Supporting New Zealand's Public Records Act compliance obligations with Microsoft 365

Published by Microsoft New Zealand (January 2021)

Microsoft

INFORMATION LEADERSHIP

Disclaimer

Acknowledgements

Microsoft acknowledges the key role Information Leadership has had in the preparation of this document. We would also like to acknowledge the customers and Microsoft employees who have provided feedback on this white paper.

Contents

Introduction

This white paper documents an assessment by Information Leadership of the capability of Microsoft 365 to support organisations in meeting their obligations under the New Zealand Public Records Act 2005 (PRA). The white paper offers a pragmatic approach to supporting PRA compliance obligations, balancing the needs of both information managers and users.

Microsoft's role has been to verify information about Microsoft 365 functionality and capability within the context of this white paper.

1. Purpose of this white paper

The purpose of this paper is to help customers understand that the system aspects of PRA compliance are achievable when using Microsoft 365. In particular, the paper is intended to help:

- **Business leaders** to understand that Microsoft 365 can support PRA compliance needs when configured appropriately. Section 1 of this white paper will be of more interest to this audience. It includes a discussion of Microsoft Teams, which is becoming the key Microsoft 365 workload many customers adopt to create and manage information.
- **Information management and ICT professionals** incorporate compliance needs into their Microsoft 365 configuration, following a practical framework. This framework includes leveraging approaches that users find acceptable and that are aligned to helping them work smarter and more efficiently.

The white paper describes the configuration settings and features that support PRA compliance and how these relate to key Microsoft 365 workloads such as Exchange Online, Microsoft Teams, SharePoint Online, OneDrive for Business and Stream.

As the paper outlines the key *system needs* for PRA compliance, customers should also evaluate other aspects of achieving PRA compliance such as governance, training, etc. It should be noted that software does not comply with the PRA – organisations do. Choosing the right software and then configuring and using it appropriately enhances their ability to comply. This white paper does not constitute a guarantee of compliance, and this assessment is done against current Microsoft 365 capabilities. Still, it is the customer's responsibility to evaluate against new features and changing legislation and standards continually.

2. Summary

The key points of consideration when considering PRA compliance are as follows:

Compliance needs can be practically supported:

Microsoft 365 can be configured and used in ways that support the system aspects of PRA Compliance. Microsoft 365 is an excellent platform choice for meeting compliance needs. The platform is what users interact with daily; therefore, they do not need to learn a new system or tools or move their content. It provides compliance by design that is invisible to users most of the time.

Use of Microsoft 365 promotes higher adoption:

The Microsoft 365 features described in this document create a better user experience than previously possible in creating and using content. This better experience increases compliance. Typically, many more records are managed compared to adoption rates of legacy EDRMS alternatives.

For collaboration, Teams messages are copied into Exchange for compliance aspects, and files are stored in SharePoint Online. Note that other Teams content will need to be assessed based on its recordkeeping value (Whiteboard, Planner, third party apps, etc.)

A practical approach is to attach mailboxes and sites to default retention policies (for instance, retain content for two years and then delete). Whereas the Team's purpose is more than general collaboration, some or all of its content may need to be retained longer or transferred to Archives NZ. We can achieve this through a combination of one or more of the following:

- Attaching the mailbox and site to a retention policy with a longer disposal period
- Overriding the mailbox or site's policy with retention labels for important individual records Using advanced features for automated labelling of records in a site, document library, document set, or folder

The approach to compliance:

Where possible, use broad retention policies on mailboxes and sites that include Teams and other content. Where it is necessary to separate content for more fine-tuned retention and disposal, use retention labels on mailbox and library folders, as well as document sets and individual files.

This approach may require using advanced features and/or approaches that leverage the in-platform low-code and automation capabilities available via Power Automate and Power Apps or other methods.

3. How to read this white paper

This white paper has the following three key sections:

Section 1: How Microsoft 365 helps supporting Public Records Act requirements

This section works through each of the minimum compliance requirements in the Information and Records Management Standard and identifies relevant capabilities in Microsoft 365 to support each requirement, where appropriate.

Section 2: Framework for using Microsoft 365 to support the Public Records Act

This section provides a framework for using Microsoft 365 to support the Public Records Act. It is structured around eight design configuration needs. For each need, it provides the following:

1. Linkage to the Standard and Implementation Guide - the link to the specific minimum compliance requirement along with the explanation associated with the requirement
2. Tactics - the specific tactics and approach for how to meet this requirement
3. Application - any specific considerations in how to apply these tactics in Microsoft 365

Section 3: Features and Licensing Summary

We describe specific Microsoft 365 features throughout the paper, which are available with Microsoft 365 E3 licencing. This approach provides a robust compliance base for protecting, maintaining, and disposing of content. Several other advanced features, which provide specific additional records management functionality, are also described throughout this white paper. You can license this functionality via various options in addition to Microsoft 365 E3. This section documents the licensing requirements for these advanced features.

Section 1:
How Microsoft 365 helps to support PRA requirements

1.1 Introduction

Public Records Act (PRA)

The Public Records Act sets out two duties for public offices and local authorities:

1. The requirement to create and maintain records; and
2. That authority is required to dispose of public records and protected records

Information and Records Management Standard

Under section 27 of the Public Records Act Archives New Zealand can issue standards supporting the Act. The Information and Records Management Standard (July 2016) supports the "*systematic and efficient management of government information and records, outlining the obligations of regulated organisations under the Public Records Act.*"

The Information and Records Management Standard is a mandatory standard. It *"establishes how to manage information and records efficiently and systematically. It sets out the minimum level of compliance that organisations must meet."*

The Standard is organised around three principles:

1. Organisations are responsible for managing information and records
2. Information and records management supports business
3. Information and records are well managed

For each principle, the Standard lists the minimum compliance requirements.

Implementation guide – Information and records management standard

The Implementation guide explains each of the minimum compliance requirements in the Standard and references key guidance for implementing the requirement.

Public Records Act 2005

Information and Records Management Standard

Implementation Guide: Information and Records Management Standard

1.2 PRA Standard's requirements

The Information and Records Management Standard gives 21 minimum compliance requirements. However, not all these requirements relate to systems, with many being about governance, people and process matters. The following tables list the three Information and Records Management standard principles and their associated minimum compliance requirements. For each of the identified requirements, it documents the role Microsoft 365 plays in helping the organisation meet them.

Principle 1:
Organisations are responsible for managing information and records

	Minimum Compliance Requirement	Role of Microsoft 365
1.1	Information and records management must be directed by strategy and policy which is reviewed and monitored regularly.	N/A Not a system requirement
1.2	Information and records management must be the responsibility of senior management. Senior management must provide direction and support to meet business requirements as well as relevant laws and regulations	N/A Not a system requirement
1.3	Responsibility for the oversight of information and records management must be allocated to a designated role (the Executive Sponsor).	N/A Not a system requirement
1.4	Organisations must have information and records management staff, or access to appropriate skills	N/A Not a system requirement
1.5	Business owners and business units must be responsible for ensuring that information and records management is integrated into business processes, systems, and services.	This requirement relates to responsibilities for ensuring that appropriate information and records management is included in all systems and processes used. Business owners and units may find it useful to know that information, records, and record aggregations can be connected to their business context in Microsoft 365 through the use of: a) metadata: automatically applied, inherited, or inferred b) structure of document library folders and Team channels c) Retention Policies and Labels can explicitly denote the business process or activity

		In section 2.4 Configuration Need #4, we describe the metadata types that provide this business context. Organisations may have additional metadata that is important to them. In section 2.5 Configuration Need #5: Easy and obvious for users to file content, we describe how much of this metadata collection can be automated. In section 2.2 Configuration Need #2: Teams files/SharePoint Online retention & disposal design, a series of worked examples are included that demonstrate the use of structures and metadata.
1.6	Staff and contractors must understand the information and records management responsibilities of their role. They must understand relevant policies and procedures.	N/A Not a system requirement
1.7	Information and records management responsibilities must be identified and addressed in all outsourced and service contracts, instruments, and arrangements.	This requirement relates to the inclusion of information and records management in all service contracts, instruments, and arrangements. Organisations can consider using Microsoft Teams for collaborating and working with outsourced providers. When configured appropriately, Microsoft Teams can provide for the management of information, records, and associated metadata created through these relationships. These capabilities include the ability to email records to channels of a Team, that has been organised to suit collaboration and records capture. Refer to section 2.4 Configuration Need #4: Adequate metadata to provide context, section 2.5 Configuration Need #5: Easy and obvious for users to file content and section 2.7 Configuration Need #7: Provision and manage at scale for how to configure Microsoft 365 to help appropriate capture of information and records and associated metadata.
1.8	Information and records management must be monitored and reviewed to ensure that it is accurately performed and meets business need	For records created, managed, or stored using Microsoft 365, Microsoft's compliance centre provides a wide range of reporting and auditing of user activity. Refer to the following link - Search the audit log. The Advanced Audit functionality provides the ability to conduct forensic and compliance investigations (refer to advanced features). Options for retaining and managing the log files of deleted items are provided in section 2.4 Configuration Need #4: Adequate metadata to provide context.

Table 1 - Principle 1 Organisations are responsible for managing information and records

Principle 2: Information and records management supports business

	Minimum Compliance Requirement	Role of Microsoft 365
2.1	Information and records required to support and meet business needs must be identified.	Identifying functions and activities can help an organisation determine what information and records it needs to support the business. The function and activity of information and records can be held in Microsoft 365 either as stand-alone metadata or controlled through the term store. Microsoft Teams and SharePoint Online structures can follow functions and activities. Retention Policies and Labels can explicitly name the functions and activities they pertain to. Other requirements can also be recorded and provided for using metadata, as can the design and configuration information. Refer to section 2.4 Configuration Need #4: Adequate metadata to provide context for the types of metadata that need to be catered for and how to do this. In section, Configuration Need #5 we describe how much of this metadata collection can be automated.
2.2	High risk/high-value areas of business, and the information and records needed to support them must be identified and regularly reviewed.	This requirement is not, primarily, a system requirement. However, Microsoft 365 can help with this by applying either: a) Broad retention policies on mailboxes and sites that include Teams and other content; or b) Using retention labels on mailbox and library individual files plus with advanced features doing the same for mailbox and library folders as well as on document sets Refer to section 2.1 Configuration Need #1: Rule types & Approach per App for information about the approach to applying these. Refer to section 2.2 Configuration Need #2: Teams files/SharePoint Online retention & disposal design about how export, migration and transfer requirements can be met.
2.3	Information and records management must be design components of all systems and service environments where high risk/high-value business is undertaken.	The below design decisions for Microsoft 365 can support good information and records management: a) Core metadata can be captured and maintained. b) Metadata and information related to disposal can be captured and retained. c) Refer to section 2.4 Configuration Need #4: Adequate metadata to provide context for the metadata types that need to be catered for.

		d) Core process metadata is captured and made available through the Microsoft 365 Compliance Centre. e) The Advanced Audit functionality provides the ability to conduct forensic and compliance investigations (advanced features).
2.4	Information and records must be managed across all operating environments.	Microsoft 365 provides tools and functionality for managing information and records created within and across the Microsoft 365 workloads: Exchange, Teams, OneDrive, SharePoint Online. Section 2.1 Configuration Need #1: Rule types & Approach per App provides information about how to configure Teams, SharePoint Online, Exchange (email), and OneDrive for good records management. More information is also provided in section 2.8 Configuration Need #8: Approach per App. SharePoint Online lists can be designed and configured to support the management of paper records.
2.5	Information and records management must be designed to safeguard information and records with long-term value	Information and records can be safeguarded through a combination of: a) User permissions b) Setting a retention label or policy to retain the content c) Monitoring audit logs for deletion and other user actions d) Deletion process controls. e) Using the advanced feature "record" retention label to prevent a file from being changed Refer to section 2.6 Configuration Need #6: Protect content that can be used to safeguard records.
2.6	Information and records must be maintained through systems and service transitions by strategies and processes specifically designed to support business continuity and accountability.	Refer to section 2.2 Configuration Need #2: Teams files/SharePoint Online retention & disposal design for information about how export, migration and transfer requirements can be met.

