

Modern Records and Information Management with Microsoft 365



Written by:

- Matthew Dodd | Digital Workplace Consultant
- Andrew Jolly | Information Management Practice Lead

With thanks to the following for their advice and contributions:

- Damian Shepherd | Director State Records, and all the team at State Records Office of WA
- The Department of Local Government, Sport and Cultural Industries Western Australia Records Management Working Group
- The Government and Modern Workplace team from Microsoft Perth

Table of Contents

1	Executive Summary	3
2	The challenge and opportunity	4
2.1	Practical problems.....	5
3	A risk-based approach to information governance.....	6
3.1	Back to basics.....	6
3.2	Managing the risk.....	7
3.3	The three lines of defence.....	7
4	Using M365 as the basis for a records and information management system.....	9
4.1	M365 as the Platform.....	9
4.1.1	Reducing risk.....	9
4.1.2	Sensitivity labelling	10
4.1.3	Classification boundaries.....	11
4.1.4	Licencing.....	13
4.2	People considerations.....	14
4.2.1	Roles	14
4.2.2	Change management.....	15
4.3	Processes.....	15
4.3.1	Self service.....	16
4.3.2	Record Management Operations (RM Ops).....	17
4.4	Policies	18
4.4.1	Classification schemes	18
4.4.2	Retention labels.....	19
5	Conclusion.....	22
5.1	Key Takeaways.....	22
6	About the Authors.....	23
6.1	Andrew Jolly.....	23
6.2	Matt Dodd.....	23

1 Executive Summary

Research at both a national and state level shows an alarming volume of digital records and information remains unclassified and unmanaged. The long-held promise of electronic document and records management remains unfulfilled.

With organisations increasingly adopting cloud-based productivity platforms such as Microsoft 365 there is an opportunity to rethink traditional approaches to information governance.

Modern records and information management can take a risk-based approach to leverage developments in cloud technology, automation, and artificial intelligence and blend these with pragmatic people focused processes and policies.

Microsoft 365 offers compliance and security functions that, when configured, can provide organisations with three lines of defence against unmanaged and unclassified records and information.

Records Managers can simplify governance tasks by specifying default metadata such as classification terms, sensitivity or retention labels or build searches that will auto-apply labels based on categories or content.

Administrators can set broad retention rules based on storage locations (such as SharePoint, OneDrive or Teams), or apply them to groups of people, creating a safety net to aid compliance with record keeping obligations.

Finally, exception reporting, monitoring and reviews allow Records Managers to support people with their information governance. Acting as supervisors they can bring their expertise to bear on the high value or high-risk areas of the organisation.

This paper explains how Microsoft 365 can be used for a modern records and information management approach and ways to make this successful in reducing the risk currently presented by unmanaged records and information. Key to delivering this vision are three recommendations:

- Using Microsoft 365 for modern records management requires a mindset shift from the traditional approach used in many DRM Systems.
- Aiming to simplify the records and information management system for users requires significant effort from records management practitioners and teams, but Microsoft 365 can lighten the load.
- The Microsoft 365 platform alone will not reduce the risk. You need to consider your information governance process, policies, and people for it to be effective.

2 The challenge and opportunity

Digital information is being created at incredible rates yet alarmingly the majority remains unmanaged and unclassified. This means despite previous investments in electronic document and records management systems, critical information and records are often being stored in a way that does not meet the needs of the organisation.

“We’re creating information in 2021 and still trying to manage it like it’s 1921.”

In the most recent [National Archives of Australia Check-up PLUS Whole of Government](#), agencies reported **63% of digital material they hold is un-sentenced and has unknown disposal classifications**. Only **12.4% of digital information records have been sentenced**, compared to 54.3% of physical records. Yet in the same survey **81% of agencies work as digital by default**. Research in 2015 by the State Records Office of Western Australia indicated that only a third of information systems in use by state government agencies had in-built record keeping capabilities - with data being manually exported to record keeping systems; and 40% of agencies reporting that network drives were being used to store most records.

It would seem that existing approaches to information management are often not making the most of digital technology and are unable to keep pace with the changing needs of people.

