

DECEMBER 29, 2020

MILLICAN & ASSOCIATES - NARA COMPLIANCE WITH MICROSOFT 365

A WHITE PAPER PREPARED BY TIM SHINKLE



CONTENTS

Millican & Associates - NARA Compliance with Microsoft 365.....	2
Overview	2
Background	3
NARA UERM Requirements.....	3
Microsoft 365	3
Millican’s Experience.....	5
M365 Implementation	6
Implementation Steps.....	6
Repeatable erm implementation methodology.....	6
M365 Features	7
Security & Compliance Features	7
eDiscovery Features and advanced data governance	9
Powershell	9
Social Media records and flow connectors	10
Power apps and connections	12
M365 Enhancements and third-party add-ons.....	13
M365 third-party Considerations.....	13
SUMMARY	14

MILlican & ASSOCIATES - NARA COMPLIANCE WITH MICROSOFT 365

OVERVIEW

The U. S. National Archives and Records Administration (NARA) has published a set of universal electronic records management (UERM) requirements to help agencies and vendors better understand what is required for implementing automated electronic records management (ERM). Until recently, many agencies relied upon the DoD 5015.02-STD standard developed in the '90s to help guide them on what automated electronic records management systems require. The new UERM requirements provide a modern approach to ERM for products such as Microsoft 365 to automate and meet NARA compliance cost effectively.



- Microsoft 365 has built-in functionality to implement the NARA Universal Electronic Records Management requirements.
- To gain greater benefits from automation, organizations may want to consider extending Microsoft 365 with additional functionality using third party software.
- Microsoft is investing heavily in records management and compliance functionality for Microsoft 365, positioning themselves to be the central repository for an organization's e-records.