Table 2 - Principle 2: Information and records management supports business

Principle 3: Information and records are well managed

	Minimum Compliance Requirement	Role of Microsoft 365
3.1	Information and records must be routinely created and managed as part of normal business practice.	M365 provides for records to be routinely created and managed through: a) Teams b) SharePoint Online c) Exchange Online d) Microsoft 365 Enterprise Applications (Outlook, Word, Excel, PowerPoint…) e) OneDrive f) Stream Refer to section 2.1 Configuration Need #1: Rule types & Approach per App for how to configure and use each of these to assist in the creation and management of information and records. Refer to section 2.5 Configuration Need #5: Easy and obvious for users to file content for how Microsoft 365 makes it easy for users to routinely create records and information.
3.2	Information and records must be reliable and trustworthy.	Core metadata can be captured and maintained. Metadata and information related to disposal can be captured and retained. Refer to section 2.4 Configuration Need #4: Adequate metadata to provide context for the metadata types that need to be catered for. Core process metadata is captured and made available through the Microsoft 365 Compliance Centre. The Advanced Audit functionality provides the ability to conduct forensic and compliance investigations (refer to advanced features). A range of functionality is available to protect the integrity of information and records. Refer to section 2.6 Configuration Need #6: Protect content.
3.3	Information and records must be identifiable, retrievable, accessible, and usable for as long as they are required.	Appropriate minimum metadata can be associated or linked to records held or created in Microsoft 365, including a file's system metadata that is automatically created. Refer to section 2.4 Configuration Need #4: Adequate metadata to provide context and section 2.8 Configuration Need #8: Approach per App.
3.4	Information and records must be protected from unauthorised or unlawful access, alteration, loss, deletion and/or destruction.	Deletion, access, and changes can be prevented, protected against, or managed using a combination of: a) User permissions

		b) Using the "record" retention label to prevent a file from being changed c) Setting a retention label or policy to retain the content d) Monitoring audit logs for deletion e) Deletion process controls. Refer to section 2.6 Configuration Need #6: Protect content. Where needed, separate tenancies can be set up for sensitive information, including deciding on where the data is physically located.
3.5	Access to, use of and sharing of information and records must be managed appropriately in line with legal and business requirements.	Broad and fine-tuned security and permissions can be set on mailboxes, document libraries, and other information assets. This includes the use of Retention and Sensitivity labels as well as the native configuration of Teams, SharePoint Online, Exchange Online, etc. Metadata should be used to record content security classification that is also embedded in the content. Exchange Online admins can create mail flow rules in the Exchange admin center to detect outgoing email attachments that contain this text or property values. Azure Conditional Access Policies can be used to deny access to sites that have one of three possible application-level tags applied to them.
3.6	Information and records must be kept for as long as needed for business, legal and accountability requirements	Microsoft 365 has various functions that support the retention and disposal of records. This includes Retention Policies and Labels. Policies can be linked to classifiers that look for specific patterns within files and set retention and sensitivity labels. In addition, Microsoft 365 has robust EDRMS capabilities such as security and permissions, content hierarchies, metadata types, version control, managing user and system deletion. Care needs to be taken in to design and configure these features in the right combination to have the right effect. Refer to section 2.2 Configuration Need #2: Teams files/SharePoint Online retention & disposal design.
3.7	Information and records must be systematically disposed of when authorised and legally appropriate to do so.	Files deleted by Retention Policies or Labels go through a two-stage recycle bin process. Audit reports allow information managers to review files and restore, where necessary before they are permanently deleted. The Disposition Review advanced feature in Microsoft 365 provides for a systematic review process before deletion, including approval from key managers.

		Refer to section 2.3 Configuration Need #3: Deletion Authorisation.

Table 3 - Principle 3: Information and records are well managed

Section 2: Framework for Using Microsoft 365 to Support the PRA

We have consolidated the system related PRA requirements into eight key design configuration needs. Together these form a framework for helping organisations achieving practical Public Records Act compliance obligations with Microsoft 365. The image below shows the needs and is followed by a table describing why each is important.

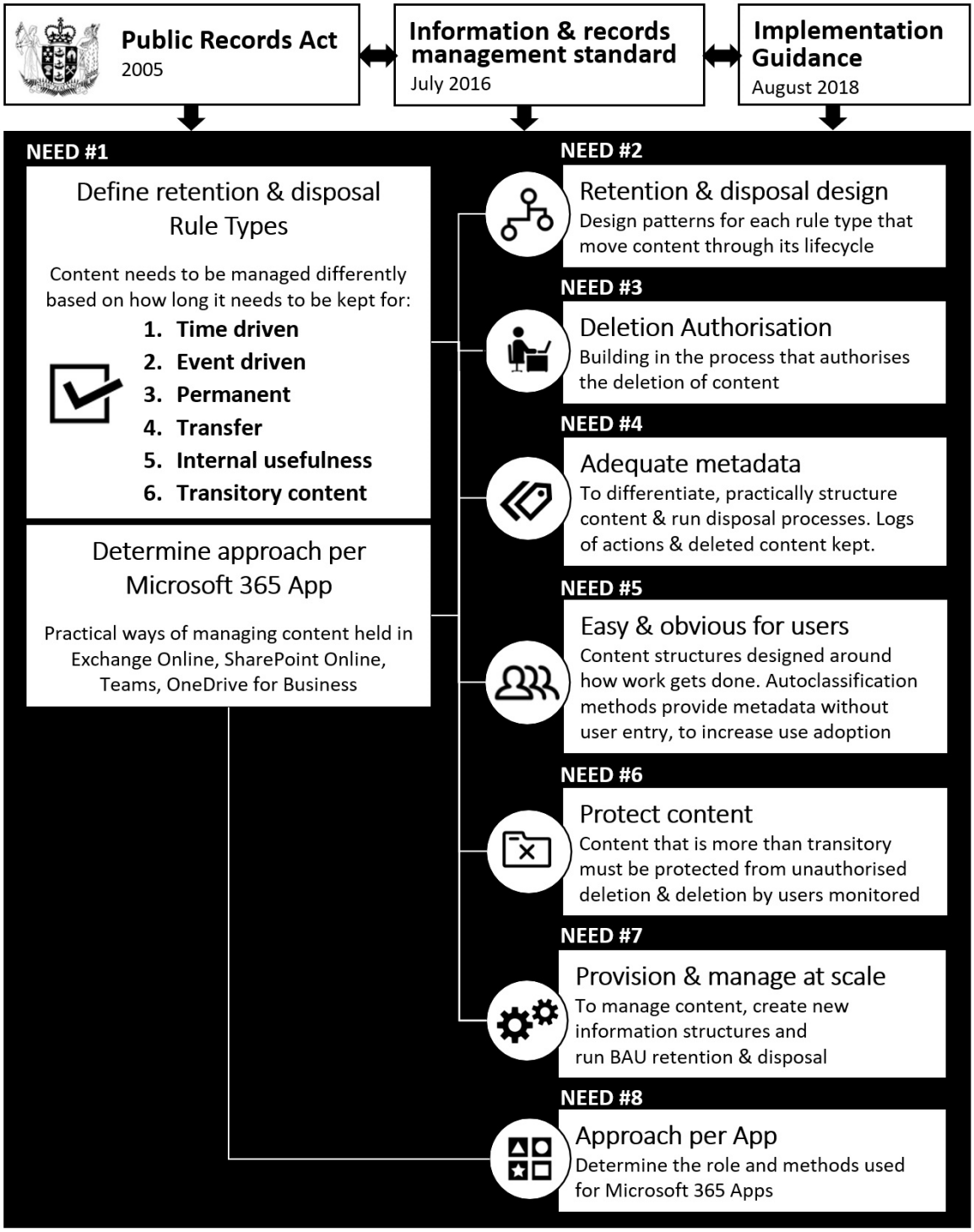


Figure 1 – Key Design Configuration Needs

Explanation of Design Configuration Needs

The following table provides an overview of the eight key design consideration needs within the framework.

	CONFIGURATION NEED	IMPORTANCE
1	**Define retention and disposal rule types**	By being able to define and identify the relative importance of different content, we can then manage it appropriately. For instance, not all records and information are of equal value, and more emphasis needs to be placed on the higher value record, especially those to be transferred to Archives NZ or permanently held. There are design challenges in managing this efficiently at scale. **Need 1** explains how to configure Microsoft 365 such that this identification can take place. Refer to: Section 2.1 Configuration Need #1: Rule types & Approach per App
2	**Retention and Disposal Design**	There is a range of functionality in Microsoft 365 that makes it possible to apply different disposal classes, triggers, and retention actions. **Need 2** explains approaches to design retention and disposal deliberately to use the right functionality for the right situation. We extend this explanation by providing a range of worked examples to assist Information Managers in understanding how this works practically. Refer to: Section 2.2 Configuration Need #2: Teams files/SharePoint Online retention & disposal design
3	**Deletion Authorisation**	Before content can be deleted/destroyed/removed, most organisations require that this action be officially authorised. **Need 3** explains the functionality provided to support this. Refer to: Section 2.3 Configuration Need #3: Deletion Authorisation
4	**Adequate metadata**	Metadata is a key tool for search, findability, providing context to information, and applying retention and disposal. **Need 4** describes how metadata needs can be catered for in the implementation of Microsoft 365. We also explain the functionality available in Microsoft 365 for the retention of metadata after the disposal has taken place. Refer to: Section 2.4 Configuration Need #4: Adequate metadata to provide context
5	**Easy and Obvious for Users**	One of the challenges of legacy EDRMS has been the usability of systems designed primarily for records management. In Microsoft 365, the end-user experience comes first, which means that adoption is higher, and hence more records can be actively managed. In designing the deployment of Microsoft 365 to support compliance grade information management, it is important that barriers to use are not introduced.

