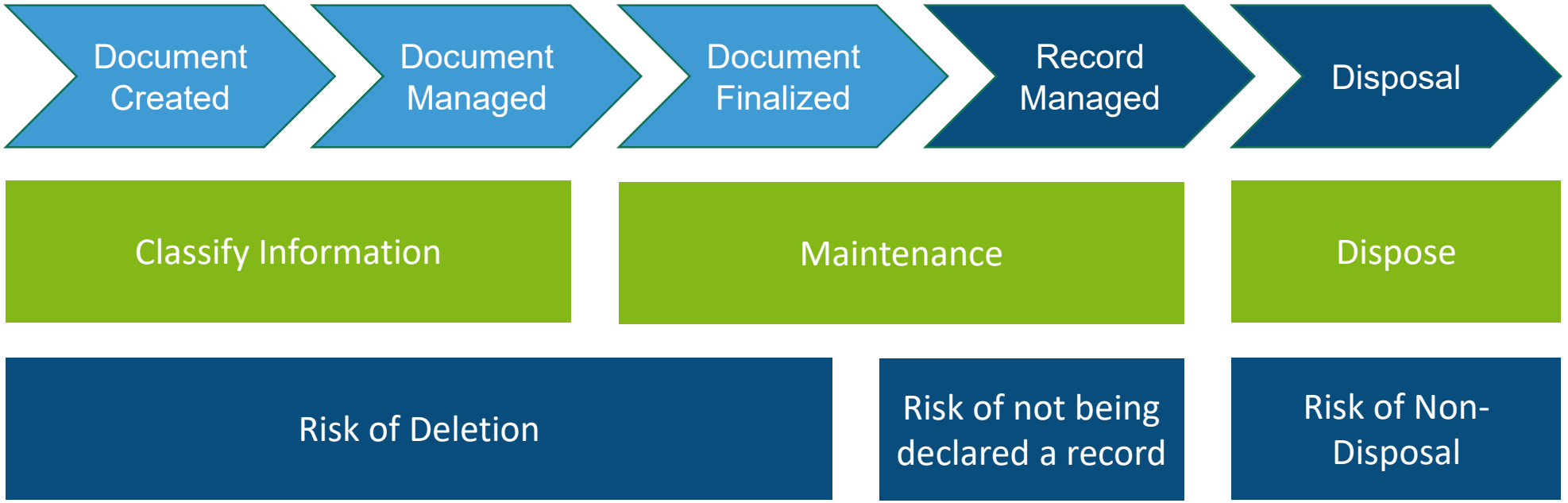
MODERN

- Automated rules engine classifies content
- Extensible connector framework (e.g. O365, Azure, AWS, ECMs)
- Federated data management
- Retire legacy systems and enable the modern workplace

TRUSTED

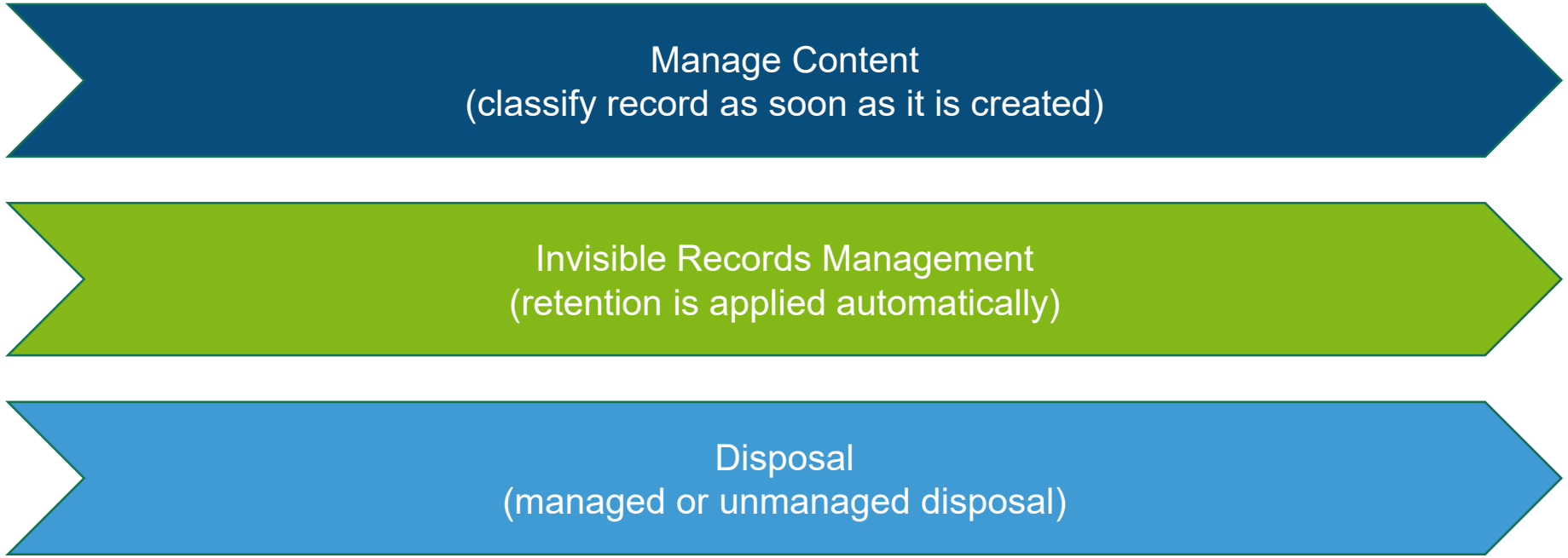
- Compliant with local, state, federal, and global standards (e.g. WPA, GDPR, CCPA)
- Maintain data onshore to meet data sovereignty compliance
- Certified on security and operation standards (e.g. HIPAA, CJIS, FedRAMP)