BACKGROUND

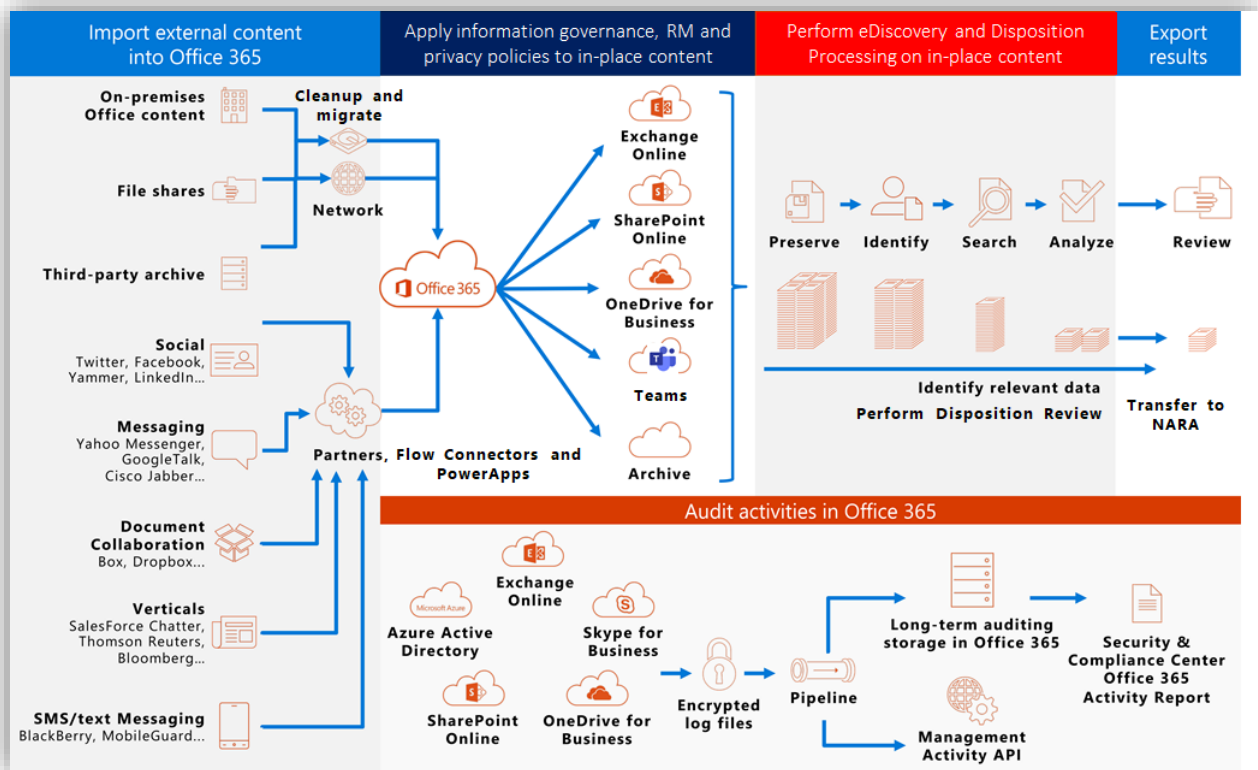
NARA UERM REQUIREMENTS

Req ID	Requirement Text	Lifecycle Phase	Req Type	Priority	Source
0.01	Agencies must manage all electronic records including all recorded information, regardless of form or characteristics, made or received by a Federal agency as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the US Government.	Full Lifecycle	Program	Must Have	44 USC 3301
0.02	Agencies should monitor and review access rights and permission rules for electronic records regularly; these access rights and permission rules should be updated on a regular basis.	Full Lifecycle	Program	Should Have	ISO 15489-1:2016, Section 8.4 Access and permission rules
0.03	Agencies must have controls to prevent unauthorized access, alteration, concealment, or destruction of records. Examples include access lists, monitoring, and agent validation.	Full Lifecycle	System	Must Have	ISO 15489-1:2016, Section 5.3 Records Systems
0.04	Agencies should regularly monitor and evaluate their records controls.	Full Lifecycle	Program	Should Have	ISO 15489-1:2016, Section 6.4 Monitoring and evaluation
0.05	Agencies retain responsibility for managing their electronic records, regardless of whether they reside in a public, private, or community cloud; a contracted environment; or under the agency's physical control.	Full Lifecycle	Program	Must Have	NARA Bulletin 2010-05: Cloud Computing
0.06	The records system must have the ability to prevent unauthorized access, modification, or deletion of records, and must ensure that audit trails are in place to track use of the records.	Full Lifecycle	System	Must Have	Requirements Working Group

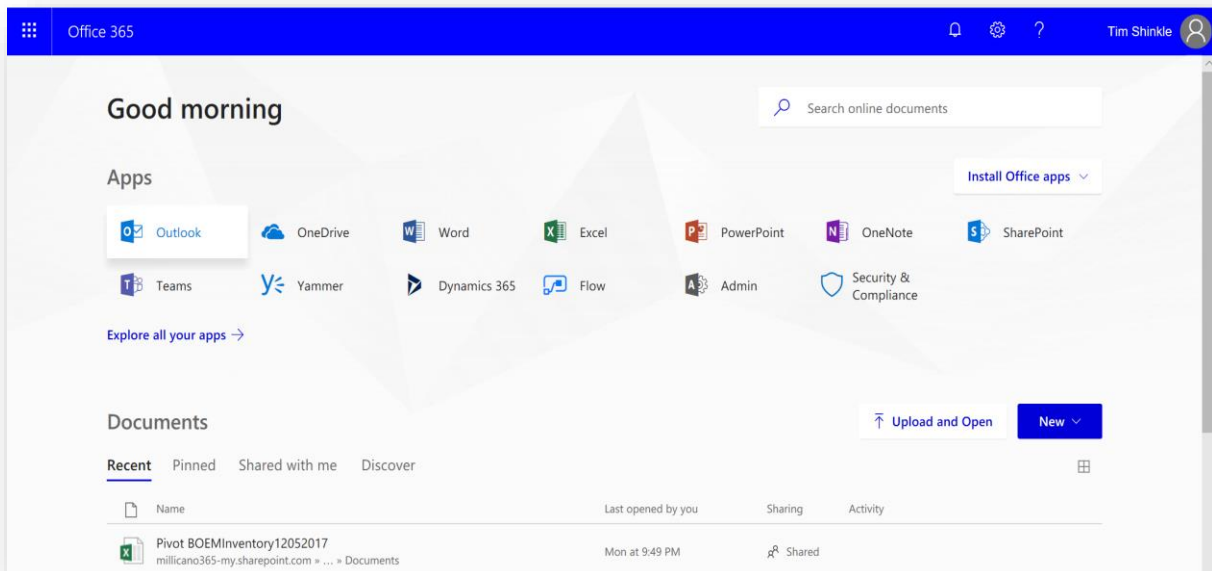
The UERM has 69 requirements some of which are optional. The requirements are either “program” requirements, relating to the design and implementation of an agency’s ERM policies and procedures, or “system” requirements, providing technical guidance to vendors in creating ERM tools and specifications for agencies to consider when procuring them. There are six categories based on the records lifecycle, including: **capture, maintenance and use, disposal, transfer, metadata and reporting**. NARA identifies 11 record types to which the requirements apply, these include: **desktop applications, electronic messages, social media, cloud services, websites, digital media (photos, audit, video), databases, shared drives and engineering drawings**.

MICROSOFT 365

The following diagram outlines how content can be loaded into M365 and more effectively managed for compliance with privacy and records management.

