

Microsoft 365 Compliance

This advice is a discussion document on Microsoft 365 (M365) Compliance. The intention of this document is to provide context for anyone considering the suitability of M365 Compliance for ACT Government recordkeeping. The primary focus of the Territory Records Office is the records management toolset of M365 Compliance, but the discussion is applicable to anyone wanting to manage and protect information within M365.

M365 Compliance is still an emerging technology in the information governance space. This product is not currently available or deployed within ACT government systems. At this point in time, our assessment is that M365 Compliance may be useful to automate the retention of records within a narrow set of specific business processes, but it is likely to be unwieldy when scaled to manage records in place across the whole of government.

What is M365 Compliance?

Microsoft 365 Compliance is a set of tools within the M365 environment that enable compliance with legal or regulatory standards at an organisational level. M365 Compliance is bundled as part of the Microsoft 365 E5 licensing tier, although components of the suite are available at lower licensing tiers. The tools provide information protection and governance capabilities with a focus on security, managing risk, compliance with international data and privacy standards, eDiscovery, and auditing.

Recently, Microsoft 365 Compliance has been advanced as a solution to records management issues within the Microsoft 365 suite of applications. M365 Compliance operates on most of the M365 products that contain an 'information store'. These include Outlook, Teams, SharePoint, and OneDrive.

Is M365 Compliance a fit for purpose Records Management option for ACTGOV?

Although records management is a promoted feature, available documentation indicates that records management functionality is a minor subset of the information governance features of M365 Compliance.

The primary use cases documented by Microsoft are in the realm of banking and financial services, and energy and utility services. There are additional compliance resources for government, which are framed around deploying Microsoft Teams at the various tiers of US Federal Government information system security accreditation.

M365 Compliance deployments for financial services and public utilities are broad brush approaches. Blanket retention policies are set across most of an organisation's communications and documents to meet minimum legislated retention requirements, triggers are set up to detect improper access to documents, and business units have their communication and documentation ringfenced to meet insider trading and other integrity regulations. Within a given Microsoft domain, sub-units (such as the agencies within the ACTGOV domain) may have different Compliance configurations. The more granular information governance an organisation requires, such as meeting the needs of individual business units within the larger organisation, the greater the ongoing effort required for configuration and administration of M365 Compliance.

The currently endorsed ACT Government electronic document and management systems (EDRMS—Objective ECM & Content Manager/TRIM) are highly structured storage environments. A 'record' is

essentially a standard set of metadata with an embedded electronic document or data file. When creating or managing records, metadata properties (such as audit logs) are embedded within the record. Records containing different file formats have consistent metadata. In this environment, records are managed using the administrator interface of the EDRMS.

M365 Compliance essentially manages records 'in place' within the source M365 applications. The available tools within those applications allow information governance policies to be created at high levels, which are then inherited by any document created under that level. Management at individual record level requires customisation using scripting languages.

Increasingly, records management solutions, including Content Manager and Objective, also offer manage in place functionality, with the key difference that the metadata to support the ongoing integrity of the records is managed centrally in the records management software. These systems also support capture of document contents into the central repository, if required, after it is no longer required in its native application environment.

Deploying M365 Compliance may require multiple approaches to records management within each application. As an example, MS Teams may be used for day to day communication within a small team, collaborative editing of documents, or coordinating a project across agencies. Each of these scenarios may have differing record retention requirements, and a resulting customisation of policies within M365 Compliance. Recordkeeping approaches and configurations needs will likely differ between directorates, and between business units within directorates. This is also likely to be the case in other manage in place systems, however the centralised management of metadata and, optionally, content, is likely to be easier to manage on an enterprise level.

At the most fundamental level, record management within Microsoft 365 Compliance is designed around the US legislative model of recordkeeping, that requires a record to be 'declared', rather than all business information becoming a record on creation. Moving to a 'declaration' model would be inconsistent with Australian practice and ACT records and information legislation. It is also unlikely to remove the recordkeeping compliance burden for end users.

How does Microsoft 365 Compliance record management work?

The basic mechanism to manage records within M365 is the retention label. M365 Compliance allows individual documents to be tagged with 'retention labels'. A Record retention is simply a metadata label for a document, email or other file object within M365. The label places restrictions on an end user's actions according to a table of policies. Rather than being a property integral to the metadata of a labelled document, details of the retention label appear to be stored centrally within a given product.

