Western Australian Government

Records Management Advice

Microsoft 365 Compliance Centre for Records Management

For further information contact:
State Records Office of Western Australia
25 Francis St
Perth Cultural Centre
Perth WA 6000
+61 8 9427 3636

sro@sro.wa.gov.au

Document Version

This is a controlled document: Revision 1.1 (17 February 2022).

USING MICROSOFT 365 COMPLIANCE CENTRE FOR ROBUST INFORMATION AND RECORDS MANAGEMENT

PURPOSE

The purpose of this document is to provide high-level advice to information managers and relevant executives within Western Australian government agencies about the suitability of Microsoft 365 Compliance Centre[1] capability, and more specifically the Records Management module for managing records of information. This is intended to assist agencies in their consideration of using this technology in meeting regulatory obligations for the management of records of information.

> With effective project and information governance, as well as detailed planning for implementation, Microsoft 365 Compliance Centre capabilities can, with appropriate configuration, provide a digital records management environment to support Western Australian regulatory requirements.[2]

Note: This document contains high-level advice, however nothing herein constitutes a recommendation, or direction (implied or express), by the State Records Office of Western Australia (SROWA) for Government Organizations (as defined under the State Records Act 2000) to adopt Microsoft 365 Compliance Centre for records management in preference to any other product: SROWA makes no representation on behalf of Microsoft or any other EDRMS vendor. This document is a response to the considerable interest in the product suite, and specifically in response to the common question as to whether it can meet records management compliance obligations in the jurisdiction of Western Australia.

KEY POINTS FOR SENIOR MANAGEMENT

- Microsoft 365 provides capability for managing digital information and 'in-place recordkeeping' in accordance with the State Records Act 2000.
- A thorough understanding of M365 features and limitations is required to ensure an effective implementation that supports regulatory requirements.
- Agencies should develop a business case to ensure comparison between existing EDRMS licensing and Microsoft licensing is on a 'like-for-like' basis.
- An effective information governance function is essential within the organization to ensure appropriate decision-making with reference to business and regulatory requirements as these inform system configuration and deployment decisions.

[1] The Compliance Centre portal is available at https://compliance.microsoft.com/

[2] Agencies will need to consider the ongoing requirements for effective and compliant management of legacy hard copy files (and mixed-format files) – including product licensing, data migration, ongoing collection management (discovery, information security, archival management), and retention and disposal. These considerations should be made during planning for adoption of M365 Compliance Centre as part of business case development.

INTRODUCTION

A significant challenge for modern information management, in the context of a digital information economy, is to balance the demands for: flexible and mobile working; interagency and portfolio collaboration; innovation; and responsiveness to stakeholder needs, with the perennial requirements for: appropriate accountability; transparency; legal compliance; and meaningful preservation.

Whilst this document specifically addresses the suitability of Microsoft 365 Compliance Centre capability (hereinafter referred to as "M365 Compliance"), the broader matters of project and information governance in respect of information management system implementation are applicable irrespective of the product selected.

MICROSOFT 365 AND COMPLIANCE CENTRE

Microsoft 365 is the evolution of Office 365 for enterprise users, combining the range of Office 365 cloud-based products with Windows desktop licensing, Enterprise Mobility and Security. Enterprises scaling from an E3 to a full E5 license gain additional capabilities in: meetings and voice; advanced analytics; identity and access management; threat protection; information protection; and, compliance management[3]. It seeks to provide for both compliance and flexibility in digital information management. The suite provides for centralised governance across the suite of cloud-based applications, collaborative workspaces, and processes.

There is potential for the suite to support consistency in the governance settings used across agencies. Supporting consistent information classification settings and role definitions would help agencies to share information securely, where appropriate.

Microsoft's desktop and server file stores, as well as its productivity and collaboration tools (both on premise and online) have not previously been appropriate for records management, because they lacked the capability to meet the requirements of the *State Records Act 2000* (**the Act**) and the legislated Standards. However, with the addition of M365 Compliance modules, organisations have an opportunity to balance regulatory and productivity goals, subject to a sound business case and effective implementation planning.

> Agencies should not assume that M365 Compliance is a 'magic bullet' that will solve the seeming competing priorities of regulatory and operational requirements for records management, or that it will relieve them of the need for a dedicated records management team: without significant effort in governance, planning, deployment and ongoing information management practice, agencies will find they have yet another information store that is poorly managed, generally increasing their overall compliance burden.