Traditional Records Management



WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Modern Records Management



Microsoft 365 Compliance Features

Retention

Retention policies are applied automatically when content is created

Labeling

Enable your users to apply a retention manually to content

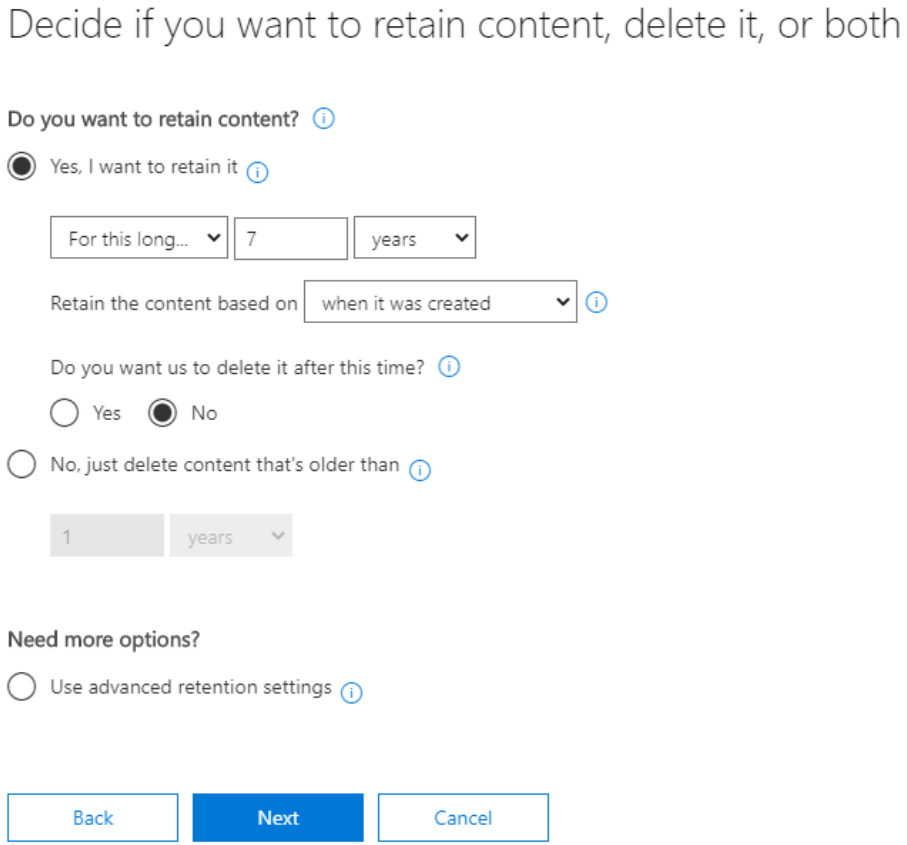
eDiscovery

Identify, collect, and produce electronic records

Retention Policies

A Retention Policy is separate from a Label and provides an overall retention to a location. It can do the following:

- Delete content automatically.
- Retain content for a specific time period.
- Delete content once a retention period has passed.
- Do nothing.
- Start the retention period from when content was created or last modified.



How To Create Retention Policy

Name the Policy

- Name
- Description

Configure Retention Settings

- Define retention period
- Select trigger date field
- Choose how to delete
- Set advanced retention settings

Choose Locations

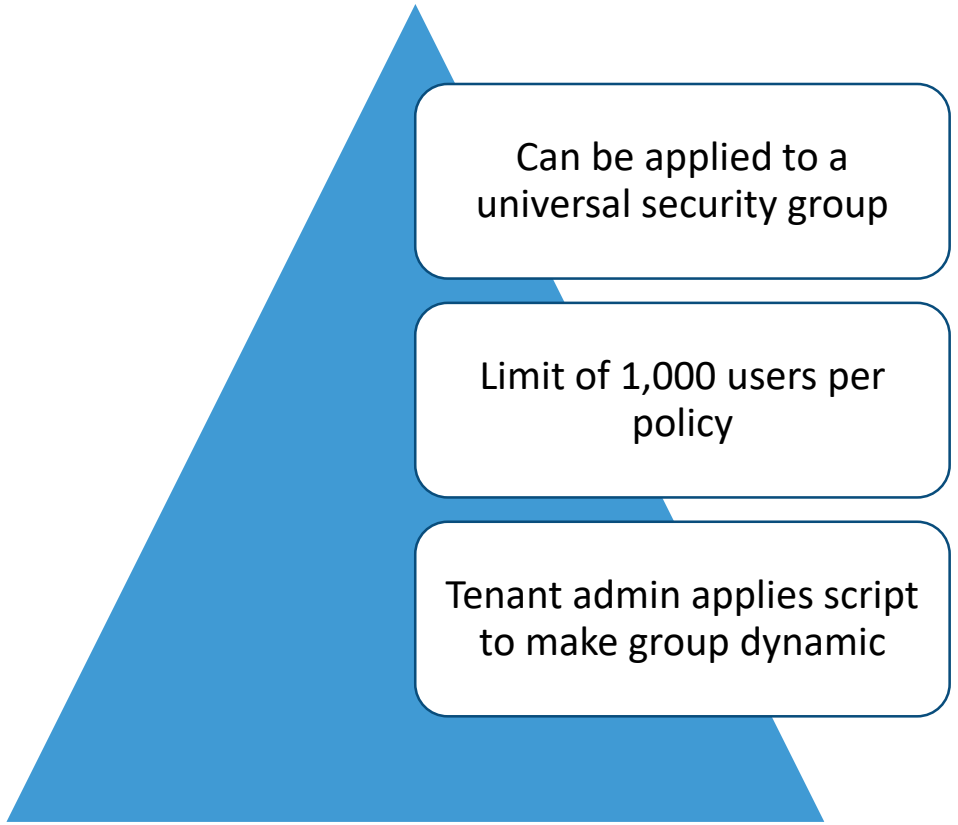
Choose where the retention policy will be deployed by M365