		Need 5 explains how to deploy Microsoft 365 in a way that enables good information management and makes it easy and obvious for users to do the right thing. Refer to: Section 2.5 Configuration Need #5: Easy and obvious for users to file content
6	**Protect Content**	Content must be protected from unauthorised deletion. There is various functionality in Microsoft 365 that can provide this protection. **Need 6** explains the design choices at play in determining which functionality and configuration of functionality to choose. Refer to: Section 2.6 Configuration Need #6: Protect content
7	**Provision and manage at scale**	The amount of content that can be created, held, and managed in Microsoft 365 is huge, even for small organisations. It is vital that when designing and deploying Microsoft 365, organisations consider how to design their deployment so that it works at scale and does not overwhelm Information Managers with tasks that could otherwise be automated. **Need 7** identifies approaches that can be used for working at scale. Refer to: Section 2.7 Configuration Need #7: Provision and manage at scale
8	**Approach per App**	Historically SharePoint (and now SharePoint Online) has been Microsoft's EDRMS equivalent. But many organisations have embraced Teams and OneDrive as well as needing an approach for managing email (Exchange Online). **Need 8** discusses specific design considerations for Microsoft Teams, OneDrive for Business, and Exchange Online. Refer to: Section 2.8 Configuration Need #8: Approach per App

Table 4 - Eight Key Design Configuration Needs

How to read this section

The following section is structured around each of the eight key design configuration needs outlined on the previous pages. For each need, it provides the following:

1. **Linkage to the Standard and Implementation Guide -** the link to the specific minimum compliance requirement along with the explanation associated with the requirement
2. **Tactics -** the tactics and approach for how to meet this requirement
3. **Application** - any specific considerations in how these tactics are applied in Microsoft 365

2.1 Configuration Need #1: Rule types & Approach per App

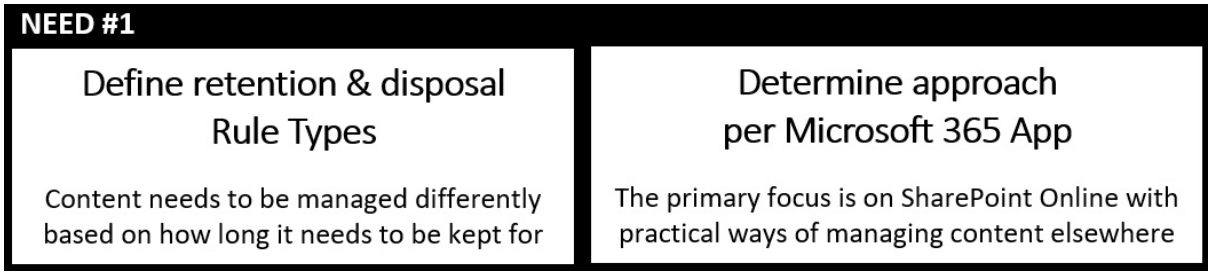


Figure 2 - Configuration Need 1

a) Linkage to the PRA Standard and Implementation Guide

2.1	Information and records required to support and meet business needs must be identified. *This work provides the foundation for understanding what information and records to keep. It identifies what systems and business processes are high-risk, high-value, or both for the organisation and the information and records required to support these.*
2.2	High-risk/high-value areas of business, and the information and records needed to support them, must be identified and regularly reviewed. *An organisation must identify the areas of high risk, high value, or both of its business. An organisation can better prioritise how it manages, treats, and protects these critical systems and the information and records they contain.*

b) Tactics

Content Lifecycles

PRA compliance requires that an organisation can identify the value of its content, so it can be appropriately managed:

Retention and Disposal Rule Types

MOST IMPORTANT…

- Type 1 **Transfer:** Files to be kept by transfer to Archives NZ
- Type 2 **Permanent:** Files to be kept indefinitely (e.g., Council property records)

NEEDS TO BE MANAGED…

- Type 3 **Event-driven:** Disposal triggered by an event (e.g., ten years after an asset is sold)
- Type 4 **Time driven:** Disposal based on time since the file was created or last changed
- Type 5 **Kept for internal administrative purposes** only – can be disposed of when operationally the files are no longer required. This reduces clutter, improves search, and reduces storage cost

UNMANAGED…

- Type 6 **Transitory content** that is up to users to keep or "soft" delete when no longer required into recycled bins (that can be monitored)

Approach for Compliance

The approach to compliance for Microsoft 365 in this white paper is to, where possible, use broad Retention Policies on mailboxes and sites that include Teams and other content.

Where needed to separate content for more fined tuned retention and disposal, retention labels can be used on mailbox and library folders and document sets and individual files.

The Design Challenge

Content (files, data, records) needs to be structured and organised to support people working efficiently and collaborating. This requirement practically means thousands of Mailboxes, SharePoint Online sites and document libraries, and hundreds of Teams. Retention and disposal rules act on these to separate content by how long it needs to be kept.

The design challenge is how to identify the retention and disposal rules needed and how to interconnect these to the content in the sites, libraries, and Teams:

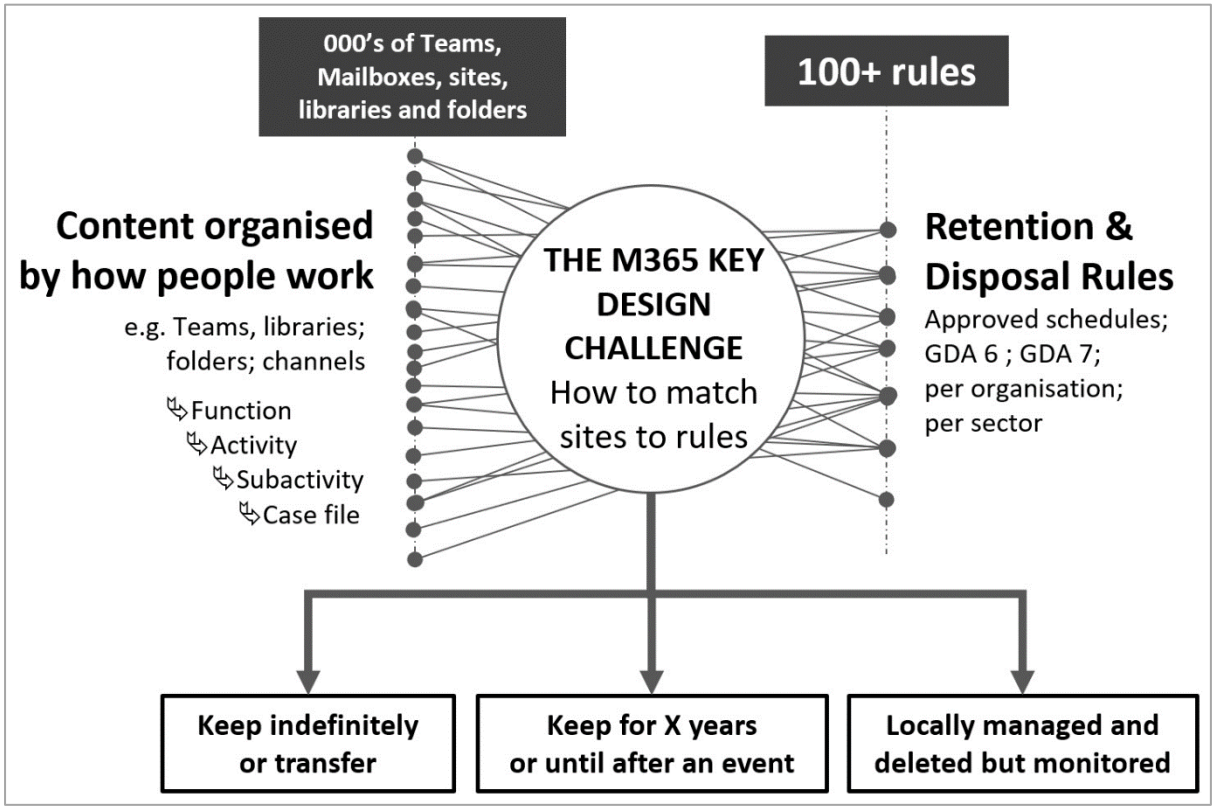


Figure 3 – The key design challenge of matching retention and disposal rules to workload content

One way to simplify this task is to rationalise retention periods into fewer groupings. For instance, five, seven, and ten year retention periods could be managed by a ten-year retention policy or label.

However, organisations should be careful about simplifying all retention and disposal to a single global retention policy on all content in a tenant, site, or mailbox. While this might prevent accidental or deliberate deletion of content, it is unlikely to meet their recordkeeping requirements and prevent legitimate and necessary disposal.

c) Approach for Teams and SharePoint Online

Linkage to the Standard and Implementation Guide:	
3.1	Information and records must be routinely created and managed as part of normal business practice *Policies, business rules, and procedures must tell an organisation's staff the requirements and responsibilities for creating, capturing, and managing information and records.*

Microsoft Teams allows users to access content from many sources.

Chat and channel messages. For detail on applying retention policies, refer to this link and this useful FAQ.

Email. Each Team channel has an email address. Emails and attachments are stored in a dedicated folder of the channel. Additionally, each Team is backed by a Microsoft 365 group where email is stored if not emailed to the channel but rather to the group.

SharePoint Online. When creating a new Team in Microsoft Teams, it is attached to a SharePoint Online document library that allows users to add files via a channel's "Files" tab. Emails and their attachments that have been sent to the channel mailbox are also stored in the document library. The document library can be configured with retention policies and/or labels. Refer to sections 2.3 to 2.7

Third-Party Apps. Although Microsoft Teams and other workloads can be integrated with third-party Apps (e.g., Trello, Survey Monkey), dealing with PRA compliance obligations for these third-party applications is out of the scope of this paper.

Application to Teams: A practical approach is to attach mailboxes and sites to default retention policies (for instance, retain for two years and then delete). If the Team's purpose is more than general collaboration, then the content may need to be retained longer or transferred to Archives NZ. This can be achieved through a combination of:

- Attaching the mailbox and site to a retention policy with a longer disposal period and/or
- Overriding the mailbox or site's policy with retention labels for important individual records and/or
- Using advanced features to attach a retention label to a site, document library, document set, or folder

SharePoint Online document libraries used alone or via Teams provide EDRMS level functionality through out-of-the-box configuration and design. This functionality includes managing files, folders, subfolder structures, standardised metadata, version control, search, etc. The libraries, appropriately configured, are the primary repository for content covered by Retention and Disposal Rule Types 1-4.

This scope includes Microsoft Stream content.

Document libraries are also suitable for managing Type 5 and 6 data and can be configured to be separated from the more important content.

Refer to sections 2.2 to 2.7 for more information on the above.

d) Approach for Email and OneDrive

Linkage to the Standard and Implementation Guide:	
3.1	Information and records must be routinely created and managed as part of normal business practice *Policies, business rules, and procedures must tell an organisation's staff the requirements and responsibilities for creating, capturing, and managing information and records.*

Exchange Online

Exchange Online requires an information management policy for email that needs to be managed (i.e., Types 1-4)

- Users (or automated processes or classifiers) are expected to forward or copy into SharePoint Online content that needs to be separated into higher value retention and disposal types 1-4. As outlined in the tactics section, many organisations that have existing EDRMS systems use this tactic.
- In Exchange Online, use Retention Policies to apply broad retention & disposal as a safety net. This approach could be the same policy for all users or differing retention periods based on their role and business activities.

e-Discovery can analyse and return/cover content if required.