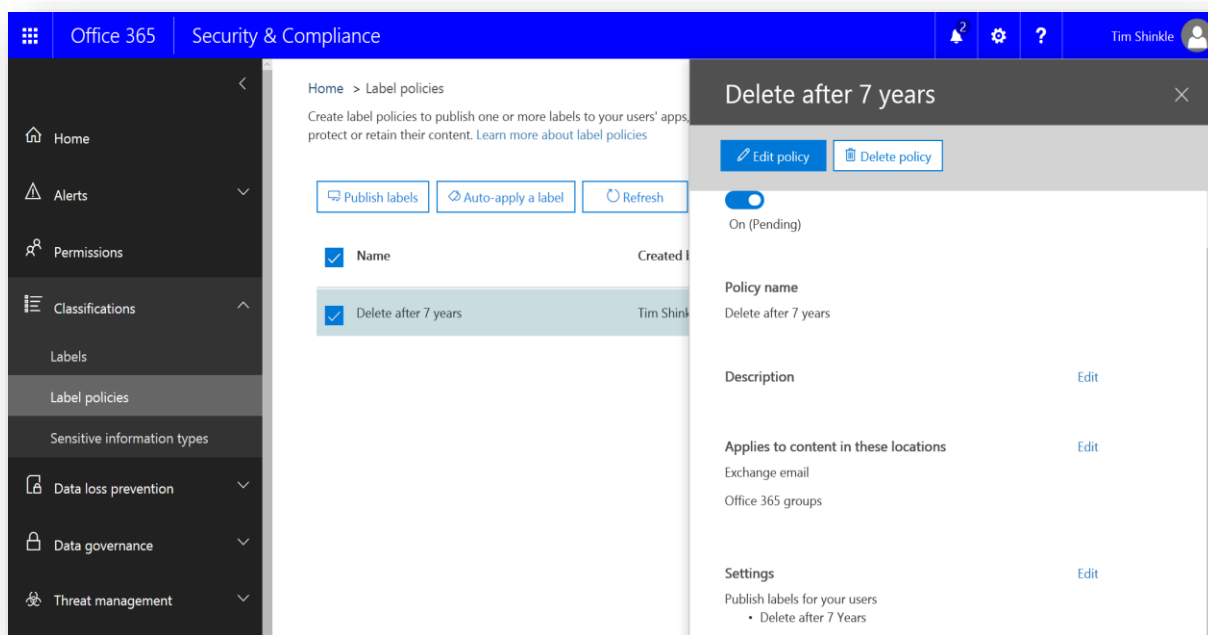


There are multiple apps included in M365.



Microsoft 365 is a platform that provides several applications for business productivity. These applications include messaging, collaboration, file sharing, document management, web content management, internal/external web portal, workflow, ERP, CRM, database, multi-media, application development and more. To better manage the content in Microsoft 365, Microsoft provides security and compliance features. The compliance features allow users to create custom tags with retention and privacy policies once and publish them to many Microsoft 365 application repositories. The policies can

be inherited from containers, applied manually or applied automatically pattern matching queries. These policies, along with other features for security, tracking changes (e.g., with logs) and workflow, provide enough functionality to map effectively to the UERM requirements from NARA.



MILlican'S EXPERIENCE

Millican implemented a Capstone solution in Microsoft 365 for a large federal agency, applying retention policies to approximately 15,000 mailboxes to meet the UERM messaging requirements. The solution was implemented using the compliance features of Exchange Online in the Microsoft 365 platform and Powershell used for implementing solutions at scale with scripting. The approach included walking through a requirements and policy decision matrix that was used to interpret what each requirement meant and how best to implement it with no impact to the business user.

The decision matrix was used to determine how best to implement challenging requirements such as culling, which requires the ability for a trusted custodian to determine what messages are not valid records and remove them as needed. The implementation of culling exploited existing customer habits, such as filtering junk mail, using the clutter folder and deleting unwanted messages as part of the business user's routine use of email maintenance. The solution supplemented the records policy in the form of an administrative executive order and is compliant with the UERM requirements and recent use cases published by NARA for management of electronic messages. The approach included how best to capture records from employees onboarding, offboarding and acting on behalf of high-level Capstone officials.

M365 IMPLEMENTATION

IMPLEMENTATION STEPS

The steps followed to implement the Capstone solution in Microsoft 365 included:

1. Identifying and submitting the Capstone Officials list.
2. Reviewing various technical approaches.
3. Defining roles and retention for temporary and permanent records.
4. Developing a decision matrix to gain consensus and executive sign-off for key requirements such as culling (non-record), legacy email, etc.
5. Developing and approving an email policy.
6. Defining use cases for testing solution in Microsoft 365 test accounts (lab).
7. Mapping HR process when employees leave, are hired or act in a Capstone role.
8. Rolling out solution running scripts to apply retention policies to approximately 15K employee mailboxes in time for the Dec 31, 2016 deadline.

The most crucial part of any solution is how the requirements get implemented. The best approach is to use a flexible and repeatable process as part of your organization's system development lifecycle or SDLC driven.

The solution should follow the golden rule of modern ERM: no end user intervention required to capture and manage records. In Microsoft 365 each application can manage its e-content in-place or move it to an archive, leveraging search and eDiscovery services for all records stored in Microsoft 365.