Microsoft 365 Compliance provides a basic set of retention labels that are intended to enable recordkeeping activities. There are four tiers of 'baked in' record labels that progressively restrict actions on a particular document/record. The first of these tiers is a basic 'tag' with a retention period that can be applied by any user. To apply stronger protections, such as restrictions on deletion or editing, administrator privileges are required. Out of the box, records retention labels have three default actions: metadata tag only, delete automatically according to a trigger, or begin a disposal approval process on trigger. To apply more sophisticated protections, such as a workflow approval for the deletion of records at the end of their retention period, script based customisation is required.

There is a special Microsoft Active directory administrator class called Records Manager that has been introduced, that gives an end user appropriate administrative privileges within the M365 Compliance tools, rather than requiring full system administrator privileges. A M365 Records Manager may have privileges specific to an organisational subdomain, rather than having oversight over the records of an

entire organisation. Only a Records Manager can apply retention policies with stronger protections such as restrictions on editing or deletion.

Administrators can set up automatic application of policies based on any number of criteria. Each automatic classification process requires configuration. Examples of classification processes would be to apply a label when a document is dragged into a folder/container, or all content for a particular Teams channel could inherit a label.

It is possible to automate record label classification based on metadata and content keywords. AI or search engine-like agents can potentially be 'trained' with specific content and metadata terms.

Are there records management gaps in M365 Compliance?

The ACT, along with other states, territories and the National Archives of Australia, has adopted the [principles and functional requirements](#) of EDRMS systems as defined by the International Council of Archives. The following highlights some key differences between M365 Compliance and our endorsed EDRMS systems along with associated principals.

How does M365 Compliance handle Metadata?

Principles:

- Business information has to be linked to its business context through the use of metadata.
- Systems for capturing and managing business information have to rely on standardised metadata as an active, dynamic and integral part of the recordkeeping process.

A retention label is simply a metadata label for a document, email or other file object within M365. The label places restrictions on an end user's actions according to a table of policies. Rather than being a property integral to the metadata of a labelled document, details of the retention label appear to be stored centrally within a given product. This is similar to SharePoint, where documents within SharePoint can be given labels and other metadata properties that are stored within SharePoint rather than being an intrinsic part of a document or data file.

If something is exported or deleted – what metadata is left behind?

Principles:

- Business information has to be able to be disposed of in a managed, systematic and auditable way.
- Systems should have the capacity for bulk import and export using open formats.

Record labels and associated metadata are not exported by default from M365 Compliance when documents or records are transferred to another repository. There is potential to script the export of metadata for a particular batch of records, but this will likely require customisation for each export process.

The file names of records deleted through a M365 Compliance approval process are recorded in a central database, along with details of the approval. This database can be exported to Excel/CSV. Without an export process, log files containing records of deletions are only retained for a limited time.

Are actions using MS tools auditable?

Principles:

- Electronic business information has to be actively managed and reliably maintained as authentic evidence of business activity.

- Systems must maintain business information in a secure environment.

Auditing is a separate feature of M365 Compliance. An audit trail of particular actions on documents or records can be captured. Basic audit capability is 90 days retention on a standardised list of actions, or advanced auditing and retention of audit trails for up to 10 years can be custom configured on specific criteria. If audit trails are not configured, no specific audit information is kept other than general operating system logs. This is a significant departure from the audit capabilities of Content Manager and Objective, where every record has a permanent embedded log of access and actions.

References & Resources:

Compliance overview:

[Microsoft 365 E5 Compliance | Microsoft Security](#)

Purview Compliance Documentation:

[Microsoft 365 Purview compliance documentation | Microsoft Docs](#)

Records Management Documentation

[Records Management in Microsoft 365 - Microsoft 365 Purview | Microsoft Docs](#)

Information governance training modules:

[SC-400 part 3: Implement Information Governance in Microsoft 365 - Learn | Microsoft Docs](#)

Data protection resources:

[Data Protection \(microsoft.com\)](#)

Security and compliance for financial services:

[Key compliance and security considerations for US banking and capital markets | Microsoft Docs](#)

Security and compliance for energy and utility services:

[Key Compliance and Security Considerations for the Energy Industry | Microsoft Docs](#)

ICA Principles and Functional Requirements for Records in Electronic Office Environments

https://www.naa.gov.au/sites/default/files/2019-09/m1-ica-overview-principle-and-functional-requirements_tcm16-95418.pdf