Refer to section 2.8 Configuration Need #8: Approach per App for more information on above.

OneDrive for Business

Microsoft 365 includes OneDrive for Business, which provides a place in SharePoint Online for each user to store files (similar to home drives on shared file servers). This approach creates a personal site in SharePoint Online for each user with a document library.

Refer to the section on 2.8 Configuration Need #8: Approach per App for more information on the above.

Note that OneDrive accounts provided by Microsoft's consumer offerings should not be used to hold business content.

2.2 Configuration Need #2: Teams files/SharePoint Online retention & disposal design

Most organisations have a wide range of content and types of retention and disposal (R&D) rules to manage. The rules need to be effective in moving content through its lifecycle and being efficient and transparent for the information managers to have oversight and administer.

a) Linkage to the Standard and Implementation Guide

3.6	Information and records must be kept for as long as needed for business, legal and accountability requirements. *An organisation must implement policies, business rules and procedures to ensure that information and records are kept for as long as required and to identify how their disposal is managed.* *Information and records must be sentenced and disposed of in line with the practices of authorised disposal authorities.* *Information and records of permanent value that are identified as public or local authority archives must be transferred to Archives New Zealand, an approved repository, or a local authority archive, when authorised and no longer needed for business purposes.*

b) Tactics

Design of content structures (Teams, channels, sites, libraries, folders) needs to identify content based on the different disposal classes, triggers and retention actions outlined in section 2.1 Configuration Need #1: Rule types & Approach per App.

The tactics required to run retention and disposal are:

- Having adequate metadata to drive the rules (2.4 Configuration Need #4: Adequate metadata to provide context)
- Using autoclassification of retention labels and other metadata (2.5 Configuration Need #5: Easy and obvious for users to file content) so that retention and disposal rules can be attached to document libraries, mailboxes, etc
- Using provisioning (2.7 Configuration Need #7: Provision and manage at scale) to do this efficiently and consistently at scale

In many cases, content pending disposition needs to be reviewed and approval given to dispose (2.3 Configuration Need #3: Deletion Authorisation). This requirement needs to be factored into the approach chosen.

c) Application in document libraries

Document libraries hold files created and worked on in Teams as well as other SharePoint Online sites. There is a range of technology approaches available to choose from:

- **Microsoft 365 document libraries provide robust EDRMS capabilities** (e.g., security & permissions, content hierarchies, metadata types, version control, basic retention & disposal, and managing user or system deletion).
- **Advanced features** provide additional security, sensitivity, monitoring, and retention & disposal functionality. This functionality includes allowing libraries, folders, and document sets to inherit or infer metadata and retention labels onto files
- **Power Platform** for supporting business processes, surfacing information and alerts to users and information managers
- **Power BI** can provide dashboards of compliance information for review, alerts, and action.
- **Use of PowerShell commands.** Refer to this example of how to use the functionality in automated and programmed ways

d) Using Retention Policies and Retention Labels

Microsoft 365 supports a wide range of retention and disposal processes through:

- **Use Retention policies** to apply default retention at a site level. The result is that all libraries, folders, and document sets in the site inherit this retention policy
- **Use Retention labels** to determine retention and disposal actions and status. With advanced features, they can be applied at the library, folder, or document set level. This includes the common case of wanting to override a default policy where a library needs multiple retention periods to be applied. Through retention label policies, users can also be empowered to override the above (e.g., marking an important document that should be kept longer). This provides a default and straightforward way to set up practical retention and disposal

Retention labels or policies can do each of the following:

- **Retain and then delete** (e.g., retain all changes to a file for X years then delete it)
- **Retain-only** (e.g., retain all changes to a file for X years, then keep the latest version of the file and delete the saved changes). From X years, changes can be made to the file
- **Delete-only** (e.g., allow the user to make changes or delete the content as they wish but delete files that have not been modified for X years)
- **Trigger a disposition review** (an advanced feature) so that the disposal is manually approved or rejected

Learn about retention policies and retention labels for further details on the differences between retention policies and labels.

Designing for multiple retention types in a document library. In many cases, a library (used directly or via Team's "Files" tab) will need more than one retention period applied to it. A standard pattern is:

a) Optional policy on the library
b) Default retention label at library or folder level
c) Override the default in b) with a label at the folder, subfolder, or file level
d) Optionally allow user override at the file level

Classifiers. Retention labels can also be set by advanced features (2.3 Configuration Need #3: Deletion Authorisation).

- Pattern Matching (keywords, alphanumeric patterns, metadata, file properties)

- Built-in and Trainable classifiers
- Based on metadata or file properties (e.g., a content type defined in SharePoint)

Refer to Learning about trainable classifiers for more information.

Also, when more than one retention policy is attached to a site or mailbox, the following is used to determine which one takes precedence. This also applies when a combination of policies and labels is used.

Retention & disposal worked examples and use cases

SharePoint Online/Teams practical walkthrough

The process below is based on the logic in the preceding sections. It is geared to the finer demarcation for selecting retention types that is available (by document library, folder, and/or document set). Information managers can apply this process to each document library, or automated provisioning could apply this as part of standard settings.

While there are usually thousands of libraries in an agency's deployment, the information manager is only actively involved in the greyed first stage. The remaining actions & processes are automated by Microsoft 365.

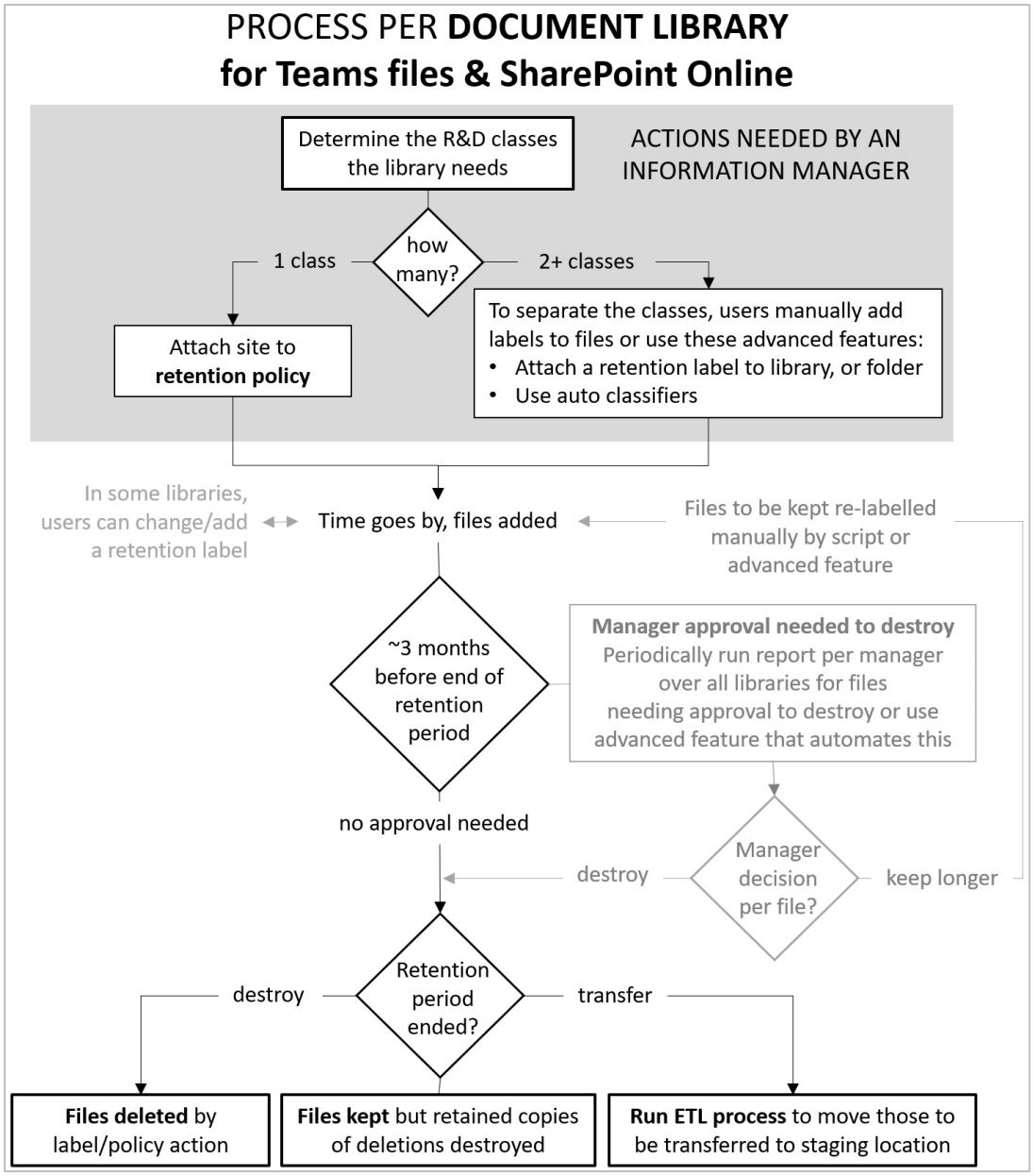


Figure 4 - Process for setting retention and disposal per document library

(i) Governance meetings example

Say a Team for governance meetings has been designed with a channel per meeting, and the Files tab has two subfolders that users drag/drop files into:

1) One for meeting administration
2) The other for meeting papers such as agenda, meeting documents, and minutes

Retention is applied as follows:

- The Team's SharePoint site can be attached to a 'retain for two years' retention policy. This will inherit down to all content in the library
- The folder with the agenda, meeting documents, and minutes for each meeting uses an advanced feature to tag the folder with a 10-year label that overrides the two-year label
- In this way, the clutter of administration is disposed of after two years while the higher value content is kept for a longer period
- If the longer retention period is only needed for a small number of individual files, users can manually apply a retention label to each

(ii) Major and minor documents example

Below is an example from GDA 6 (General Disposal Authority 6 has been developed for the use of public offices wishing to dispose of common corporate public records legally. GDA 6 covers generic classes of records created through business functions, which are common to most public offices).

Class & Description	Action needed
Class 2.2.2 Legal Opinions that set a precedent relating to the agencies policy and procedures	Transfer to Archives NZ after ten years
Class 2.2.3 Legal Opinions that do not set a precedent	Destroy After seven years

Table 5 - Major and minor documents example

This can be designed for in SharePoint Online by creating separate retention rules using one of the following:

- **Separated.** Hold 2.2.2 and 2.2.3 content in different Teams, sites, document sets, document libraries, or folders – this is the most straightforward. However, in cases like this, it may not be how a department would want to work. Refer to the Governance Meetings section above, where content is separated into folders
- **Manual.** All content is stored together in the same Team, library, or folder. Key staff need to override the default retention label per file or document set (e.g., "Legislative Submissions and Legal Opinions 2.2.3" - no precedent replaced with "Legal Opinions that set a precedent 2.2.2") label
- **Business Process.** There could be a business rule that requires Legal Opinions setting a precedent to be approved. The approval workflow could also override the default label
- **Automated rules.** Inference rules based on the filename (e.g., Legal Opinion-precedent setting xyz.docx). Some options to consider for this are as follows:
    - Leveraging Power Automate - this may prove to be complex as it may require hundreds of rules depending on the number of Teams and/or libraries.
    - In some cases, classifiers can achieve this efficiently by finding patterns in content to set retention labels. This also includes the ability to train a classifier to identify those documents

- Consider leveraging SharePoint Syntex for this and to extract metadata, which is later used to apply retention labels.