REPEATABLE ERM IMPLEMENTATION METHODOLOGY

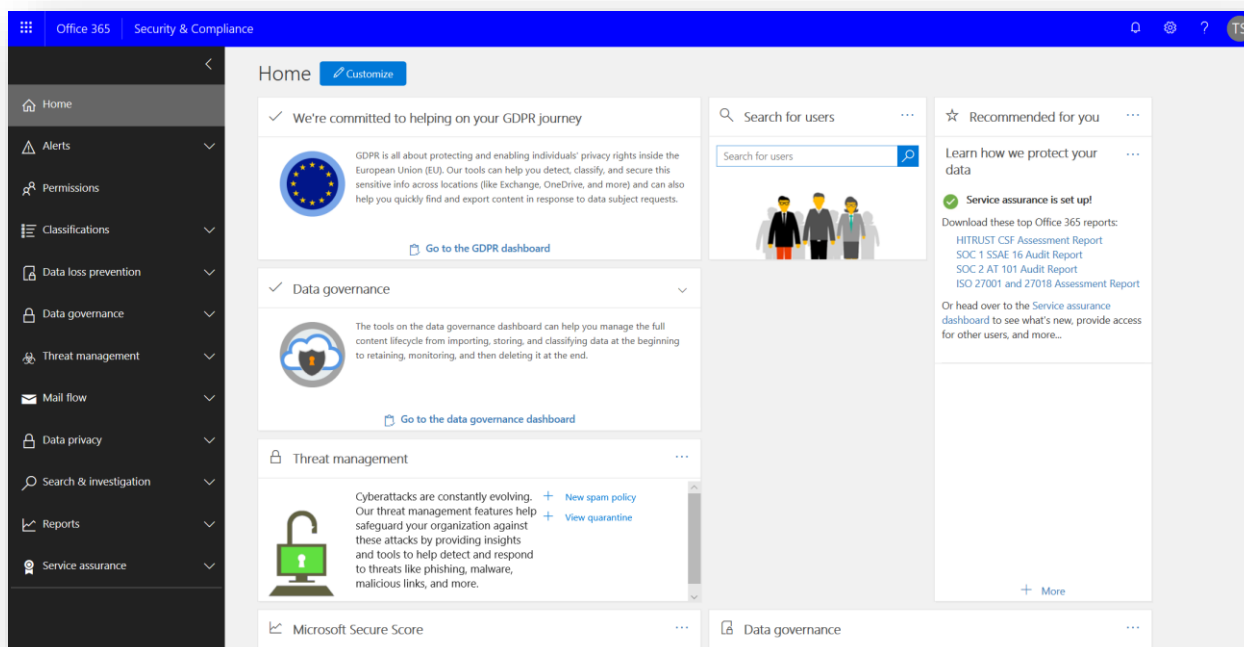
The recommended repeatable UERM implementation steps include:

1. **Simplify** – Define a simplified set of ERM requirements based on the UERM.
2. **Analyze** – Know the landscape of existing systems and their use (i.e., Microsoft 365).
3. **Prioritize** – Address systems and applications in order of importance (e.g., Exchange Online).
4. **Integrate** – Integrate the ERM requirements in the SDLC to enhance the target systems and applications functionality as needed based on cost, risk, and benefit. Options include:
 1. Do nothing.
 2. Configure, customize or enhance.
 3. Integrate with another third-party system (manage records in-place or move to an archive).
 4. Replace or upgrade.
5. **Monitor** – Define success criteria and audit for improvement.
6. **Decommission** – Develop a decommissioning plan for retiring legacy systems (e.g., a Microsoft 365 SharePoint Online and Teams sites decommissioning plan).
7. **Repeat** – repeat the approach as systems and applications are added, upgraded, replaced or retired.