However, the suite of products does present an opportunity to bring together the productivity applications that information workers use every day and the long-sought goal of "in-place recordkeeping".

[3] Further details on licensing are available at https://www.microsoft.com/en-au/microsoft-365/compare-microsoft-365-enterprise-plans and an overview poster of the Microsoft 365 'ecosystem' is available here https://tinyurl.com/2hm8jkkh

Licensing

It is important to understand the licensing that will be required for your implementation of Records Management and other information governance module in Microsoft 365. You can get started with the quick licensing guide[4].

Microsoft's E3 license available to WA Public Sector departments and agencies who qualify under the State Government Enterprise Agreement[5] can provide a limited degree of information compliance capability (such as allowing users to manually apply a predefined retention label to content, or compliance managers to apply an information governance policy across all sites without adaptability). E3 licensing does not provide for auto-classification for information protection or retention, or for adaptive scoping of information governance and records management. With the full E5 license (which comprises both information security and compliance) the organisation is able to access the complete range of security, compliance, information governance and information protection tools. The full E5 license also provides for network protection (firewall), as well as threat detection and management – whilst these are beyond the scope of information management, they should be considered as part of the broad business case to ensure a robust solution comparison.

AGENCY CONSIDERATIONS, PROJECT MANAGEMENT AND GOVERNANCE

SROWA recommends that agencies wishing to explore the use of these compliance capabilities take a well-planned approach with appropriate consideration of:

- Program / project governance to provide alignment with business objectives:
    - Executive commitment and support for change
    - Identification of key corporate risks potentially mitigated through adoption of M365 Compliance including security risks
    - A detailed Business Case
- Information governance and design of information management and technology services, including:
    - IM/ICT support processes and compliance management
    - Information classification and role definitions
    - Preparation for organisational change
- Solution design and implementation, including:
    - Licensing requirements
    - Alignment with enterprise architecture
    - Migration considerations (which may be significant, depending on your organisation).

It is important to understand that M365 Compliance, whilst potentially suitable within the WA regulatory context, includes some central design elements that are built around the North American concept of "regulatory records". In Western Australian, the Act provides for a much broader definition of a "record of information" and there is no need to "declare a record" for preservation purposes.

[4] Further details on licensing are available at https://www.microsoft.com/en-au/microsoft-365/compare-microsoft-365-enterprise-plans

[5] The WA State Government's Enterprise Agreement for Microsoft 365 licensing excludes Local Government, Government Trading Enterprises and the Education Sector (these sectors may have separate commercial arrangements with Microsoft and/or a directly negotiated arrangement with their local service provider).

Although there may appear to be clear and immediate financial advantages in adopting M365 Compliance for records management (in view of working under the State's Enterprise Agreement with Microsoft), agencies should address the entire procurement lifecycle by means of a business case, which should consider their agency specific needs including significant matters of managing legacy information and / or systems, as well as data migration and change to business processes.[6]

Subject to resource constraints and the complexity of their operations, agencies should consider undertaking a limited trial using a standalone Microsoft Tenant[7] for that purpose. This will assist the agency's information management practitioners gain hands-on familiarity with the products and their complexities.

Agencies deciding to adopt M365 Compliance should approach the proposed change with the same level of rigour that would be expected of any other technology implementation. This would include (without limitation):

1. Development of a Project Initiation Document (or similar) and a Project Plan / Business Case. This will help drive necessary decisions and provide support from senior management – this should also include, at the appropriate time, a change management and communications plan for onboarding users.
2. Development of either a set of technical and functional requirements or adopting an agile methodology by developing user stories and planning for 'sprints'. In either case, the end goal should be clearly defined (MVP or 'minimal viable product')[8].
3. The close involvement of a senior Information Manager (for example, the CIO or equivalent) and a "business owner" to act as "Supplier" and "Project Sponsor", respectively – the project should not be driven from an Information Technology perspective (or Cyber Security), but will need a good level of IT support – there are policy decisions about the value, risk and protection of business information and the way in which the MVP solution can support that.
4. An understanding of specific risks or digital transformation goals for your business in moving to this platform (not general project management risks alone).

INFORMATION GOVERNANCE AND INFORMATION MANAGEMENT SERVICES

A business-driven view

It is important to consider the functions of the organisation and the levels at which various functions will be represented in a 'boundary map'. For instance, Finance as a function may operate as a single site, with various libraries as sub-functions ('channels' in MS Teams), or there could be sites for sub-functions with libraries for specific activities. This has implications for information security and sharing across the organisation, as well as for the application of information classification and retention labels.