(iii) Working and Final Content example

Similar logic would apply to the common use case of working versus final content. From GDA 6:

Class & Description	Action needed
Class 1.2.2 Business Unit Contribution to Corporate Plan An individual business unit's contribution to strategic or corporate planning.	Destroy when administratively no longer required
Class 1.2.3. Administrative Planning and Reporting Administrative and operational planning and reporting records.	Destroy After seven years

Retention and disposal can be designed for using the Governance Meetings pattern defined on the previous page. Users would easily get used to a "working" folder for drafts and working copies and a "final" folder for what has been agreed/approved. Alternatively, working content could be at the root level and covered by a site retention policy. This would then have override labels per folder or document set for "final" content.

(iv) Event-based retention and disposal example

In these cases, the trigger date to commence disposal actions is not necessarily known when content is created or modified. This rules out using the standard retention policy or label rules based on "Created" or "Modified" dates. Some examples from GDA 6:

Class & Description	Action needed
Class 4.2.5 Lease Agreements. Leasing agreements and contracts on capital items, e.g., buildings, land, major plant, etc	Destroy Seven years after termination of lease agreements
Class 8.1.1 Purchase, Development & Operational Management of Systems used to Manage &/or hold Records	Retain for the active life of the system

Several approaches are possible, including:

Manual or automated, so when a lease is terminated in the lease management system, it triggers an event in Microsoft 365.

This can apply a label to a file, folder, or library after the event happens (e.g., termination of the lease) that will start the disposal countdown. In the case below, the five-year countdown starts when the label was applied.

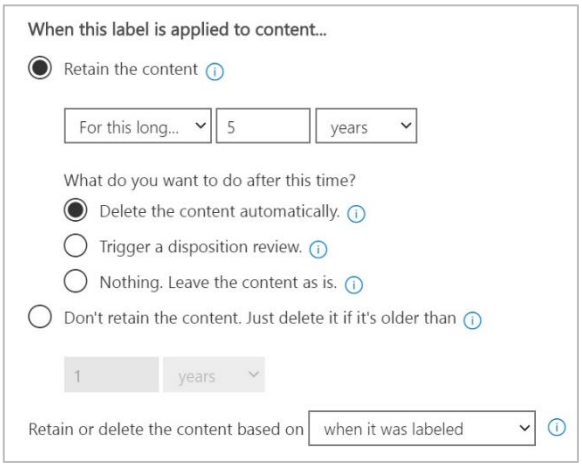


Figure 5 – Screenshot example showing dialogue for setting event-based retention and disposal

However, there needs to be a way of protecting the content before the trigger event (e.g., termination of the lease) happens. This can be done by the content having a label that has a long retention period (e.g., 50 years). The label to commence the disposal countdown replaces this.

As the process is manual with many cases to manage, this would require significant ongoing time, as well as an overview to confirm it is happening.

Event-based labels. This advanced feature specifically caters to this use case. A file, folder, document set, or library can be tagged with a label for a particular event. For instance, a lease would be given Asset ID.

When the lease is terminated, an Event entry needs to be created. This could be done by one of the following methods, so that if the lease was terminated on 1/1/2020, then this becomes the trigger date to start the disposal countdown:

- An information manager or admin person manually adding this information
- Power Automate as part of the lease process
- Triggered by the lease management system

These methods automatically protect the content from deletion and records changes in the preservation hold library before the trigger date is known. For a range of methods, refer to start retention when an event occurs link.

Refer to this link for an example:

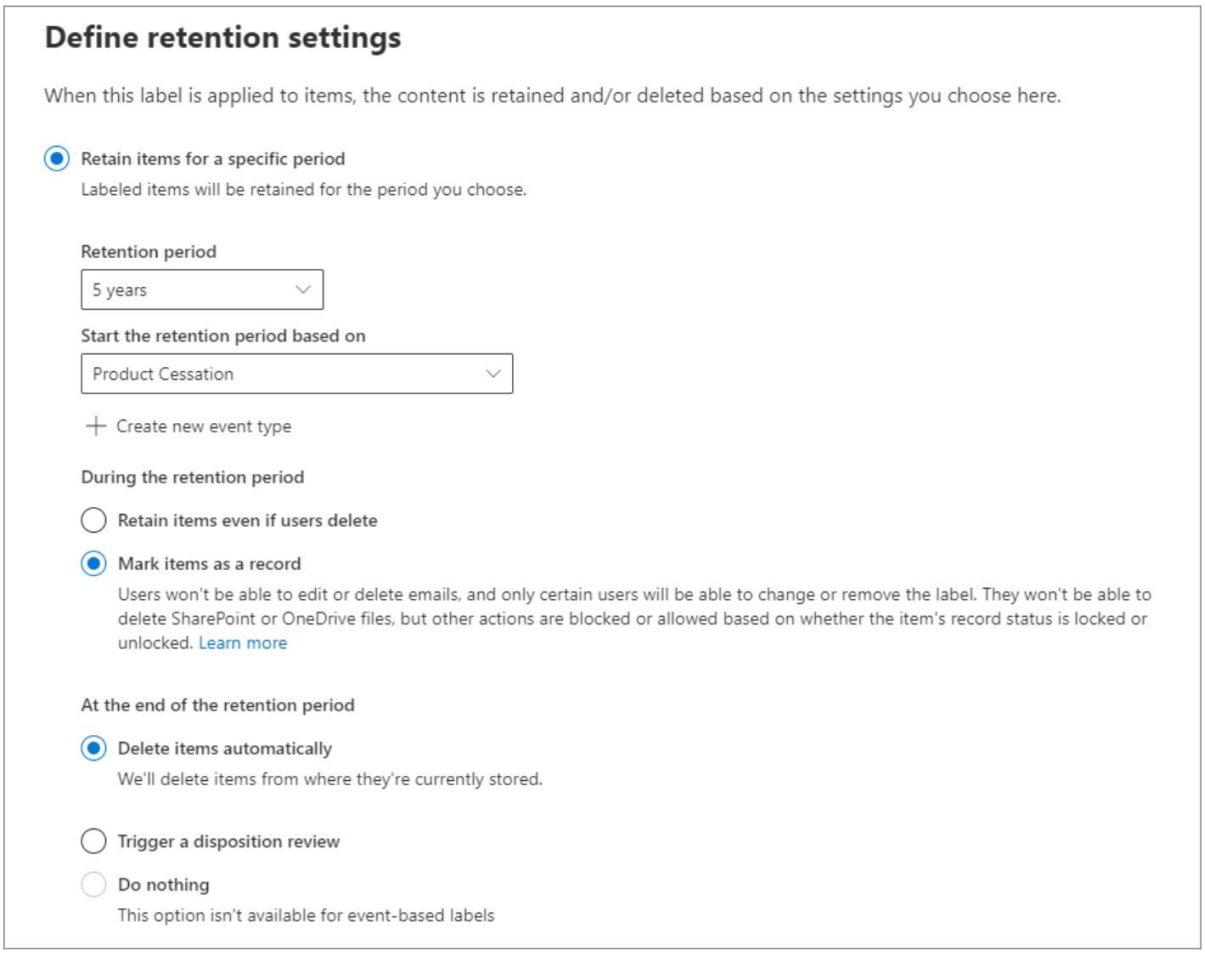


Figure 6 - Screenshot example showing dialogue for event-based retention and disposal actions

(v) Content to be kept indefinitely example

Retention labels can do this by attaching a retention label to the file or with advanced features to a document set, folder, or library:

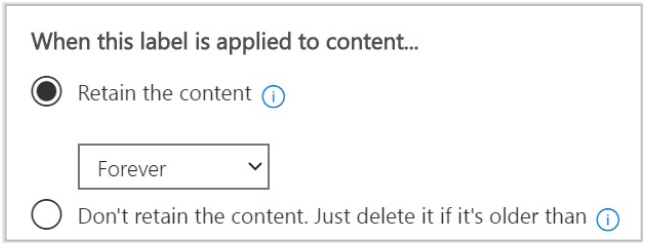


Figure 7 - Screenshot example showing the setting for keeping content indefinitely

An alternate approach is to apply the “record” label to a file, folder, document set, or library (an advanced feature). Note that the language used is based on a record being “declared.” This is not the New Zealand legislative model, as files and other content are records as soon as they are created.

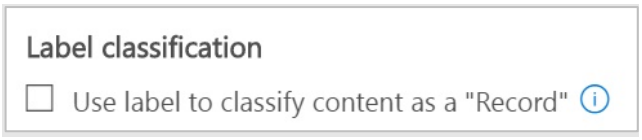


Figure 8 - Screenshot example showing a record classification being attached to a file

While this will not stop users from changing the content, a copy of the previous version is retained in the preservation hold library for each site).

(vi) Transfer to Archives NZ

In this case, content and its metadata need to be batched and packaged into a format suitable for transfer to Archives NZ. This is a standard ETL (extract, transform, and load) process.

- **Extract.** The content to be transferred needs to be identified. Out of the box, retention policies and labels only have three actions (do nothing, delete, and manual disposition), none of which achieve what is needed here. Instead, a search or eDiscovery query can be created that will identify files to be transferred based upon the retention label they have and the date the records were created and last modified)
- **Transform.** The files and their metadata identified above can be converted using code or scripts into the format Archives NZ requires. eDiscovery and its export functionality could also be used for this purpose
- **Load**. Archive NZ has a set ingestion process to be followed to transfer the files. They should also be deleted from the tenancy (e.g., by script or code) once it is confirmed the transfer was successful and Archives NZ's needs have been met

Third-party migration Apps can also move files to/from Microsoft 365 or leverage the in-platform code.

(vii) Content kept for administrative purposes or transitory content example

Two example approaches are:

- **No mandated retention period.** An unmanaged approach would be to not use retention labels and policies and just leave it up to users to decide what to keep.

- **Retain for a nominated period.** For instance, retain the content for at least two years and then automatically delete it. During the year, users could delete content that is not needed, but a copy would be held in the site's preservation hold library for the year and then deleted via the recycle bin process

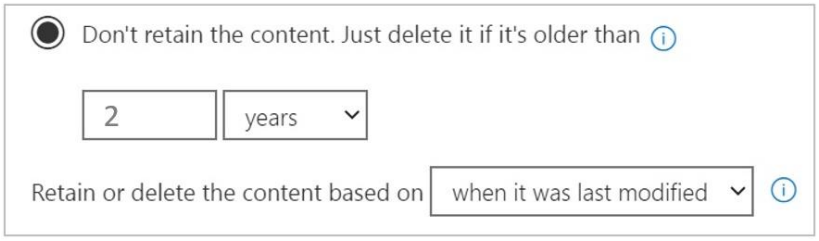


Figure 9- Screenshot example showing the setting to keep content for two years

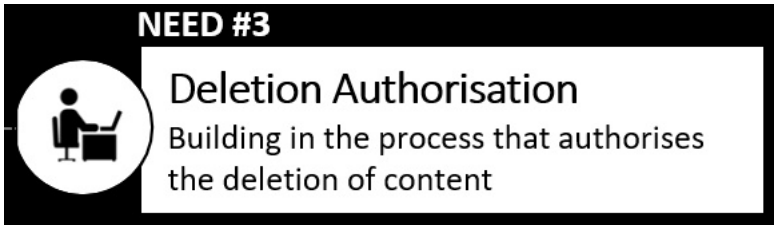
Both approaches are practical but unlikely to be liked by all users. While no mandated period gives freedom to users to keep what they need, the downside is that they end up not removing content, which leads to information clutter.