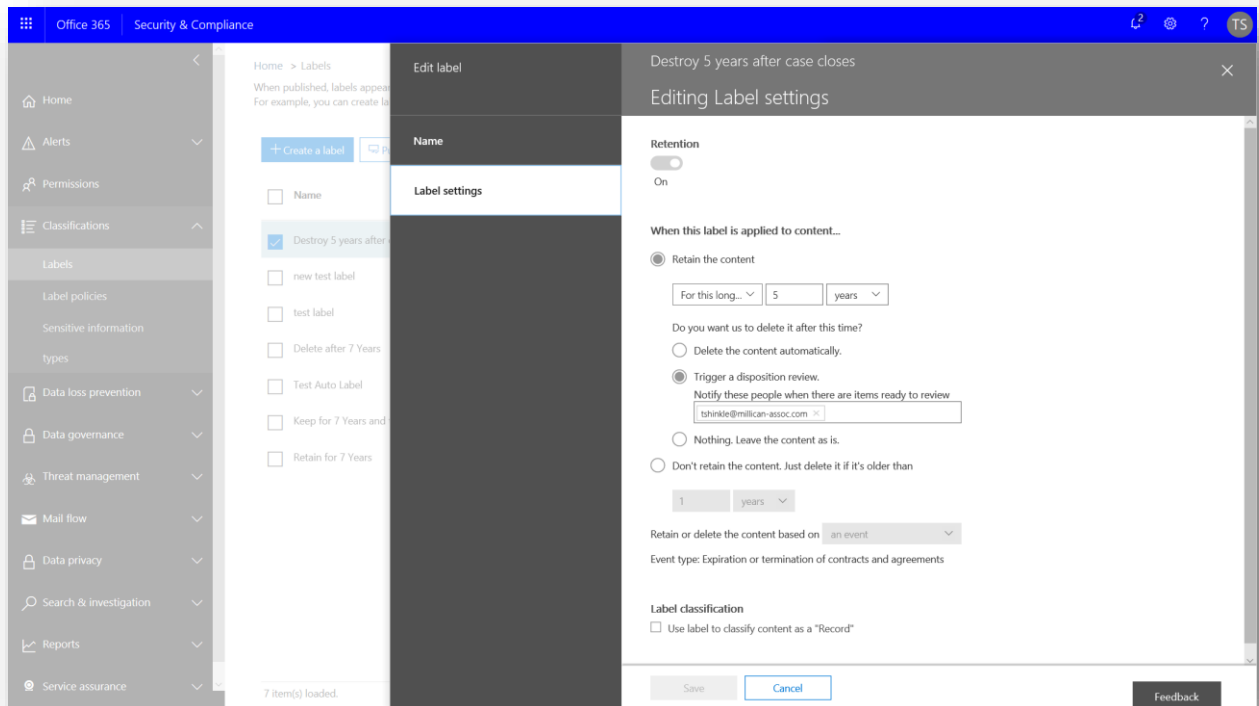
M365 FEATURES

SECURITY & COMPLIANCE FEATURES

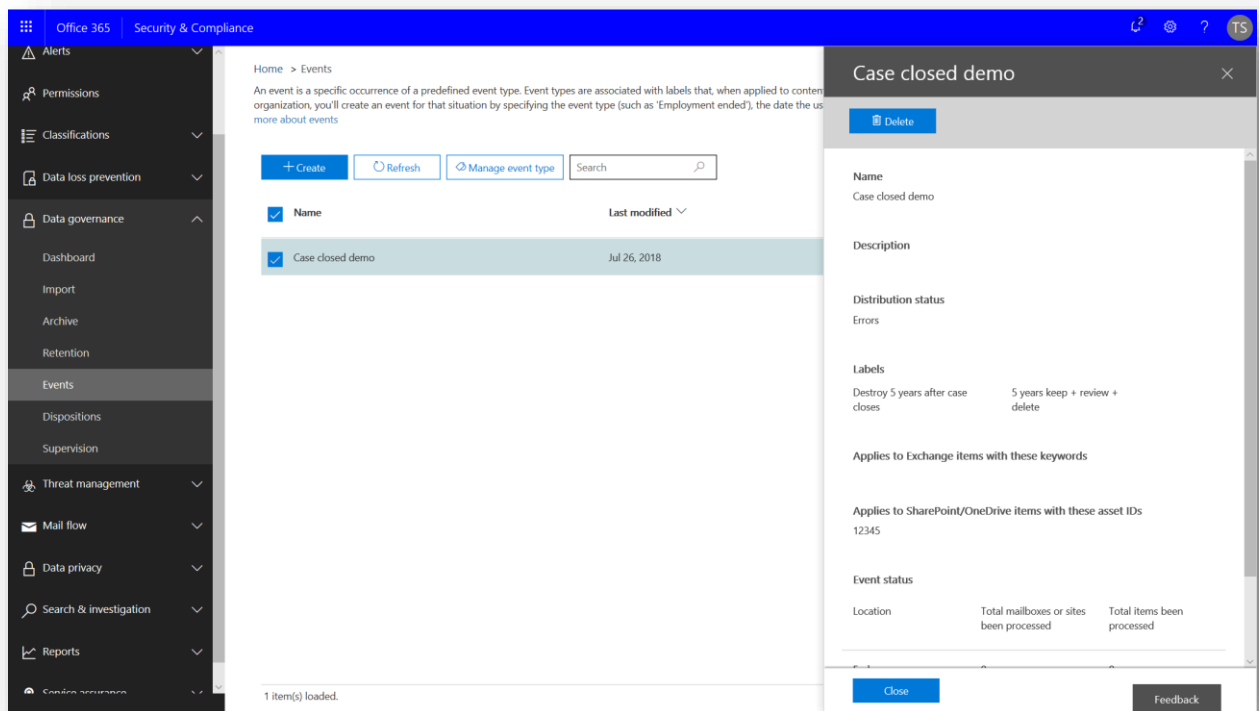
The M365 Security & Compliance Center provides a portal dedicated to the features use for privacy and records management policy compliance across all M365 apps including Teams and SharePoint Online, OneDrive and Exchange Online and others. A Security & compliance role can be set up for privacy and records to configure, manage and monitor the application of compliance policies across the entire M365 platform.



Labels can be created that map to retention policies for publishing to apps that contain records found in Teams, SharePoint Online, OneDrive, Exchange Online and other apps.

