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”
# Records Principles

<table>
<thead>
<tr>
<th>EASY</th>
<th>MODERN</th>
<th>TRUSTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Reduce complexity for record creators</td>
<td>• Automated rules engine classifies content</td>
<td>• Compliant with local, state, federal, and global standards (e.g. WPA, GDPR, CCPA)</td>
</tr>
<tr>
<td>• Employees are not compliance experts</td>
<td>• Extensible connector framework (e.g. O365, Azure, AWS, ECMs)</td>
<td>• Maintain data onshore to meet data sovereignty compliance</td>
</tr>
<tr>
<td>• Seamlessly manage content across multiple repositories</td>
<td>• Federated data management</td>
<td>• Certified on security and operation standards (e.g. HIPAA, CJIS, FedRAMP)</td>
</tr>
<tr>
<td>• In-place records management across cloud and on-prem</td>
<td>• Retire legacy systems and enable the modern workplace</td>
<td></td>
</tr>
</tbody>
</table>
Traditional Records Management

- Document Created
- Document Managed
- Document Finalized
- Record Managed
- Disposal

- Classify Information
- Maintenance
- Dispose

- Risk of Deletion
- Risk of not being declared a record
- Risk of Non-Disposition
Modern Records Management

- **Manage Content**
  - (classify record as soon as it is created)

- **Invisible Records Management**
  - (retention is applied automatically)

- **Disposal**
  - (managed or unmanaged disposal)
Microsoft 365 Compliance Features

Retention
RetentionPolicy 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.

<table>
<thead>
<tr>
<th>Entire Locations</th>
<th>Office 365 Locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Email</td>
<td>Exchange Public Folders</td>
</tr>
<tr>
<td>SharePoint</td>
<td>Teams Channel Messages</td>
</tr>
<tr>
<td>OneDrive</td>
<td>Teams Chats</td>
</tr>
<tr>
<td>O365 Groups</td>
<td></td>
</tr>
<tr>
<td>Skype for Business</td>
<td></td>
</tr>
<tr>
<td>Recipients (up to 1000)</td>
<td>Exchange Public Folders</td>
</tr>
<tr>
<td>Sites (up to 100 sites)</td>
<td>Teams Channel Messages</td>
</tr>
<tr>
<td>Accounts (up to 100)</td>
<td>Teams Chats</td>
</tr>
<tr>
<td>Groups (up to 1000)</td>
<td>All or None</td>
</tr>
</tbody>
</table>
Exchange Online Retention Policy

- Can be applied to a universal security group
- Limit of 1,000 users per policy
- Tenant admin applies script to make group dynamic
SharePoint Retention Policy

- Applied to individual sites
- Limited to 100 sites per policy
- SharePoint admins apply retention to their site
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.

- **All Locations**
  - Entire Locations
    - Exchange
    - SharePoint
    - OneDrive
    - O365 Groups
  - Include or Exclude
    - Recipients (up to 1000)
    - Sites (up to 100 sites)
    - Accounts (up to 100)
    - Sites (up to 1000)
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

- Labels are auto-applied
- Label policy is synced to locations
- Labels applied automatically to content within 7 days

1 day

7 days
# Label Location Detail

<table>
<thead>
<tr>
<th>If the label is...</th>
<th>Then the label policy can be applied to...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Exchange</td>
</tr>
<tr>
<td>Published to end users</td>
<td>X</td>
</tr>
<tr>
<td>Auto-applied based on sensitive...</td>
<td></td>
</tr>
<tr>
<td>information types</td>
<td></td>
</tr>
<tr>
<td>Auto-applied based on a query</td>
<td>X</td>
</tr>
</tbody>
</table>
eDiscovery
## Discovery Tools

<table>
<thead>
<tr>
<th></th>
<th>Content Search (G3)</th>
<th>Core eDiscovery (G3)</th>
<th>Advanced eDiscovery (G5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Export</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Legal Hold</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Advanced Review</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
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://protection.office.com/homepage)

• [https://compliance.microsoft.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_PartialSMTPAddress -like '*@watech.wa.gov'
 -or Mailbox_Company -like 'ocs'
 -or Mailbox_PartialSMTPAddress -like '*@ocs.wa.gov'
 -or Mailbox_Company -like 'ocio'
 -or Mailbox_PartialSMTPAddress -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*'}