Retaining for a period of time may annoy some users who have content they want to access for a longer period. Tactics to make this more acceptable include:

- Users can move the content to other libraries or subfolders that have longer retention periods
- Users can add retention labels themselves to files they wish to keep
- Reports can be written and sent to users on files that are due to be deleted

The exception for Teams use is where the purpose of the Team is general collaboration. In this case, a retention policy can be applied that retains the content for a nominated period of time then disposes of it.

2.3 Configuration Need #3: Deletion Authorisation



a) Linkage to the Standard and Implementation Guide

3.7	Information and records must be systematically disposed of when authorised and legally appropriate to do so. *An organisation must implement policies, business rules, and procedures that identify how the disposal of information and records is managed. This includes:* *- assigning responsibility for sentencing and disposal of information and records (sentencing is using a disposal authority to decide whether to keep, destroy or transfer a record)* *- using disposal authorisation processes* *- implementing disposal actions* *- deleting metadata* *- decommissioning systems* *- documenting the disposal of information and records.*

Most agencies typically manage this through a process run by the Information Management Team with final approval given by the relevant senior manager (usually the business owner of the content). This usually takes the form of an electronic report of files for the disposal that they sign-off.

Some organisations will mandate this as part of their information policies to reduce the risk of key information being lost.

b) Approach for Microsoft 365

Use the disposition review advanced feature

The native behaviour for labels and policies is to trigger a disposition review:

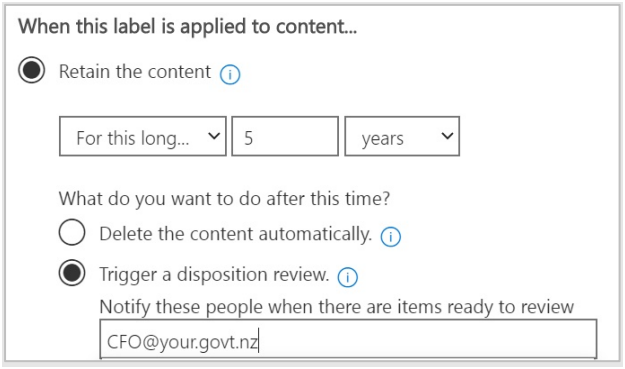


Figure 10 - Screenshot example showing the setting to gain manager approval for disposal

This creates a review list that the manager can browse and set actions per record:

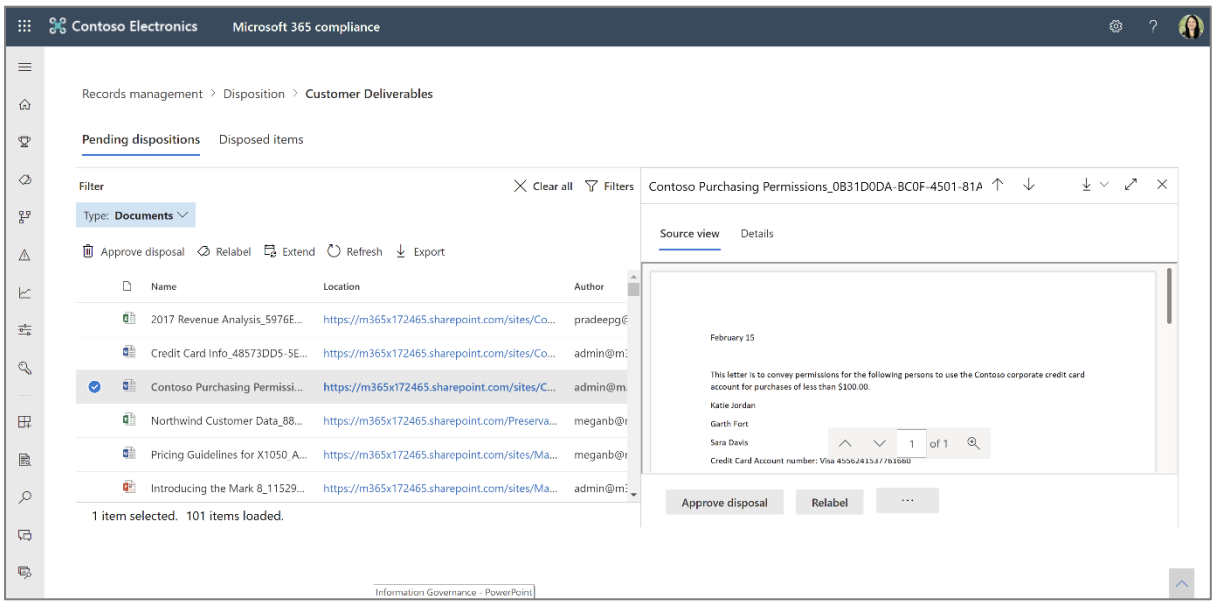


Figure 11 - showing how a manager reviews documents set to be disposed

However, this is unlikely to be used at scale as the manager has to approve, extend the retention period, or tag with another label each record in turn. Potentially a list of the files to be reviewed can be exported and interacted with within Excel. A process would then be developed to update the action to be taken on each file based on the manager's decision. Refer to the disposition of the content link for more information.

We are aware that Microsoft is working on an improvement to this process that may be available shortly.

Practical alternative: batched reporting just prior to disposal

Reports can be created by the function and activity of files that are due to be deleted. This can be done by a search query on files with a particular label and where the period of time is almost up (e.g., three months before the retention period ends).

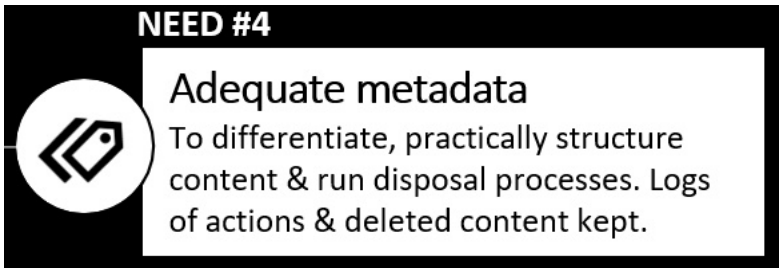
The report could be formatted and sent to the manager for review. This could use the Power Platform (app, workflows, and BI dashboard).

The authorising manager would review and give feedback on exceptions, potentially live on the dashboard. This could include instructions to do one of the following:

- Delete the content as per schedule (which will automatically happen)
- Keep the file for longer (e.g., by changing the label)
- Have an information manager review its value

The files where the label had not been removed or another reapplied at the end of the period (e.g., five years) would be automatically deleted. The file would remain available in the recycle bin and then for a further period in the tenancy backup. This logic simplifies the process and considers that almost always all files would be approved for deletion.

2.4 Configuration Need #4: Adequate metadata to provide context



a) Linkage to the Standard and Implementation Guide

Sufficient metadata needs to be created and kept:

3.2	Information and records must be reliable and trustworthy. *An organisation's information and records must have enough metadata to ensure they are reliable and trustworthy.* *Information and records must be accurate, authentic, and reliable as evidence of transactions, decisions, and actions. This requirement ensures that information and records have appropriate minimum metadata to provide meaning and context (including te reo Maori) and that this metadata remains associated or linked.*

Metadata is kept on the disposal of records and under what authorisation they have been disposed of.

3.7	Information and records must be systematically disposal of when authorised and legally appropriate to do so. *An organisation must be able to account for their disposal of information and records in business systems, outsourced arrangements, and physical storage. This includes providing evidence that the disposal of information and records is permitted and authorised under disposal authorities' and legal obligations, including the Public Records Act 2005.*

b) Application for Teams files and SharePoint Online

Standardised designs. The document libraries used stand-alone or via Teams should be created from standard templates to be "ECM Compliance libraries." These have locked down permissions so that the settings are protected. The following metadata types can be catered for:

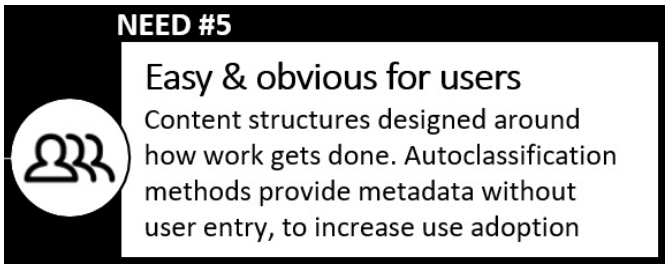
- Free text and pick-list based metadata
- The business classification (e.g., function, activity, sub-activity, case file) as well as other hierarchies
- The type of document (e.g., contract, report, submission)
- Status/condition related (e.g., the close date of a case, whether the content is 'working' or 'final,' tags for privacy or security)
- System related (e.g. created / modified dates; creator /modifier names); and
- Recordkeeping metadata (e.g., the status of the record, disposal class and actions, trigger dates)
- Unique document ID can be turned on via a library setting

Log records of deletion. When files are deleted, they move through a recycle bin process. The actions associated with this are recorded in log files. Entries are kept for a period of time and then deleted.

The PRA requires that records of deletion be kept. This can be achieved by:

- The proof of disposal feature will keep metadata of all records disposed
- Snapshots of the audit log files of deletions to a permanent database using low-code methods. This would include sourcing a file's metadata to capture key metadata such as the business classification and the retention label if one was applied.
- Other methods including third party Apps

2.5 Configuration Need #5: Easy and obvious for users to file content



a) Linkage to the Standard and Implementation Guide

3.1	Information and records must be routinely created and managed as part of normal business practice. *Policies, business rules, and procedures must tell an organisation's staff the requirements and responsibilities for creating, capturing, and managing information and records.* *An organisation must regularly assess or audit its practices to demonstrate that its business rules, procedures, and systems are operating routinely.* *An organisation must identify, resolve, and document any exceptions that affect the creation, integrity, accessibility, and usability of its information and records.*

Despite EDRMS/ECM systems being deployed in agencies for the past 20 years, many organisations still have ballooning file shares, Outlook mailboxes, and Google drives, etc.

User expectations of adoption. The expectation is that users and processes will store content in the system, so that content can be managed. However, if users do not know what to do or it is too time-consuming, then in practice, they choose not to put their content in the system. Therefore, the system needs to be designed with usability, efficiency, and usefulness in mind so there is a "reasonable expectation" that users will store their content in it.

This is the primary challenge for practical compliance, with many existing legacy systems having good functionality but low user adoption because users perceive that the system is too hard to use. Microsoft 365 does not require users to learn a new system or to have to move their content. It just provides compliance by design that's invisible to them most of the time.