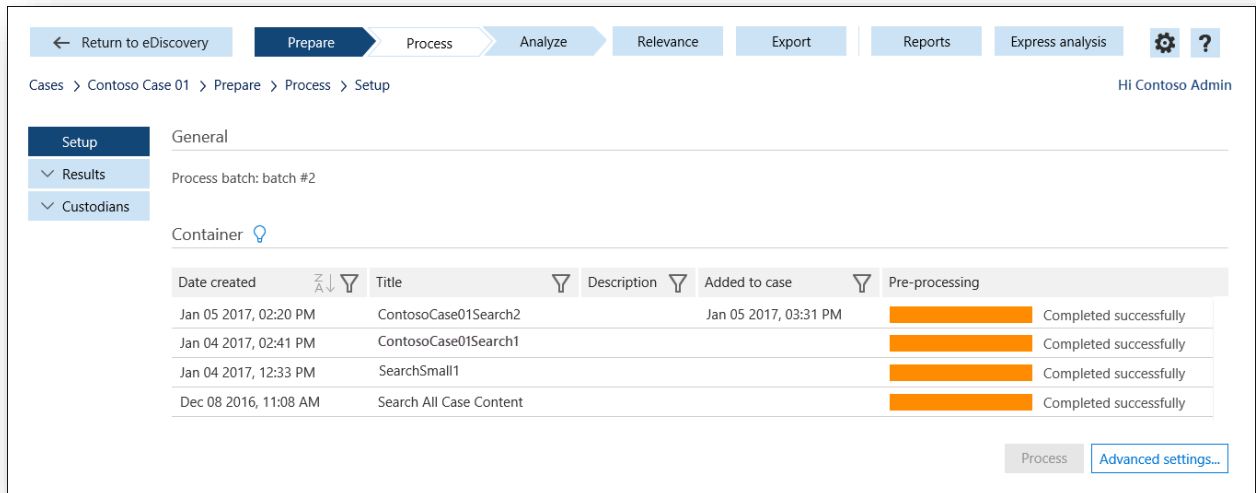


Data governance features include events and disposition processing, that enable controls to be put on in-place records requiring event or case-based retention, and review prior to final disposition.



EDISCOVERY FEATURES AND ADVANCED DATA GOVERNANCE

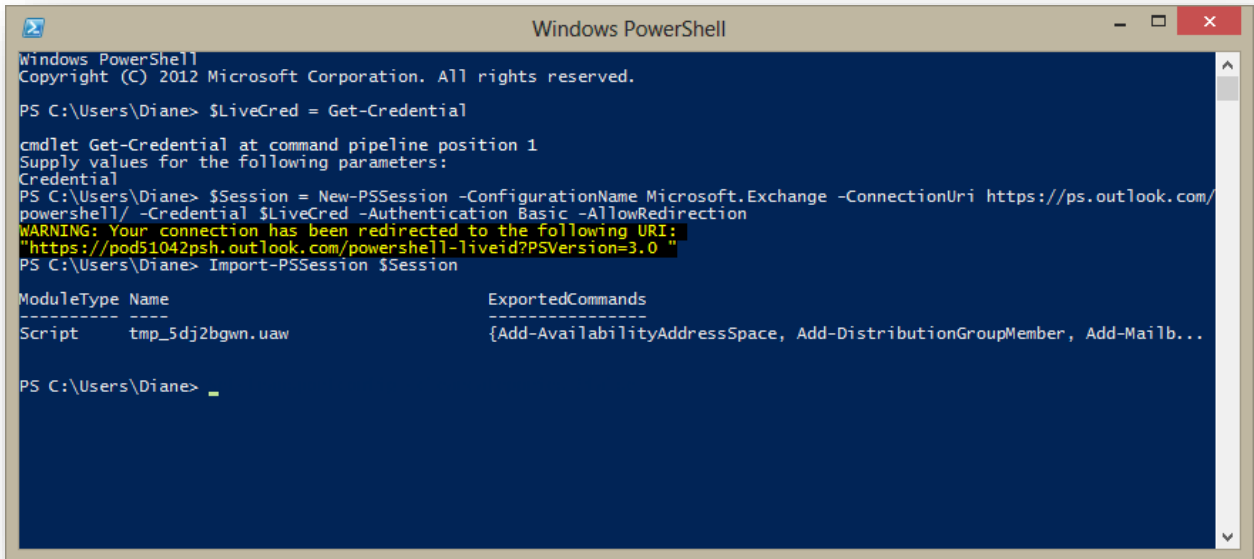
Microsoft sells a G5 license for government that includes the machine intelligence module for eDiscovery. This can be leveraged not only for eDiscovery, but FOIA and culling, for example prior to sending Capstone officials email records to NARA they should be culled to remove non-records.



The Microsoft 365 Advanced eDiscovery integrates Equivio machine learning, predictive coding and text analytics capabilities to reduce the costs and challenges that come along with sorting through large quantities of data.