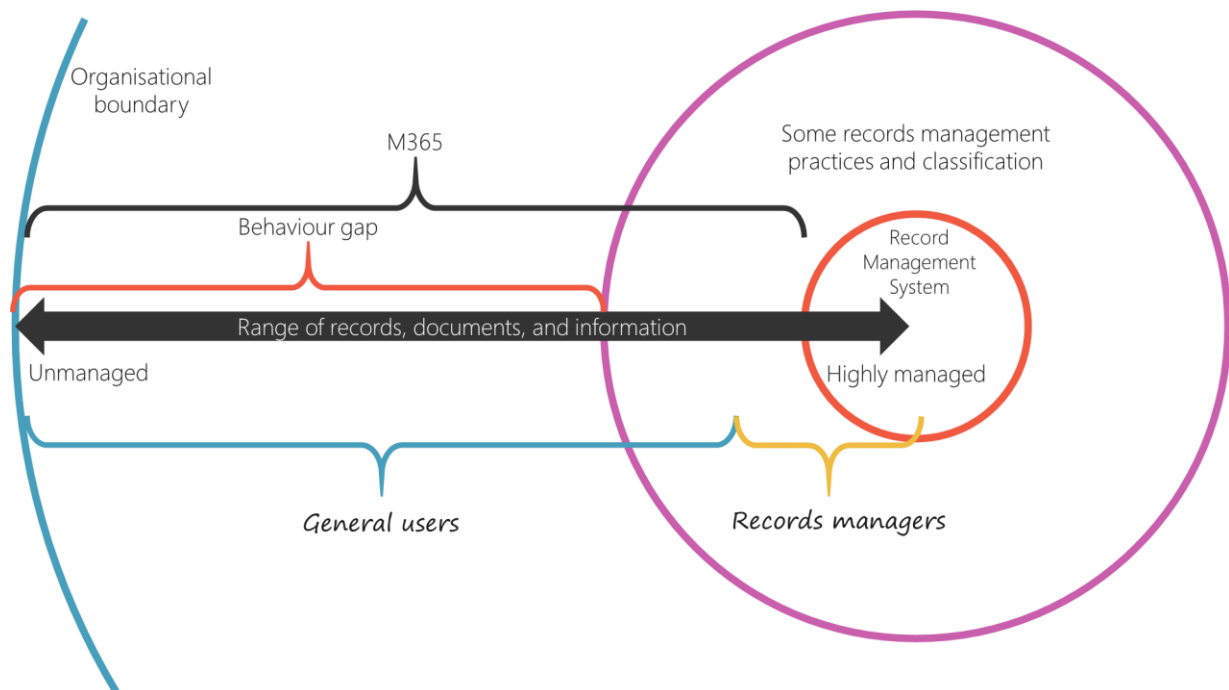


Figure 1 - The challenge of modern records management. The landscape for records management can be seen as a continuum from those records that are highly managed by Records Managers within a controlled records management system, through records that are appraised with the relevant sensitivity and retention labels, to those records that are “unmanaged”, and therefore remain unappraised and stored in a variety of settings from personal drives, file shares, and so on

2.1 Practical problems

When we've spoken with records managers, the list of issues they raise is consistent. In many cases there are multiple places to store information which means people are unsure where things go or how and when to add them. Lack of metadata creates problems in reporting and retention scheduling, coupled with items being duplicated or deleted inadvertently. Systems can make it difficult and time consuming for people to add relevant metadata, often requiring multiple steps and high levels of user knowledge to achieve this.

Any future solution should make it as simple as possible to fulfil your information management obligations, whilst making information open and accessible. Classification should be simple and easy for people to achieve, and records managers should be equipped with ways to report on the amount of information that remains unclassified or needs exceptions to policies applying.





3 A risk-based approach to information governance

Using Microsoft 365 to support information governance will not close the gap unless you approach records management differently.

Working with the State Records Office of Western Australia we have approached the challenge by developing a risk-based approach to records and information management. This shift of paradigm aims to simplify information management tasks in the place that people work every day – Microsoft 365. It acknowledges that a focus on compliance without due regard to the practical needs of people creates the risk that much of the information being created is, at best, poorly classified, and, at worse, not classified or managed at all.

3.1 Back to basics

At a fundamental level we see the objective of any records and information management system is to:

	Protect the records and information from unwanted access or unwanted restrictions.
	Preserve the records and information for future use as needed with the context needed to use the information appropriately.
	Profit from the knowledge contained within the records and information so they can support future business objectives and decisions.
	Purge (or destroy) information that is no longer needed reducing the risk of the information being used inappropriately.

With the objectives in-place we can build a system for modern records and information management comprising of the following areas:

- **Platform** – the systems and technology that supports the creation, maintenance, storage, and discovery of records. This could be as simple as a filing cabinet and dividers for physical records, through to multiple software systems and servers for digital information.
- **Processes** – the approaches and flow of information within the overall system. This is the way the information items end up or are accessed within the platform.
- **Policies** – the guidance and rules that govern the records and information. This includes any legislation, classification & sensitivity schemes, and retention schedules.
- **People** – the behaviours, knowledge, and capabilities of those creating, maintaining, storing, and searching for records and information. Without actions and decisions by people the overall system will fail.

Modern records and information management requires a renewed emphasis and revitalisation of the role of information risk assessment in developing records management policy, processes, platforms, and their application by people.