The tactics below can be complemented by the use of Microsoft's Information Protection Scanner and Microsoft Cloud App Security to identify information assets in these services to then ensure they are moved to SharePoint Online.

b) Tactic: Teams & Site structures aligned to how work is organised

Design for SharePoint Online

Suitable design for SharePoint Online includes:

- **Libraries and their folders and document sets** are organised by key metadata. Commonly this is by business classification (where individual columns hold between them the hierarchy or a Term Store is used) as well as standard metadata columns
- **Folders** can be used to separate "working" from "published" or "final" content. This can allow the content in the folders to be tagged for different retention and disposal actions
- **Retention labels and policies** can be applied that provide for the recordkeeping metadata and actions. Refer to section 2.2 Configuration Need #2: Teams files/SharePoint Online retention & disposal design for more detail.

Design for Microsoft Teams' document libraries

Suitable design for Microsoft Teams includes determining whether the Team will hold content that needs to be formally retained and disposed of (Types 1-4). If so, the Team's SharePoint Online document library should be designed in line with the above. This can include:

- **Matching the Microsoft Team structures to business classification or other hierarchies**. For example, The first-tier folder is the channel name, and subfolders can be added under this. The channel and these subfolders can be based on the business classification or other metadata (e.g., a Team for Property Ground Maintenance might have a channel per ground and a folder per work type. This can mean Case=Ground and Subactivity=work type)
- **Locking down administrative rights.** The Team's document library is configured with all the compliance and security settings of other document libraries. This includes locking down permissions to change the library's settings so only administrators and information managers can make changes
- **Making library content available to a wider audience.** In many instances, more people will need to browse and search the files created within a Microsoft Team. The permissions of the Team's SharePoint site need to be altered to take this into account

The following FAQ for Teams compliance may be helpful.

For Teams that do not have Types 1-4 content, then it is usually reasonable to just allow users to delete the content and Team when it is no longer required.

c) Tactic: Auto application of metadata

Experience has shown that it is reasonable to expect users will adopt the system if it is simple for them to drag/drop the file or email into an obvious location. A key adoption enabler is to remove the need for users to enter metadata. While this may not always be possible, in most cases, autoclassification methods can be used.

Design in SharePoint Online, including for Teams files

Where to store content needs to be obvious. SharePoint Online navigation menus can be designed to make it obvious where content should be created, stored, collaborated on, and found.

- Drag/drop or create records in the correct library, folder, or document set, and design the library such that recordkeeping metadata is auto-applied
- Drop files into Teams conversations or the File tab within channels
- A Teams channel can have an email address. This means content emailed to the channel is stored in the channel's folder of the document library, in a subfolder called "Email Messages."

Use inheritance from a location. Base the library creation and architecture as much as possible on autoclassification of key metadata:

- Metadata can be automatically applied through inheritance from the library, folder, or document set defaults. This can be applied manually or by script or an App. For retention labels, advanced features are required
- Content moved from another library/place inherits the new location's metadata inheritance and inference. Note that this works for both retention labels and document sets. For other cases, other methods are needed to detect when a file already has pre-set metadata that needs to be updated

Approaches can be used to infer metadata based on the filename, other metadata, or the content of the file. This means creating rules based on finding keywords or phrases in the file or its metadata and then setting retention labels or other metadata accordingly.

Autoclassification by pattern matching

Advanced features include the ability to find and classify content by:

- Keywords or metadata values (keyword query language). Refer to Keyword queries and search conditions for the Content Search link for further information
- Using previously identified patterns of sensitive information like social security, credit card, or bank account numbers (sensitive information type entity definitions). 100+ out-of-the-box patterns trained by Microsoft are available

This enables sensitivity and retention labels to be automatically applied for data loss prevention (DLP) and for the automatic application of policies for retention labels.

This can be extended by using the KQL (keyword query language) to update metadata and/or labels by pattern matching to existing metadata, including the filename.

Autoclassification by out-of-the-box classifiers

A growing number of classifiers that can be used to set metadata, retention, or sensitivity labels including:

- **Resumes**: detects items that are textual accounts of an applicant's personal, educational, professional qualifications, work experience, and other personally-identifying information
- **Harassment**: detects a specific category of offensive language text items related to offensive conduct targeting one or multiple individuals based on the following traits: race, ethnicity, religion, national origin, gender, sexual orientation, age, disability
- **Profanity**: detects a specific category of offensive language text items that contain expressions that embarrass most people
- **Threat**: detects a specific category of offensive language text items related to threats to commit violence or do physical harm or damage to a person or property

Autoclassification by Trainable Classifiers

This advanced feature's classification method is particularly well suited to content that is not easily identified by either the manual or automated pattern matching methods. This method of classification is more about training a classifier to identify an item based on what the item is, not by elements that are in the item (pattern matching).

A classifier learns how to identify a type of content by looking at hundreds of examples of the content you are interested in classifying. The number of examples needed is based on the diversity of content and differentiation required. You start by feeding it examples that are in the category. Once it processes those, you test it by giving it a mix of both matching and non-matching examples.

The classifier then makes predictions as to whether any given item falls into the category you are building. You then confirm its results, sorting out the positives, negatives, false positives, and false negatives to help increase the accuracy of its predictions.

When you publish the trained classifier, it sorts through items in locations including SharePoint Online, Exchange, and OneDrive, and classifies the content.

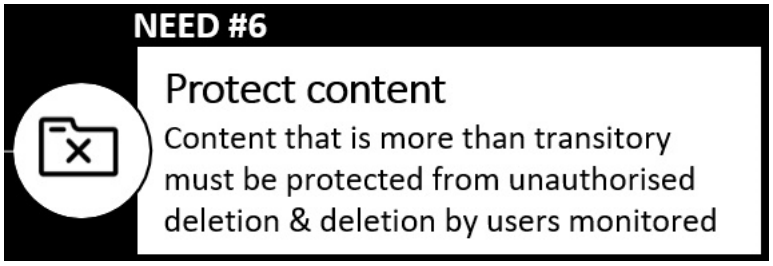
For further information, refer to Creating a trainable classifier link. This also includes the ability to train a classifier to identify those documents or even using SharePoint Syntex for this and to extract metadata, which is later used for the application of retention labels.

Users manually applying retention labels

An administrator can associate a Label Policy with a site and its libraries and within mailboxes. This holds a list of labels that users can tag a file with. This is straightforward to access and use but comes with caveats:

- All users who have 'write' access can apply labels. You cannot block a user from applying a label if they have 'write' access
- It works best for exceptions to the default library or folder settings, where the user has the subject matter knowledge to make the call that a different label to that automatically applied is appropriate

2.6 Configuration Need #6: Protect content



a) Linkage to the Standard and Implementation Guide

3.4	Information and records must be protected from unauthorised or unlawful access, alteration, loss, deletion and/or destruction. *An organisation must protect information and records* *Security measures must include:* *- access and use permissions in systems*

b) Tactics

Users can delete content from SharePoint Online document libraries. A range of safeguards are available:

Stop deletion

- In some cases, user permissions can be limited (e.g., "read-only" rights set at library or folder level)
- Using the "record" retention label (an advanced feature) to lock down a file. Refer to the following link for further information
- Setting a retention label or policy to retain content. In SharePoint Online, this then trips copies of changes to files or deletions to be sent to the site's Preservation Hold" library. Refer to the section "If the content is modified or deleted during the retention period, a copy of the original content as it existed when the retention policy was assigned is created in the Preservation Hold library" in the following link

Monitor deletion

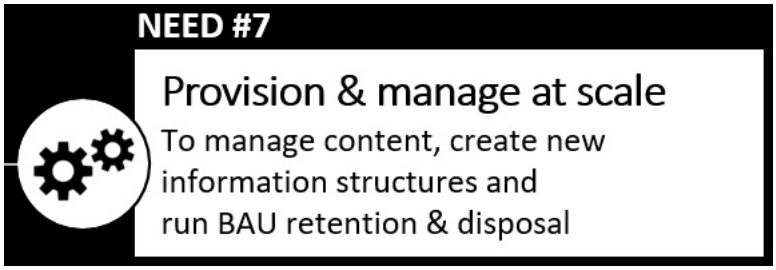
- Information managers can monitor audit logs for deletion and other user actions. Refer to the following link for further information
- Audit logs are only held for a limited period. As an advanced feature, this can be up to one year
- The Compliance Centre dashboard with Microsoft 365 has a wide range of reports to assist

Deletion process controls

- Dual-stage recycle bins hold SharePoint Online files that have been deleted by users. They remain here for 93 days before being permanently deleted

Refer to Learn about retention for SharePoint and OneDrive link for more detail

2.7 Configuration Need #7: Provision and manage at scale



Organisations are likely to have thousands of sites where content is stored. Each will have its own settings. It is not practical to expect these sites would be manually configured.

a) Linkage to the Standard and Implementation Guide

2.3	Information and records management must be design components of all systems and service environments where high-risk/high-value business is undertaken. *An organisation must consider at the start how to make **system maintenance, migrations and decommissioning easier**. In taking this "by design approach" an organisation must ensure:* *- systems specifications for information and records that are high-risk, high-value, or both, include requirements for managing them* *- systems specifications include requirements for minimum metadata needed to support information and records identification, usability, accessibility and context*
2.5	Information and records management must be designed to safeguard information and records with long-term value. *Once the organisation knows what information and records are needed long-term and where they are kept, it can safeguard and manage them.*

b) Tactics

For practical compliance, the document libraries need to have many specific settings for 'PRA grade' use. E.g., architected for security, metadata, autoclassification, and retention and disposal.

Application in SharePoint Online and Teams

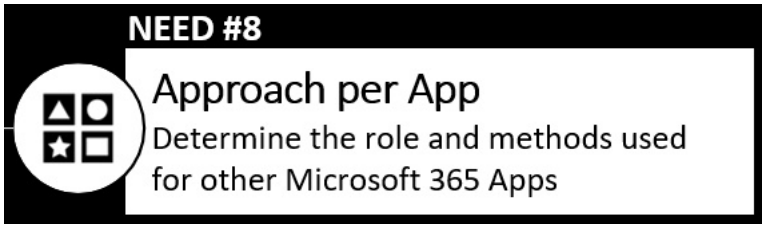
There needs to be a reasonable expectation that the methods chosen will be consistently used by information managers. With potentially thousands of Teams and sites, it is not practical to individually configure Teams, sites, and libraries from generic templates.

The application of specific settings can be made through:

- SharePoint Developer Community (SharePoint PnP) resources
- PowerShell scripts
- Third-party Apps

Library and folder level inheritance makes PRA compliance much easier. A library could easily have tens or hundreds of folders.

2.8 Configuration Need #8: Approach per App



Exchange Online

Mailboxes hold email, calendar, planner, chat content per user or group.

In Exchange Online, retention policies can be applied:

- per mailbox
- based on content (e.g., emails with sensitive information or specific words/phrases)
- based on content derived from known templates (contracts, architecture documents, patent documents) identified using trainable classifiers

For content with retention and disposal types 1-4, when it is difficult or time-consuming to set up and maintain retention policies to differentiate how long the content should be kept for, a complementary approach can be used. In this case, the content can be copied or moved into SharePoint Online document libraries. This is the custom and practice for legacy EDRMS where emails and locally created files are expected to be copied into the EDRMS rather than being stored in the email system or home drives.