Retention Policy Location Deployment

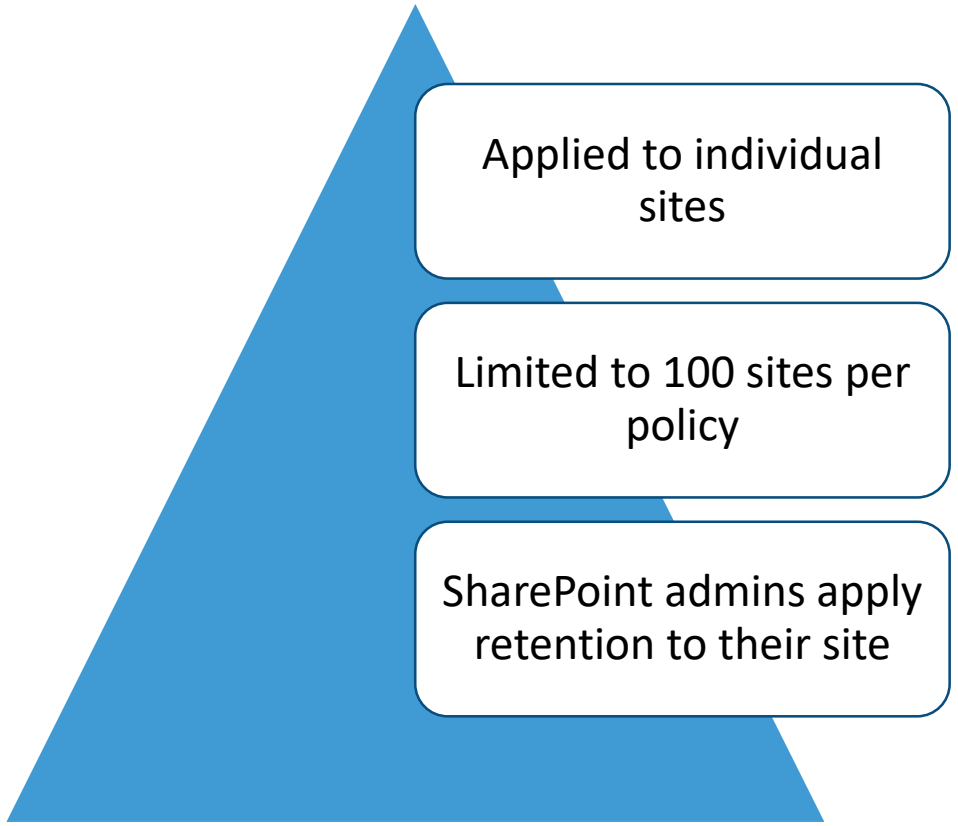
Retention policies can be deployed to specific locations or the entire organization.

	Office 365 Locations							
Entire Locations	Exchange Email	SharePoint	OneDrive	O365 Groups	Skype for Business	Exchange Public Folders	Teams Channel Messages	Teams Chats
Include or Exclude	Recipients (up to 1000)	Sites (up to 100 sites)	Accounts (up to 100)	Groups (up to 1000)		All or None		