[6] When using Microsoft E5 licensing, be mindful this includes windows licensing, full security and compliance portfolio for the purposes of comparison with existing EDRMS.

[7] Conceptually, a "Tenant" on Microsoft is the organisation's subscription and its technology resources contained within secure network boundaries.

[8] Agencies may wish to refer to Functional Requirements for M365 (produced by the Australian Digital Recordkeeping Initiative - an initiative of the Council of Australasian Archives and Records Authorities – 2021 and available here: https://www.caara.org.au/wp-content/uploads/2021/12/Functional-Requirements-for-M365-Version-1.0.pdf).

Further, the organisation should have (or develop) a set of business rules to guide decisions about site creation and management. M365 Compliance can provide for a high degree of granularity when it comes to defining roles and privileges, but this should be balanced against ease of support and user experience. The level of flexibility given to users in terms of managing information is traded against compliance controls[9].

At a minimum, SROWA recommends control over the initial creation of Teams (M365 Groups) and SharePoint Sites. Agencies should develop a streamlined, controlled process to ensure these sites are aligned to the desired information architecture and site boundary mapping. This will allow for the more efficient and effective deployment of records management compliance controls.[10]

An Alternative Model – A Records Management View

An organisation may consider an implementation model that is more aligned with a structured and controlled Business Classification Scheme (BCS), in which a records management view of document management is implemented and controlled within SharePoint, by implementing sites for functions and libraries for activities within that function.

In this approach, users adopt a way-of-working that places MS Teams at the centre of their workflow and 'exposes' those SharePoint libraries as required, within the Team site according to its functional requirements.

The challenge of this approach is to limit the users' view of BCS components that are relevant to them and to prevent users from 'corrupting' the BCS by creating functional or activity folders in incorrect locations. Further, each time a MS Team site is created, a SharePoint site is automatically created: that site would be outside of the boundary of the BCS and potentially becomes a repository for ungoverned information.

M365 Compliance provides for a number of capabilities in the information governance space, such as Information Protection (sensitivity labeling used for information classification), Data Loss Protection, eDiscovery and Insider Risk Management. The business case for deploying Records Management in Microsoft 365 represents a good opportunity for the organisation to consider these other modules since there are ways in which the modules can work together to deliver value.

The agency should consider its external stakeholders (and the public too, where relevant) when considering its overall Microsoft tenant security posture, as well as its site boundary mapping. For instance, how will OneDrive for Business be used in terms of information sharing and collaboration with other agencies or the public? Can the agency define roles and assign information classification labels consistently to facilitate safe and secure information sharing across the agency and with other agencies? There are also key security settings at the tenant level which may impact the agency's business.

---

[9] Consider, too, the value of consistent definition of roles and clear definition of controls available particularly to custodians or stewards of OFFICIAL Sensitive information (see Section 6 of Information Classification Supplementary Guide produced by the Office of Digital Government https://www.wa.gov.au/government/document-collections/western-australian-information-classification-policy).

[10] Note, that restricting group creation will have other flow on effects across your organisational instance of M365: see *Manage Who Can Create Microsoft 365 Groups:* https://tinyurl.com/2p88a59a

A Note About Microsoft Tenants

From the perspective of the collection of Microsoft services available in the cloud subscription, a "tenant" represents an entire organisation. A tenant is a dedicated instance of Azure Active Directory that an organisation or app developer receives at the beginning of a relationship with Microsoft. That relationship could start with signing up for Azure or Microsoft 365[11].

Generally, there will be a one-to-one relationship between your organisation and your tenancy: that is, you will have a single tenant for your entire organisation, with a single Global Administration and a single Compliance Manager role. However, some organisations, whilst holding a single tenancy with Microsoft, will house multiple business units or agencies which host a separate domain. These units may operate somewhat independently of the "parent" organisation and have different business rules and compliance requirements for various reasons, or have different use cases when it comes to external information sharing and collaboration.

It is important to remember that the global administration and compliance settings in M365 Compliance affect the whole tenant, but it is possible to limit the effect of specific governance tools to particular sites, applications, and even users. For example, you may want to establish specific governance tools for OFFICIAL Sensitive Cabinet information and limit access to this information and set specific retention. This will require some forethought and planning.