POWERSHELL

With Microsoft 365 PowerShell, you can manage Microsoft 365 with commands and scripts to streamline your daily work. Learn why Microsoft 365 PowerShell skills are crucial to managing Microsoft 365, how to connect to your Microsoft 365 subscription, create reports, and get additional information and help from the Microsoft 365 community.



```
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Users\Diane> $LiveCred = Get-Credential

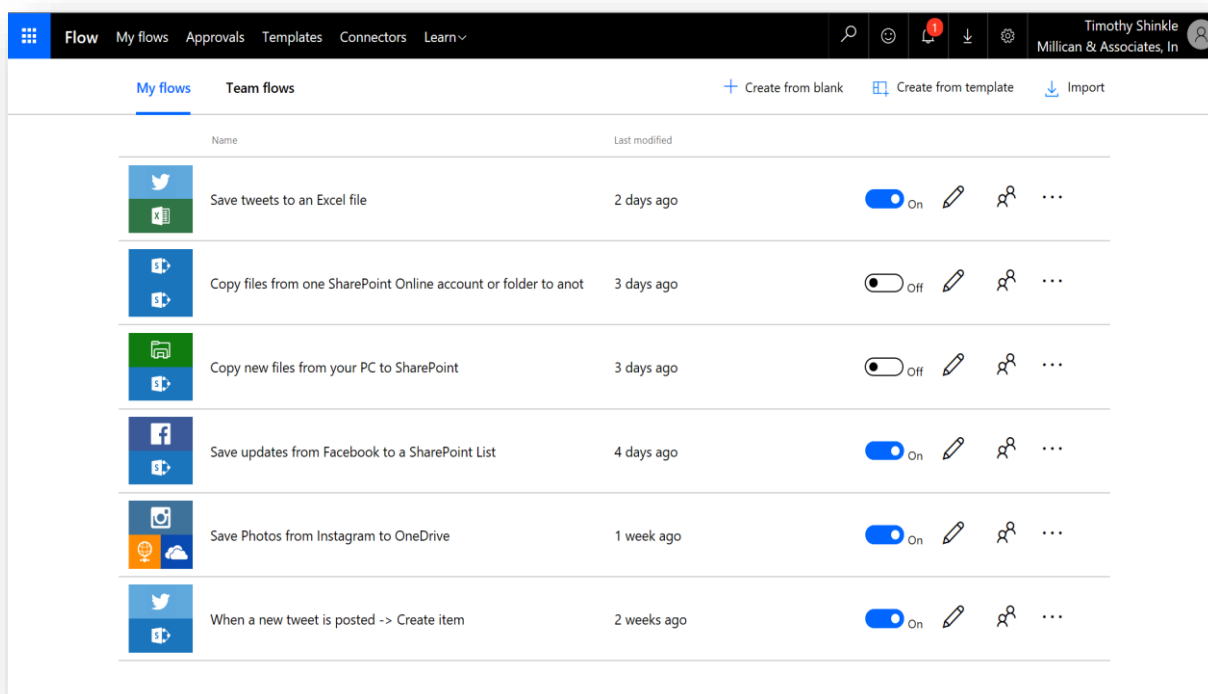
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
PS C:\Users\Diane> $Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://ps.outlook.com/
powershell/ -Credential $LiveCred -Authentication Basic -AllowRedirection
WARNING: Your connection has been redirected to the following URI:
"https://pod51042psh.outlook.com/powershell-liveid?PSVersion=3.0 "
PS C:\Users\Diane> Import-PSSession $Session

ModuleType Name                                     ExportedCommands
-----
Script      tmp_5dj2bgwn.uaw                                {Add-AvailabilityAddressSpace, Add-DistributionGroupMember, Add-Mailb...
```

A Key feature includes bulk transactions for automating tasks at scale (e.g. export emails for transfer to NARA from hundreds of mailboxes of acting HLOs across different time frames).