Exchange Online Retention Policy



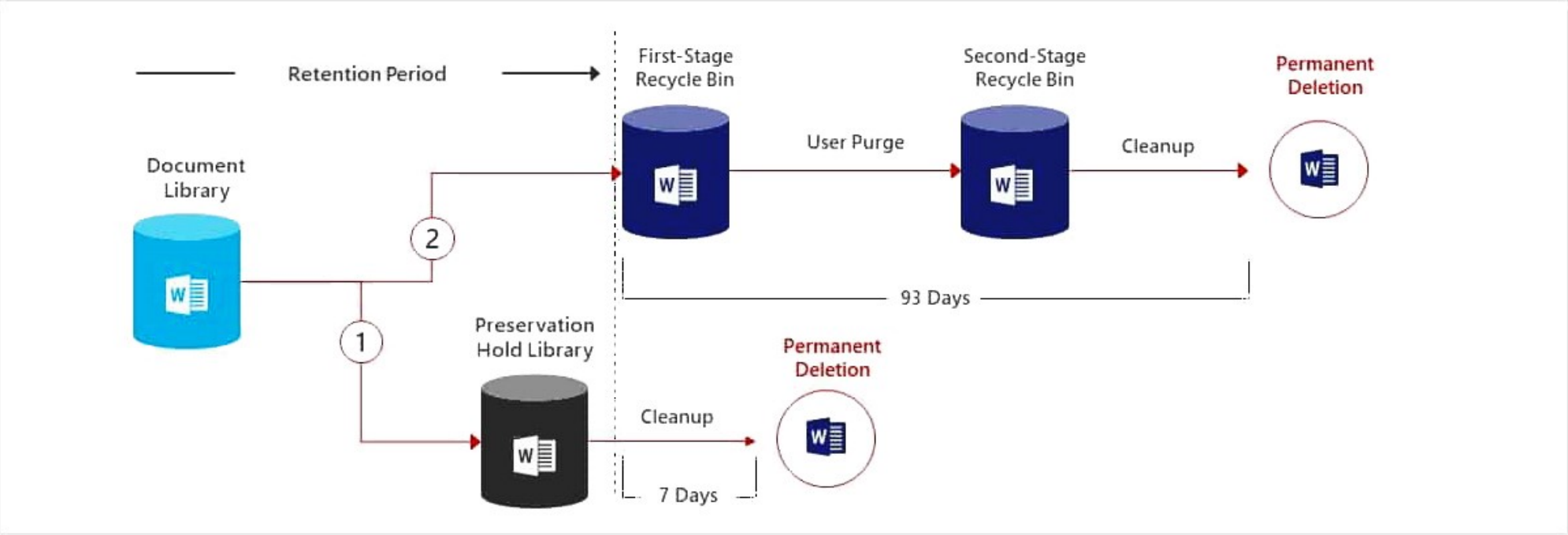
SharePoint Retention Policy



The Principles of Retention

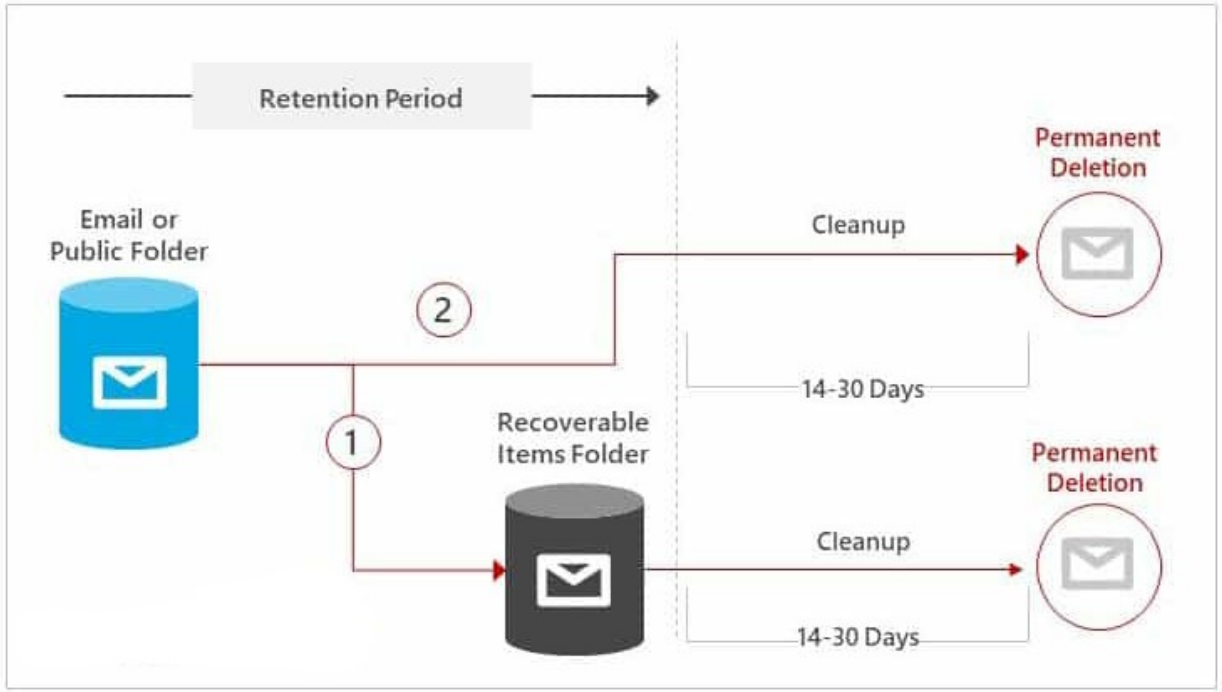
- Retention wins over deletion
- Longest retention period wins
- Explicit inclusion wins over implicit inclusion
- Shortest deletion period wins

How Deletion Works in SharePoint and OneDrive



1. If the content is modified or deleted during the retention period
2. If the content is not modified or deleted during the retention period