3.2 Managing the risk

The risk assessment comprises of considering the likelihood and impact of an event. In relation to information or records these events can be characterised in the familiar information security triad:

- People see information they should not (**confidentiality**).
- People change information they should not (**integrity**).
- People cannot discover or access information when they need it (**availability**).

The likelihood or impact of these risks happening can be mitigated by controls. In the case of information and records this can be done by

- **Sensitivity labelling** to indicate the impact of releasing the information and thereby maintaining confidentiality.
- **Permission levels** that limit the actions someone can take on a piece of information thereby maintaining integrity.
- **Retention labelling and categorization**, so information is kept for an appropriate period and is searchable thereby making it available.

Clearly, if large amounts of information remain unmanaged the risk of an event occurring that impacts the confidentiality, integrity or availability of an item is difficult to detect. Without management there is increasing risk of information inadvertently being destroyed, disclosed, or escaping the organisation. In other words

- We've been asked for it and we can't produce it - We deleted it too early.
- We've been asked for it, we've got it, but we're not supposed to have it anymore - We've held it longer than we've needed to or should have.
- A third party has it when they shouldn't - It's escaped the organisation.

3.3 The three lines of defence

Minimising the risk follows the concept of **three lines of defence**. This safeguards information by allowing users to classify information and retention, then using broad general retention policies, and finally flags exceptions to supervisors to review.

- **First line of defence:** User based classification, rules-based auto-apply or AI enhanced classification.
- **Second line of defence:** Broad retention policies to protect against deletion acting as a safety net.

Figure 2 - The three lines of defence model

- **Third line of defence:** Supervisory management by exception. Records Management staff conduct reviews of labelled material and period reviews of non-retention labelled content and assist in classification efforts either by
 - Encouraging business users to undertake remediation.
 - Remediation on behalf of the business groups
 - Audit and detection made possible by regular reporting using search and audit tools.

Once the information risk is considered and understood, it is possible to look at what tolerance there is to simplify the records and information management approach from a platform, process, policy, and people view.

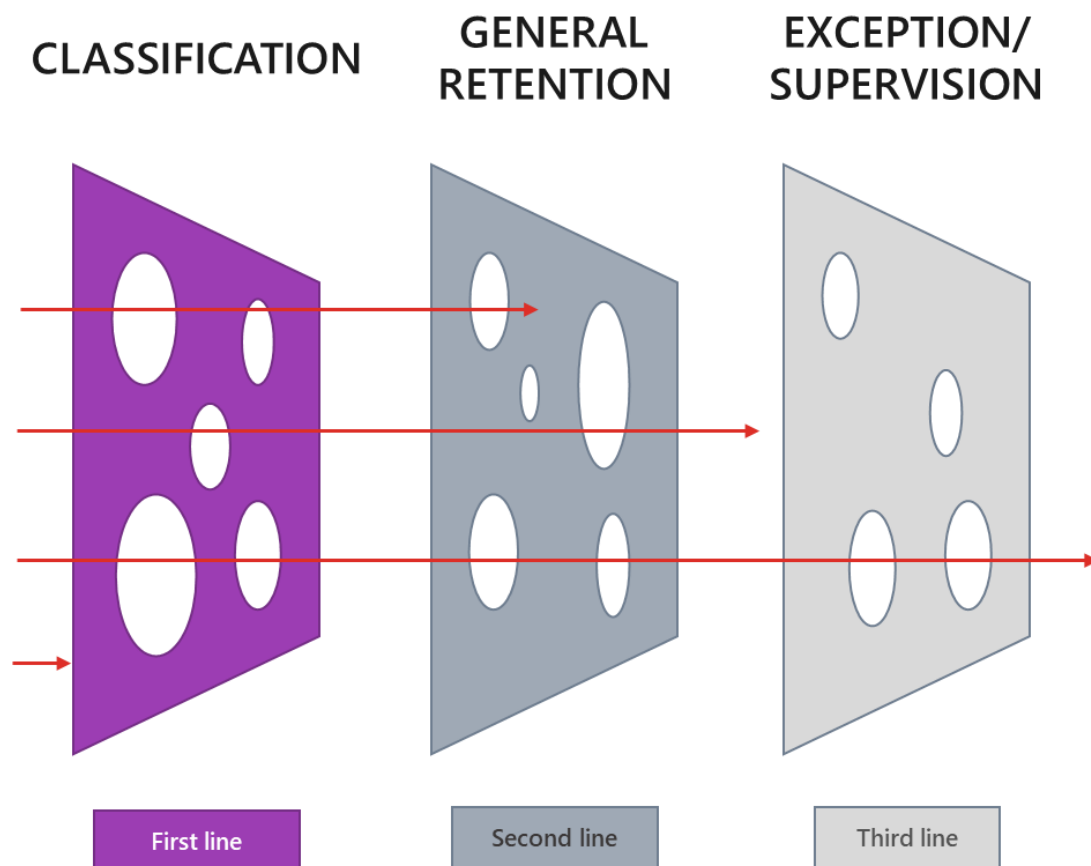


Figure 3 - Three lines of defence minimises risk.