Teams email. For Teams, a channel has an email address that stores the email and attachments in SharePoint Online in a subfolder of the channels' folder of the Team's library. Users can then forward or copy emails to this as a simple way of ingesting important information into SharePoint Online.

Forward to SharePoint Online. Users to copy or forward important emails and their attachments to SharePoint Online if this is easy for them. This can include via:

- Outlook supports drag/dropping emails and/or their attachments to document libraries via One Drive for Business synchronisation in File Explorer
- Teams have email addresses, so key emails can be sent to or forwarded to Teams. The emails and attachments are then automatically saved in the Team's document library
- Third-party Apps

Use retention policies as a safeguard. Broad policies could be applied to mailboxes to retain email for long enough to give a safety net in case the content needs to be used, discovered, or reviewed. For instance, all mailboxes could have a two-year policy to retain content. For senior roles, this could be five years.

When a retention policy is applied to a user's mailbox, all the user's content will be retained based on the criteria of the policy. In fact, if a user attempts to delete or modify an email, a copy of the email before the change is made will be preserved in a secure, hidden location in the user's mailbox. Retention policies can help organisation retains electronic communications, but those policies can be modified. Placing a Preservation Lock on a retention policy reduces the ability to change a policy. In fact, after a Preservation Lock is applied to a retention policy, the following actions are restricted.

- The retention period of the policy can only be increased, not shortened
- Users can be added to the policy, but no user can be removed

- The retention policy cannot be deleted by an administrator

Outlook rules. An alternate approach can be used in some cases where automated rules move or copy the content to a specific mailbox that has retention policies set accordingly. For instance, email subjects containing the word “contract” can be moved to a “contracts” mailbox.

Microsoft Teams

By default, Teams chat, channel, and files are retained forever. You can set up a Teams retention policy for chat and channel messages to decide proactively whether to retain the messages, delete the messages, or retain and then delete.

Remember that in Teams, files that users share in 1:1 or 1:N chats are stored in the OneDrive for Business account of the user who shared the file. Files that team members upload to a channel conversation are stored in the Team's SharePoint site. Therefore, to retain or delete files in Teams, create retention policies that apply to OneDrive for Business and SharePoint Online.

Private Channel messages. Please note that Retention policies do not yet support the retention of Private Channel messages. Since files shared in channels or chats are stored in SharePoint Online, retention of these shared files IS supported. We understand Microsoft is making changes to this in the near future.

OneDrive for Business

Users can save files they are working on in their OneDrive within the organisation’s tenancy. The files are conveniently available in File Explorer and on smart devices. Users can add, share, and delete the content as they wish.

OneDrive supports the out-of-box retention and disposal capabilities supported by the rest of the M365 suite. It allows admins to create a retention policy so that all the content stored in OneDrive is retained for the desired period of time and then disposed-off as per process. This policy holds content in the backend, even if the user deletes it from his end and the content is discoverable from the centralised e-discovery console for analysis or recovery.

The OneDrive retention policy can be based on the container (e.g., OneDrive of selected users) or based on content (e.g., documents with PII). It is important to note that OneDrive metadata is not centrally governed, and hence a centralised policy based on metadata cannot be applied to all OneDrive repositories. For such requirements, recommended tactics include:

- Users (or automated processes) copy the content to the managed library and folder of SharePoint Online.
- **Limit how much content** users can store to the minimum.
- **Monitor usage** (e.g., avoid a user having thousands of files they use and share with others – in effect forming a shadow ECM) and provide reports to line managers of users who are using OneDrive for Business as an alternative to the ECM document libraries
- **Monitor and report on deletion,** including providing reports to line managers, so they have visibility of what files are being deleted without being stored in ECM document libraries
- **Use e-Discovery** for audits and investigations
- **Auto apply metadata to files**. Advanced features can be used to set default metadata based on their role or department/section.

Stream

The New Stream stores content in SharePoint Online. This means Stream content can be managed with retention policies and labels, just like other SharePoint Online content.

Exchange Online & OneDrive for Business process

The process below is based on the logic in the preceding sections. Information managers can apply this process to each site or mailbox. This includes Teams content that is natively held in Exchange Online. While there are usually thousands of sites and mailboxes in an agency's deployment, the information manager is only actively involved in the greyed first stage. The remaining actions & processes are automated by Microsoft 365.

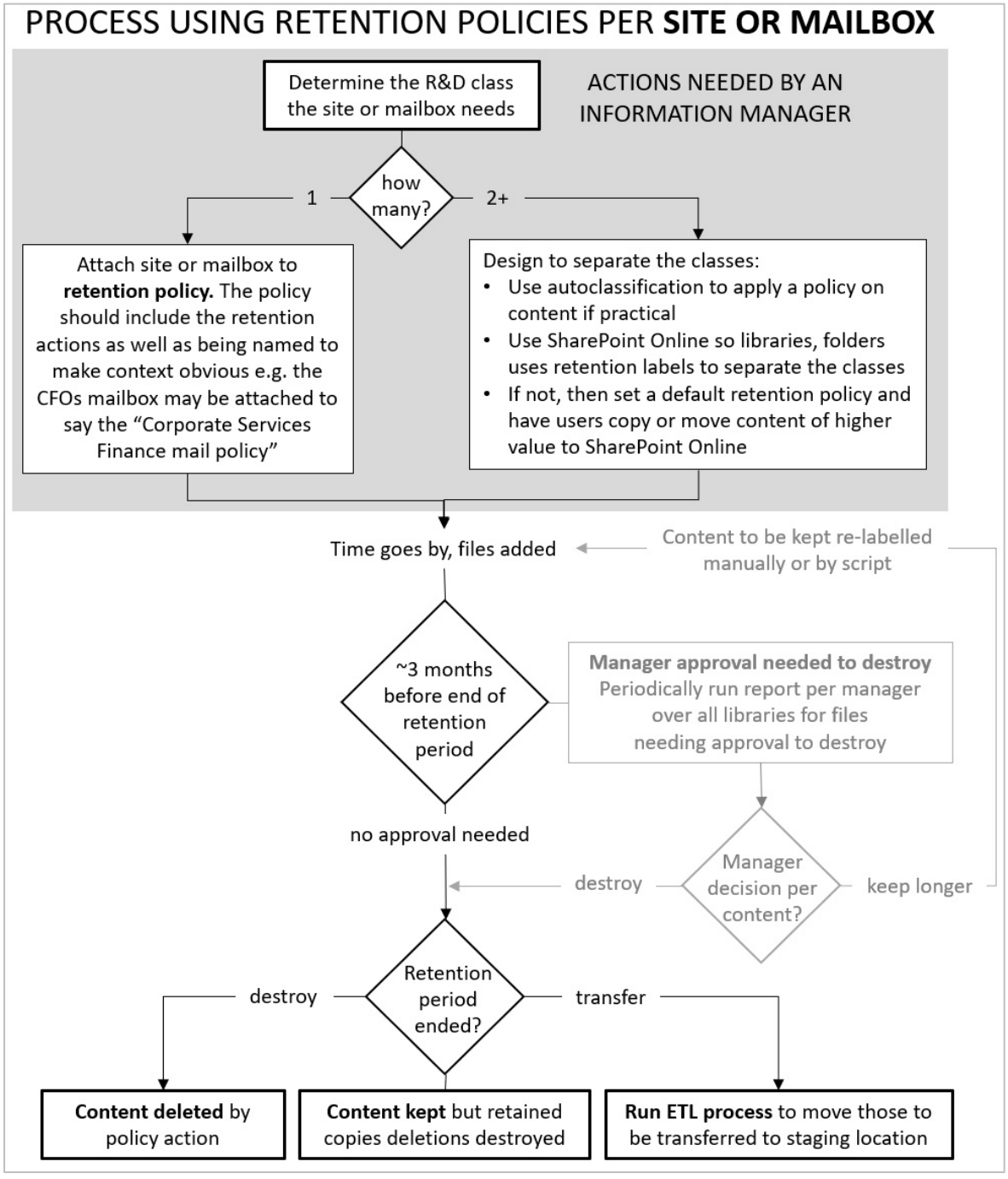


Figure 12 - Process for using retention policies per site or mailbox

Section 3: Features and Licensing summary

The paper includes references to Microsoft 365 features that can be used to support PRA compliance. Most functionality is available with Microsoft 365 E3 licenses. This specifically includes:

Manually apply retention labels	Allows users to override defaults and apply a retention label to a particular file. This is useful for exceptions but by itself not a scalable way of doing retention and disposal.
Apply a retention policy to a site	Allows administrators to apply a retention policy to a whole site (so all lists, libraries, and their folders are subject to it unless overridden). This also applies to mailboxes and each OneDrive for Business site. Useful in some situations if all content in the site has the same retention and disposal rules.

3.1 Advanced features

The table below outlines the advanced features that are discussed in this white paper:

Advanced feature	**Key use**
Default labels for libraries and folders	The key tactic for applying retention rules on document libraries where one or more rules apply to the library
Users can apply a "record" label	This locks the file down from further change, and the record label can be used alongside retention policies and labels to inform retention and disposal actions
Retention Policies via machine learning	Ability to infer what retention policy should be applied by rules or auto-classification across all Apps
Retention Policies based on events	Ability to start a retention period based upon an event (e.g., a lease has expired, an asset has been sold)
Manager review before disposal	Ability to allow manager review and approval of content that is being managed through retention policies or labels
Investigations	Advanced Audit provides the ability to conduct forensic and compliance investigations.

Licensing for the above features can be done through various licensing options as per the below table. It is important to consider the right licensing option depending on other capabilities that may be required by the organisation outside of their compliance needs.

For detailed guidance on Microsoft 365 Compliance licensing, refer to Microsoft 365 licensing guidance for security & compliance links or contact your Microsoft Licensing provider or your Microsoft Account Team as the below information is subject to change.

- Microsoft 365 E5 Information Protection and Governance (This is a stand-alone SKU and can be added on top pf M365 E3)
- Microsoft 365 E5 eDiscovery and Audit (This is a stand-alone SKU and can be added on top of M365 E3)
- Microsoft 365 E5 Compliance (This is an Add-On SKU to M365 E3 and includes the M365 E5 Information Protection and Governance and eDiscovery and Audit SKU's)
- Microsoft 365 E5 (The M365 E5 Suite includes the M365 E5 Compliance SKU)

Advanced Feature	**Licensing Options**			
	M365 E5 Information Protection and Governance	Microsoft 365 E5 eDiscovery and Audit	Microsoft 365 E5 Compliance	Microsoft 365 E5
Default labels for libraries and folders	Y	N	Y	Y
Users can apply a "record" label	Y	N	Y	Y
Retention Policies via machine learning	Y	N	Y	Y
Retention Policies based on events	Y	N	Y	Y
Manager review before disposal	Y	N	Y	Y
Investigations	N	Y	Y	Y

Table 6 - Advanced Features Licensing Options