How Deletion Works in Exchange and Public Folders

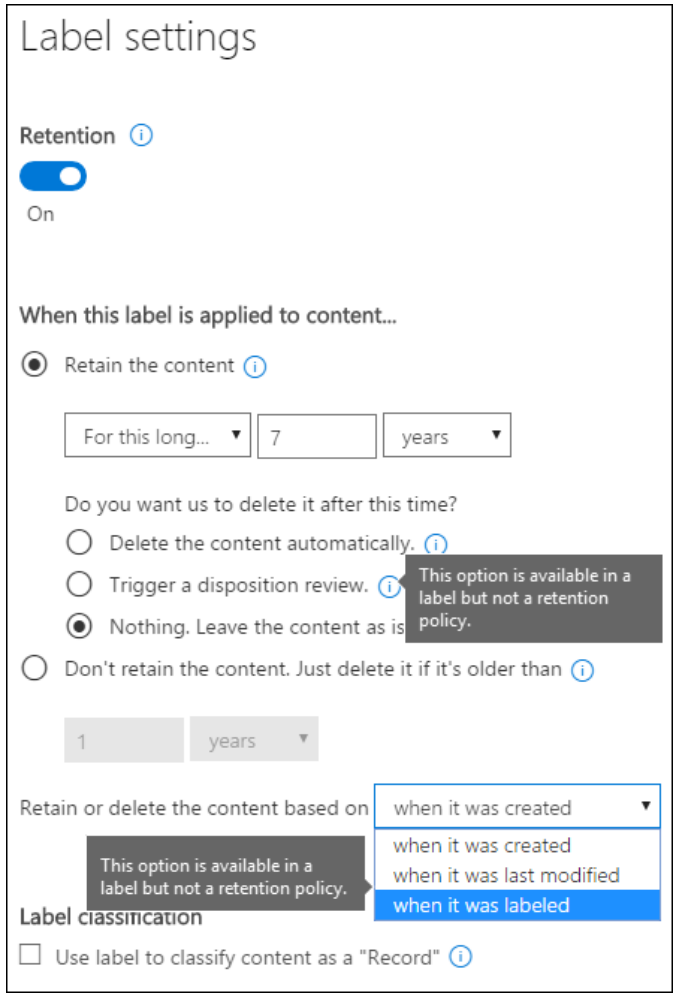


1. **If the content is modified or permanently deleted** by the user during the retention period
2. **If the content is not modified or deleted** during the retention period

Retention Labels

Labels classify documents and can apply retention. They can do the following:

- Delete content automatically.
- Retain content for a specific time period.
- Delete content once a retention period has passed.
- Trigger a disposition review.
- Do nothing.
- Start the retention period from when content was created, last modified, when the label was applied, or when an event occurred.



How To Create a Label

Create a Label

Name
Description
Retention Settings

Deploy Label Using a Label Policy

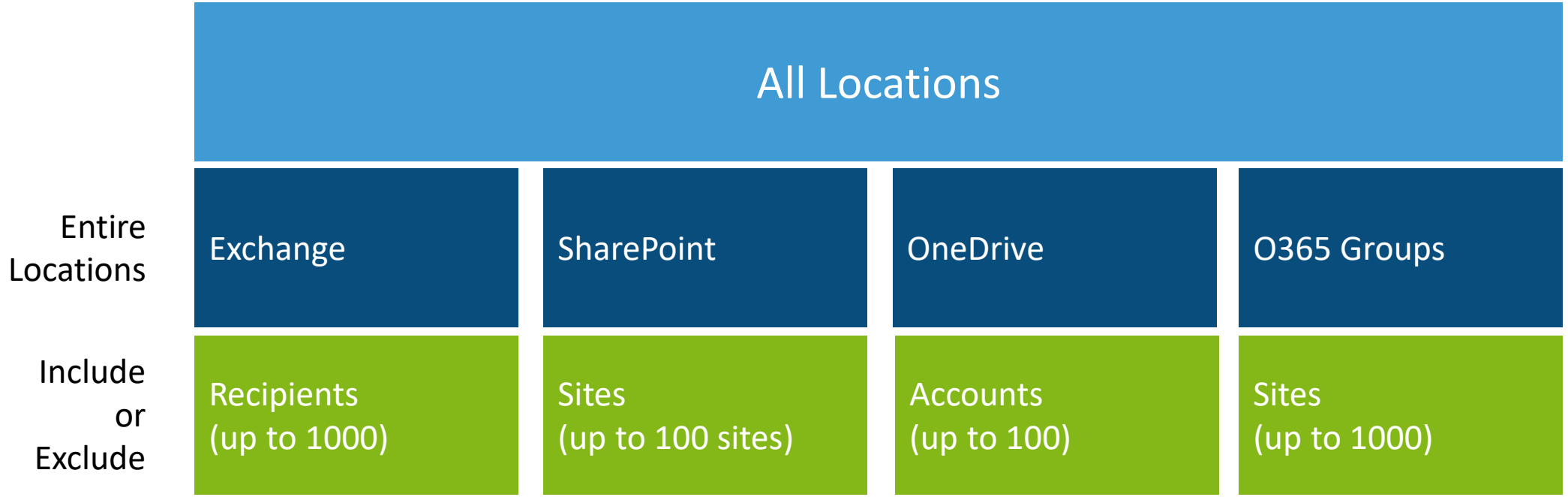
Publish to a specific location and group
Automatically apply label

Apply Label Policy to AD Group

Use custom PowerShell script to read membership of group and apply label

Labels Location Deployment

Can be deployed to specific locations or the entire organization.