SOCIAL MEDIA RECORDS AND FLOW CONNECTORS

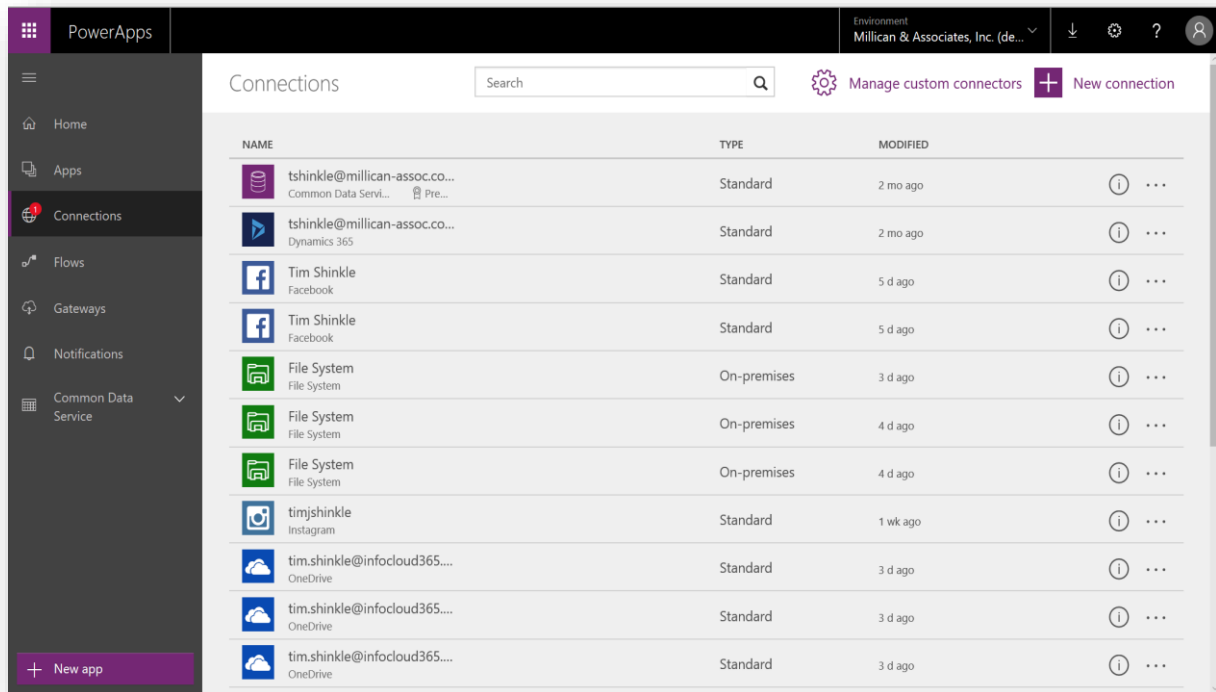
Social media contain records in third-party repositories in the Cloud. Microsoft 365 provides some very powerful features to harvest these records and ingest them into the platform for ongoing compliance with UERM. PowerApps in Microsoft 365 include custom apps, Connectors, Flows and Gateway services to integrate with both third-party Cloud vendors and on-premises systems. There are many Flow Connectors that come out-of-the-box in Microsoft 365 for the most popular social media sites, such as Facebook, Twitter and Instagram.



The Connectors have various options for when to poll the source systems and what logic to perform on a periodic basis, such as moving recent Tweets to a SharePoint Online list that can subsequently apply Information Management Policies to those Tweet records in compliance with the UERM requirements. This goes for other social media as well, including Facebook and Instagram, that may have valuable e-records to be stored and managed under the control of the organization in their Microsoft 365 environment.

POWER APPS AND CONNECTIONS

There is also the ability in Microsoft 365 to connect to on-premises systems and applications using data Gateway Cloud Services Connections – for example, to monitor for records located in an on-premises file system.



The combination of Flow and Gateway in PowerApps provides a very powerful mechanism to centralize all your e-records in Microsoft 365 from third-party Cloud and on-premises sources providing one place for all your ERM needs and compliance with UERM.

M365 ENHANCEMENTS AND THIRD-PARTY ADD-ONS

For organizations that want more automation than they get out-of-the box with Microsoft 365, but also wish to avoid custom development, there are several choices to consider:

Customize or Enhance

- Custom API services and apps, for example custom retention policies with custom Expiration Formulas.
- Out-of-the-box or third-party add-on apps (e.g., Microsoft 365 AppSource or Azure solutions).
- Client side vs. server provider host app model, e.g., Gimmal and AvePoint.
- *PowerApps* with *Flow Connectors* can be used to capture records from Facebook, Twitter, Instagram, on-premises files shares, databases and more.

Integrate

- Third party ERM – Dashboard, scan and event-based monitoring, rule-based manage in-place (e.g., Gimmal, AvePoint, RecordPoint).
- ECM redundant repository (e.g., IBM FileNet, OpenText, Alfresco, HP Trim, and others).
- Crawl technology – scan, index, identify, tag and manage in-place or move (e.g., ActiveNavigation, Nuix, Seek, Tier5Data, and others).

M365 THIRD-PARTY CONSIDERATIONS

For each of these options, there are pros and cons to consider:

Pros of Third-Party Products

- Can be built specifically for Records Managers with specialized interfaces.
- Can come pre-configured where Microsoft 365 requires expertise to configure.
- Security can be isolated.
- Additional functionality may include: retention schedules, file plans, additional security layers, enhanced audit capabilities, records reporting, disposition workflows, rules engines and more.
- Can come with native integrations with systems external to Microsoft 365.
- Microsoft requires additional licensing for move advanced compliance features that may be more expensive than third party products.

Cons of Third-Party Products

- Requires additional maintenance and support.
- Enterprise Content Management (ECM) products have redundant repositories and functionality.
- Add more complexity to the implementation.
- Requires additional training.

SUMMARY

Overall UERM can be cost effectively implemented in Microsoft 365 for meeting NARA compliance.

In summary:

- UERM looks to be a good start for a universal set of ERM requirements;
- UERM provides flexibility for how to implement the requirements;
- UERM is a good update to the legacy 5015.02-STD requirements;
- UERM can be implemented natively in Microsoft 365, but an assessment should be done to weigh the costs, risks and benefits of adding third party technology for additional automation as needed.