In implementation planning, the agency should consider users, groups (roles) and permissions – and the broad policy settings for these:

- Which role/s can manage the file plan, information classification and retention policies?
- Who manages the use of those in various Applications (including exceptions)?
- At which level can users (or a specific subset of users) override default settings?
- Defaults for sharing both internal to the organisation and external.
- Any specific controls required to support your agency's data sharing MoUs.
- Managing controls to support audit and reporting processes.

The records management function will not run itself simply because the agency has moved to M365 Compliance and in-place recordkeeping, although it may be subject to transformative change. The agency must make clear plans for the ongoing records management function to ensure appropriate, ongoing compliance activities and reporting.

RETENTION

M365 Compliance provides three key retention features:

Retention labels can be applied at a global level (such as apps, sites and users) but also at the level of individual items (such as a folder or document). Labels are created and configured in the Compliance Centre Information Governance Module and the Records Management Module. Note: a label in the Information Governance Module does not include disposition actions (these only apply to labels within the Records Management Module).

Retention label policies are used to publish retention labels in groups and apply them to specified locations. Label policies in the Information Governance Module and the Records Management

[11] See https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-create-new-tenant

Module are required so that labels are available to users and application administrators (such as a SharePoint site owner).

Retention policies are specific to the M365 Compliance information governance module and can be applied to locations globally (such as MS Teams chats). These policies are not able to discriminate between content within the location and a policy can apply to a single location or multiple locations. A single policy cannot apply to all locations at once and there are limits to what locations can be included together under a policy.

With or without an E5 license, it is easiest to map retention policies and periods to locations, such as Teams or OneDrive, and determine the appropriate retention with a risk-based assessment of the records held there.

It is recommended that the **application of retention labels** be configured at the container level. This would mean, for example, that a SharePoint library created for a specific Team (function or project) would have a retention rule applied at the top level and everything in the container would inherit the same retention settings, except if a user (or the information governance team) overrides the default.

The information governance team (or a sufficiently privileged user with an E5 license) can also configure the automatic application of retention labels to content that includes or matches:

- nominated sensitive information types
- specific keywords that match a query
- trainable classifiers.

Sensitive information types may be present in a variety of disposal authorisations, so using sensitive information types to attach retention labels to an entire collection is unlikely to be convenient or easily achieved.

M365 Compliance is somewhat skewed to the United States' regulatory conditions. Therefore, it supports a central concept of "regulatory records" which involves explicit declaration of records. When configuring a retention label in M365 Compliance Centre, a feature in the retention actions settings provides for Compliance Managers to indicate "Mark as Record" as an option. Where the label is applied, the content will be declared as a record for permanent retention at the specified time. Using this feature severely limits actions on that content and on the label itself. It is suggested therefore that this feature be used cautiously, or avoided, and do not test its use on production-level content.

FILE PLANS

M365 has the option to upload a File plan to bulk-create retention labels.

Rather than using this feature to upload entire retention and disposal schedules, SROWA recommends that you analyse your retention and disposal schedule(s) and activities in order to roll up the available disposal authorisations to a limited list that can be used as labels. Labels can be applied to site, library and folder levels allowing documents within those locations to inherit the label. Each label could indicate its retention action and minimum retention period in its name and then be applied to content as necessary. The top-level set of retention and disposal terms contained in the existing disposal authority can be created as a "Term Store" in M365 and terms can be applied as tags for disposition reviewers.

It is also possible to limit the number of labels required (and visible to users) by setting up the disposal process to allow the disposal review officer role to apply a further period of retention at the time of review. In this way, fewer broad-based retention periods can be set with the option to then apply a further period of retention.

DISPOSAL

One of the issues with M365 Compliance disposal functionalities is that disposition review or obtaining proof of disposal can be more difficult without declaration of the relevant documents as records, and which also requires an E5 license.

As stated above, declaration of a document as a record is a US records management concept. In Western Australia, the Act regards all documents (as well as data and other recorded information) as records from the moment they are created or received by a public authority – no explicit declaration is necessary.

It is recommended therefore that the ability to declare documents as records ("Mark as Record", as discussed above) be avoided as this prevents any further editing and may cause confusion about what is a state record.