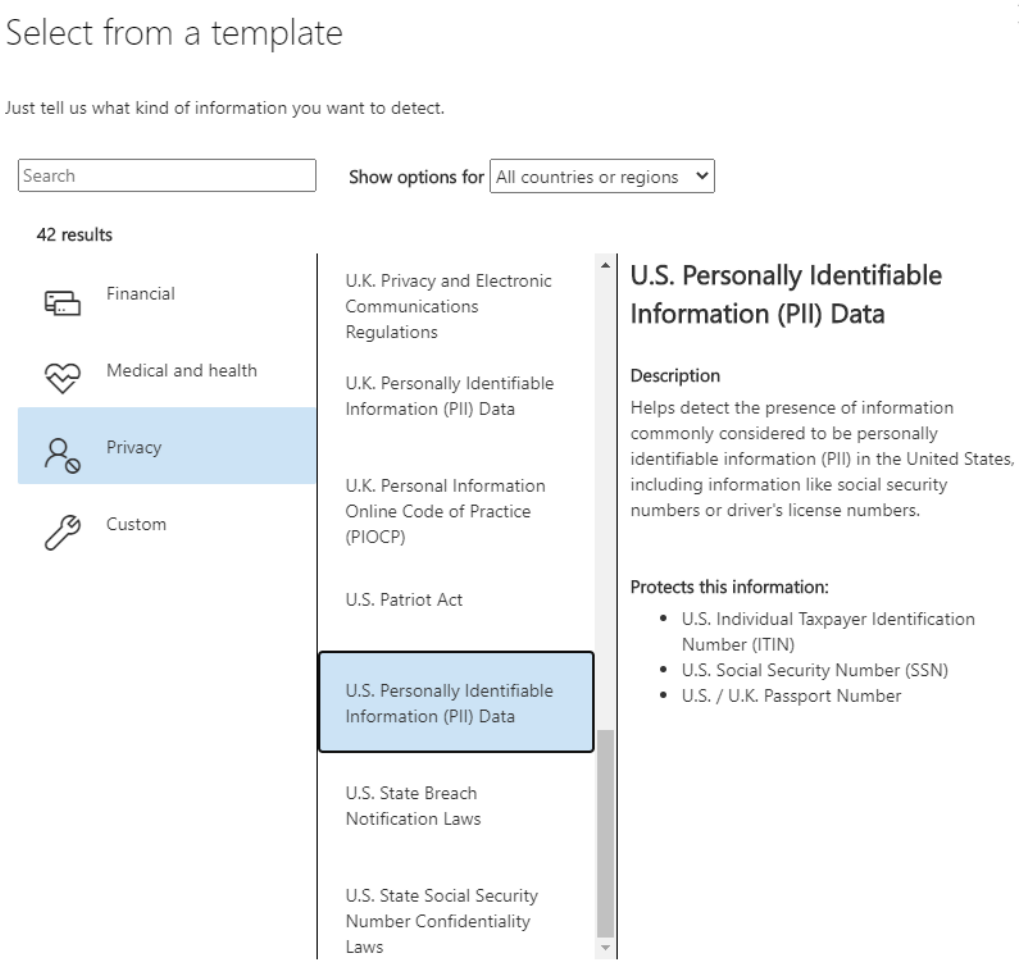
Automatic Classification of M365 Labels (G5 feature)

Auto-applied based on sensitive information types

Auto-applied based on a search query

Auto-Apply Based on Sensitive Information Types

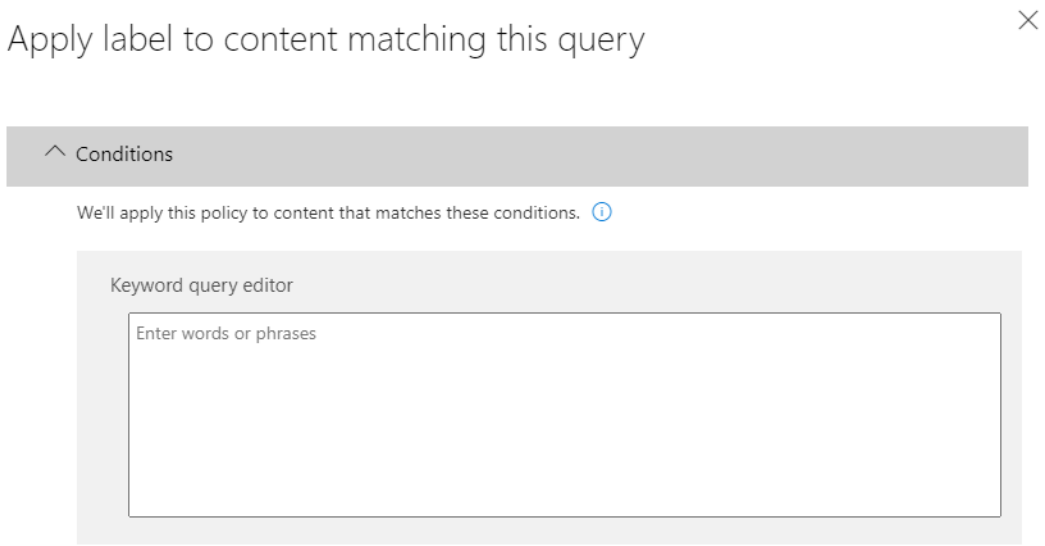
When you create auto-apply labels for sensitive information, you see the same list of policy templates when you create a data loss (DLP) policy.



Auto-Apply Based on Search Query

Query-based labels use the Content Search feature in M365 Security & Compliance Center to Identify content.

You can search for a word or phrase using Keyword Queries.



M365 Won't Auto-Apply if the Label is a Record

If a label is a record, it locks the item so it cannot be edited

A label that classifies content as a record needs to be applied manually; it cannot be auto-applied

For SharePoint content, any user in the default Members group (contribute permission level) can apply a record label to content

Only the site collection administrator can remove or change that label after it's been applied

Event-Based Retention in M365

Admin

- Creates a label based on an event & associates the label with an event type
- Publishes the label

End User

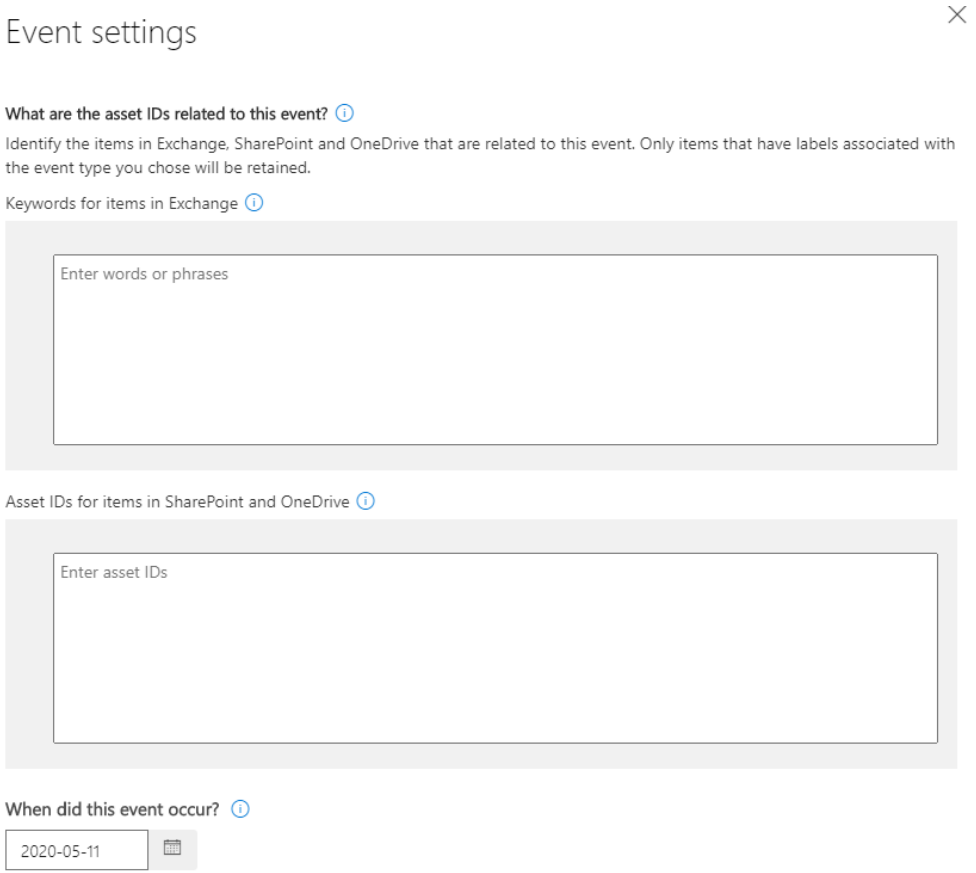
- Works on a document and applies the label
- Enters an asset ID for that document in the document properties

Admin

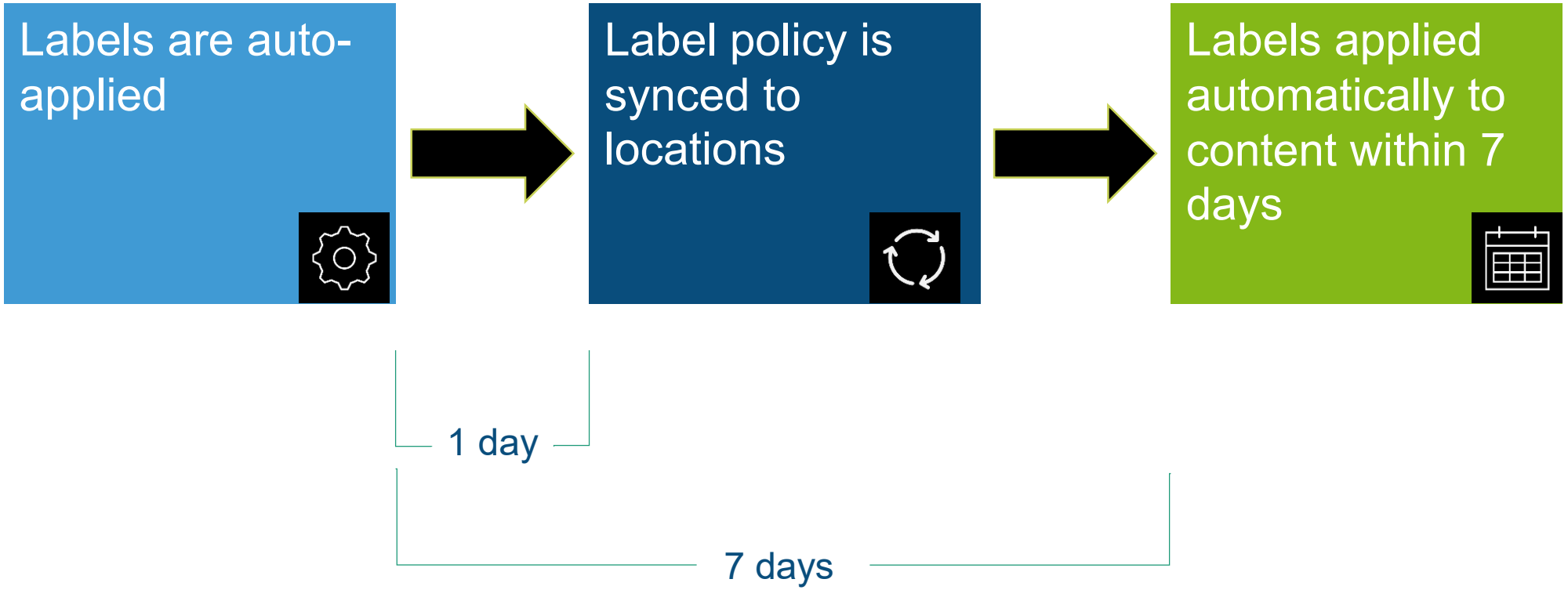
- Creates an event for that event type to trigger the retention period
- Enters asset IDs and keywords to identify content for that event