Documenting Disposal

Where retention labels or policies are in use, and the deletion of items is permitted for those policies, items when deleted by users are placed in a Preservation Hold Library (each site has its own Preservation Hold Library). This area is not visible to ordinary users. As such, deleted records could be reviewed by disposal review officers while in the preservation hold library and items are available for the eDiscovery tool (part of M365 Compliance suite). To ensure appropriate destruction of records, where deletion of content is permitted in particular locations, regular reviews of content in those locations should be conducted, in accordance with information management policies and appropriate risk evaluation.

The frequency of these reviews would need to be determined through a risk-assessment and will be impacted by any other processes in place to catch important records prior to disposal, such as education and training of staff.

It is important to note that deleted content not held in a Preservation Hold Library is moved to either the first or second stage recycle bin and is not indexed. Therefore, it will not be found using M365 Compliance content search feature for eDiscovery. As such, extra care should be taken to ensure no disposal occurs for any records that are required for current or pending legal action.

Audit logs, once enabled, capture actions performed on content including deletion. To meet disposal documentation requirements, audit logs could be used as evidence of how the records were destroyed, the description of the records and their date range. (The organisation's disposal authorisation and relevant approval documentation would need to be created separately and linked.). Audit logs are only stored in M365 for a maximum of 10 years, depending on the license. As such, audit logs will need to be extracted and stored appropriately.[12]

[12] As with any system that comprehensively audits events, implementers should understand constraints, limitations and risks in order to develop appropriate solutions that support business and regulatory requirements.

It should be noted that in M365 there is no single, central recycle bin, meaning reporting for audit purposes on deleted items would involve individually inspecting and exporting the details of each site's recycle bin's contents on a regular basis.

RELATED DOCUMENTS

Agencies could also benefit by referring to:

- *Modern Records and Information Management with Microsoft 365* (produced by Engaged[2], 2021 and made available by the State Records Office of Western Australia)
- *Functional Requirements for M365* (produced by the Australian Digital Recordkeeping Initiative - an initiative of the Council of Australasian Archives and Records Authorities - 2021[13]); and
- *Manage your records and Microsoft 365* (produced by the Queensland State Government, 2021[14]).

[13] https://www.caara.org.au/wp-content/uploads/2021/12/Functional-Requirements-for-M365-Version-1.0.pdf
[14] https://tinyurl.com/mr3rjs3t

ANNEX A: LIMITATIONS OF PREVIOUS APPROACHES

HISTORICAL CONTEXT RMS / EDRMS

Historically, hardcopy records management processes were relatively linear and controlled, with file creation and artefact storage and management centralised at an organisational level: from time to time, records required to be retained permanently were transferred to archives. Early Records Management Systems (RMS) were catalogues that captured information about physical objects (file metadata), managed business classification, retention schedules, and recorded file location and movements, supporting the managed disposition of physical files.

Electronic Document and Records Management Systems (EDRMS) evolved and attempted to bridge the gap between the hard copy and the digital worlds by providing, initially, an electronic analogue of the physical file store with storage for electronic objects included and then, in later developments, a digital workspace for document creation, development and collaboration as a superior alternative to a file server ('shared drive'). These attempts have met with varying degrees of success, often depending on an organisation's preference for compliance or for flexibility.

The tremendous growth in personal computing and electronic information systems, coupled with decentralised client-server computing models, has challenged the centralisation of the information management and governance functions, and has seen rapid growth in the production of electronic documentation.

Further, the proliferation of email alone has presented a substantial challenge, leading to vast amounts of duplicate and non-corporate or low value data kept alongside valuable information in uncatalogued electronic databases.

Government recognises the high value of its data assets and the potential for better policy and service delivery developed through sharing data across agencies. The emergency response to the COVID-19 pandemic has heightened government's appreciation of the potential value of data and data sharing. The first step to realizing this potential is for government data assets to be known and discoverable.

LIMITATIONS

Modern EDRMS solutions remain an effective and robust means to manage enterprise information in a compliant manner that reduces risks to organisations, provided they are implemented with appropriate governance. Some of the key limitations of previous approaches have included:

- **Complex and arcane EDRMS user interfaces**: these are usually separate applications that are apart from the ordinary workspaces and the 'ways of working' of general information workers (they include simple 'local and network file shares', email clients, or collaborative browser-based sites in more recent times).
- **Separate digital locations or stores for particular electronic documents**: in these approaches, 'complete' or 'final versions' are kept separate from the ordinary workspace in a compliant system, requiring users to move content from one location to another and often requiring them to fill out metadata for the purposes of classification and retention rules. This represents an additional task for busy users, and many are disinclined to perform it or are not adequately knowledgeable in information classification. This is a limitation relative to a

goal of ‘in place recordkeeping” – from another perspective, securing important, high-value records in separate locations is a sound business decision.