M365

- Uses the event date to trigger the start of the retention period
- Enforces retention rules on the document based on the applied label and asset IDs and keywords



It Takes 7 Days to Automatically Apply a Label



Label Location Detail

If the label is…	Then the label policy can be applied to…			
	Exchange	**SharePoint**	**OneDrive**	**Groups**
Published to end users	X	X	X	X
Auto-applied based on sensitive information types		X	X	
Auto-applied based on a query	X	X	X	X

eDiscovery

Discovery Tools

	Content Search (G3)	Core eDiscovery (G3)	Advanced eDiscovery (G5)
Search	✓	✓	✓
Export	✓	✓	✓
Legal Hold		✓	✓
Advanced Review			✓

Content Search

- Search and Export only
- Minimum G3 license required
- All eDiscovery Managers in the tenant can see your search and export its results
- No reason to use Content Search

Core eDiscovery (G3)

- Search, Export, and Legal Hold
- No review capabilities
- Minimum G3 license required
- Export to PST, deduplication

Advanced eDiscovery* (G5)

- Search, Export, Review, and Legal Hold
- G5 license required, or G3 + eDiscovery and Audit add-on, or G3 + Compliance add-on
- OCR, analytics, near-deduplication, legal hold notification, redaction, email/Teams communication threading, review sets, marks & tags, import 3rd party blob data
- May need 3rd party tool for advanced review and production

* Based on eDiscovery 2.0 (scheduled release 6/2020)

What's Missing?

- Review tools with a G3 license
- Ability to collect from on-prem sources
- Highlighted search terms in preview
- Full redaction: reason codes and logging*
- 'Pretty' reporting
- Ability to export to PST in Advanced eDiscovery*

* On Microsoft roadmap, possibly with eDiscovery 2.0 (scheduled release 6/2020)

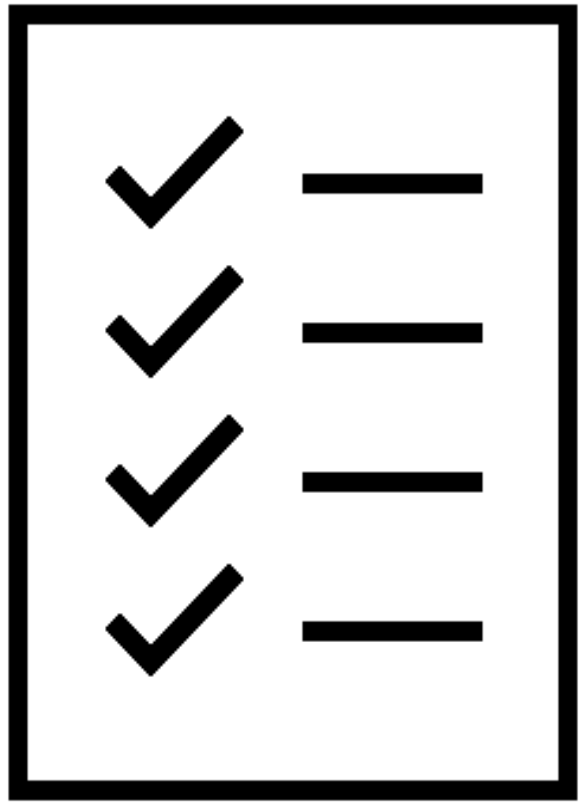
How to Get Started with eDiscovery

Licensing
- All users you need to search will require a license appropriate to the tool, either Core (G3) or Advanced (G3+/G5)

Policies
- Work with WaTech to implement your agency retention and label policies

Role Group
- Work with WaTech to assign the eDiscovery Manager role to your AD group

Boundaries
- Work with WaTech to implement compliance boundaries for your searches



M365 Links

- https://protection.office.com/homepage
- https://compliance.microsoft.com/homepage

Compliance Filters

- Separate your data from other agencies
- Assigned to your eDiscovery Manager role group
- Filter 1: Exchange Online (EXO)
  - Primary SMTP address
  - Vanity SMTP addresses
- Filter 2: SharePoint (SPO) & Teams
  - stateofwa.sharepoint.com/**sites**/watech*
  - stateofwa.sharepoint.com/**teams**/watech*

```
{Mailbox_Company -like 'watech’
-or Mailbox_PrimarySMTPaddress -like '*@watech.wa.gov’
-or Mailbox_Company -like 'ocs’
-or Mailbox_PrimarySMTPaddress -like '*@ocs.wa.gov’
-or Mailbox_Company -like 'ocio’
-or Mailbox_PrimarySMTPaddress -like '*@ocio.wa.gov'}
```

```
{Site_ComplianceAttribute -like 'WaTech’
-or Site_Site –like
'https://stateofwa.sharepoint.com/sites/watech*’
-or Site_Site –like
'https://stateofwa.sharepoint.com/teams/watech*'}
```