- **Inadequate training within organisations and inadequate controls**: for operational reasons organisations have been unwilling to strictly limit the use of file servers or other non-compliant locations.

The most significant consequence of these system and management limitations has been an ineffective or incomplete take-up and use of enterprise EDRMS, potentially resulting in:

The creation of masses of uncontrolled information whose provenance, classification, retention settings and archival status is uncertain, compelling organisations to retain digital information indefinitely and bear the risks and costs of doing so.

This is an ongoing risk for agencies, including those considering the adoption of M365 for records management.

ANNEX B: CONSIDERATIONS FOR SOLUTION DESIGN AND IMPLEMENTATION

Following are some high-level design and implementation considerations for adopting M365 Compliance for records management. SROWA intends to develop further implementation planning and guidance advice aligned to the Western Australian context.

Using a Non-Production Environment

It is possible that experimenting with some settings may result in irreversible consequences for content and configuration (remembering, too, that Compliance Centre settings are global for the MS tenant) – so it is best to not use Compliance Centre in your production environment until there is a good level of knowledge in your information governance organisation, and a plan for how the capabilities will be deployed in production.

Therefore, consider setting up a non-production tenant for testing and learning, such as a "sandbox".[15] Limiting this environment to a maximum 25 user licenses, as well as limiting usage to the included storage, will mean there is no cost to your agency and. Restrict the number of licensed users to only those that will be placed into specified roles for the purposes of testing and learning.

The non-production environment should be setup in a Microsoft tenancy separate from the main production environment: for example, it could result in a domain such as [YourOrgSandbox].onmicrosoft.com. The tenant is not hosting your business domain and is totally separate from your production information. It will have its own Azure Active Directory in the cloud space that has no relationship to your production tenant users and directory (whether cloud or on-premise). All your test users will then format as [username]@[YourOrgSandbox].onmicrosoft.com. Users' access to Exchange Online, SharePoint, Office products and so on will be via these test accounts.

The use cases for testing in the sandbox environment could also be extended to include interaction of information governance, records management and information protection. Test users could include roles for information asset custodians or stewards (as described in Office of Digital Government's Information Classification Supplementary Guide) as these roles are responsible for the management and protection of information assets. The sandbox usage could explore a diversity of information types including OFFICIAL Sensitive information.

For the tenant administration in this environment, it is best practice to separate Global Administration (GA) privileges from other user accounts: for instance, your GA might also be in a Compliance Manager role, but the GA account might be indicated with a prefix, such as 'adm' – so your GA user might be adm.[username]@[yourorg].onmicrosoft.com, with the same user in a business role being [username]@[yourorg].onmicrosoft.com

Getting Started

At this point, with a sandbox tenant established and non-production accounts for respective users in place, the design goals for the final product should be understood, along with the relevant control

[15] information and records managers can obtain test tenancies via the Microsoft developer program which provides a full e5 test tenancy with 25 licenses and test data for free – see https://developer.microsoft.com/en-us/microsoft-365/dev-program

processes to support those. It would be valuable to develop a specification or technical configuration document at this point.

If inhouse capability is not available, SROWA highly recommends that you either:

- engage a Microsoft partner organisation to assist in the configuration of the solution to meet your known business requirements. Ideally, the Microsoft partner would have knowledge of the local regulatory requirements for records management.

- if time permits, your inhouse IT and information governance teams could continue to develop their skills and knowledge in the sandbox environment, using Microsoft documentation and available training to build the necessary capability.

At a high-level, particular consideration to the following should be a core part of the organisation's planning:

- Definition of roles and privileges:
    - Compliance Manager and Global Administrator
    - User roles and privileges related to compliance
    - Compliance Manager Readers and other custom roles.
- Plan for execution of retention and disposition actions based on policies and privileges.
- Plan for establishing reporting, including for data protection and cyber security.
- Consider physical files and legacy processes and how these will either map to the new situation or will be supported in future.
- Business processes for creation of sites and their classification (application of functional disposal authority) .
- Data connectors for harvesting social media content – special privileges required .
- Define a minimum number of retention labels required to support approved disposal authorities.
- Consider the prefixing and privileging of retention labels in large and/or complex organisations to simplify the user experience.
- Consider iterative disposition processes – and resourcing for reviews.