4 Using M365 as the basis for a records and information management system

4.1 M365 as the Platform

4.1.1 Reducing risk

Many organisations and agencies use Microsoft 365 for the creation and development of information. They then ask users to move items to different systems for classification and storage. This introduces significant risk that items are deleted before they should be or kept after they should be disposed.

With the right licencing in place and using a combination of the M365 Compliance Center functions, along with search and SharePoint term store capabilities makes it possible to provide a flexible platform for records and information management

Using the three lines of defence as a concept, we use compliance and security features within M365 to support their implementation.

4.1.1.1 *First line of defence.*

M365 can be configured to allow users to select classification, retention periods and sensitivity labels (metadata) for items within the platform. There are different ways this can be applied:

- Metadata can be selected by users against individual items.
- Default metadata can be configured.
- Metadata can be automatically applied based on rules or through AI.

Within SharePoint online, classification schemes can be added to the Term Store. These can then be either chosen by users or applied as default to SharePoint libraries or folders.

Retention labels can be configured and published to SharePoint that allows either users to select an appropriate label, or for them to be applied as a default within libraries or folders.

To ease the burden on users having to decide on retention periods, it is possible to configure retention labels to be applied automatically. This is based on a chosen classification term or other document properties such as keywords. For example, a user may choose a term from a classification scheme that tags a document as 'financial'. Once a week M365 will automatically review items that have a classification term, and, where there is no retention label, will apply the associated retention label. Another example may be that based on keywords such as 'asbestos' a specific retention label that keeps the item for a significant amount of time.

The same approach can be taken for sensitivity labelling, with users being able to choose, or sensitive information (such as credit card numbers) being used to automatically apply the appropriate label.

Finally, it is possible with M365 to use machine learning to identify and classify certain types of items using trainable classifiers. This can be useful where items like purchase orders or invoices follow a pattern. Example items are loaded into M365 to teach a trainable classifier to detect

and add the necessary metadata to matching items. Using these tools reduces the reliance on users having to make choices on what classification or retention labels need to be used and therefore increases the volume of records and information that become actively managed.

4.1.1.2 *Second line of defence.*

The second line of defence acts as a safety net as M365 applies policies at the container level such as a whole SharePoint site, mailboxes, or even across the whole M365 tenant.

Retention periods can be applied from item creation or last modified dates for a wide variety of content from emails, Teams chats, Teams Channels, OneDrive, and SharePoint sites. These policies apply to the container, rather than individual folders or items. Items are placed in a preservation hold library when users delete items before the end of the defined retention period. This means the item is not available to general users but can be discovered by those with the correct records management access.

Specific users, groups and sites can have different retention policies applied. For example, this allows for those people with delegated authority to have messages held for a longer period than those who don't have budget spending authority.

4.1.1.3 *Third line of defence*

The third line of defence supports supervisors of the system to monitor and manage by exception.

Using the M365 content search and eDiscovery functions it becomes possible to report on those items that remain unclassified or search items that have been "deleted" before their retention period expires. The reporting functions also highlight items that have been classified and labelled.

The M365 records management component allows specific people to carry out the disposition reviews of items as retention periods expire. At this point items can be re-labelled with specific periods not available to normal users, or to be deleted. This means a record manager can take a view on whether content is significant or sensitive rather than relying on a decision by the content author made when the item is first created.

4.1.2 Sensitivity labelling

Classification and retention labelling mean records and information are managed and available for the right amount of time. M365 information protection adds the capability of sensitivity labelling.

A sensitivity label can be used to restrict what happens to an item such as being shared, copied, downloaded, or printed. They can also be used to apply watermarks and statements on Office documents to help highlight the business impact of an item being shared. This all helps control access and integrity – key components for information security.

A uniform set of sensitivity labels, such as 'Unofficial', 'Official', 'Official: Sensitive', can be configured within M365. As with other labelling, sensitivity labels can be applied in different ways:

- Selected by users.
- Applied automatically based on finding defined sensitive information types within items (such as tax file numbers, passport numbers and so on).
- Applied by a default setting.

For more detailed information on sensitivity labelling, see the [sensitivity labelling overview on the Microsoft website](#).

4.1.3 Classification boundaries

Configuring the platform depends on the structure and function of an organisation, and the adopted processes and policies they want to implement. To help determine any M365 global tenant level or more local site settings, it is vital to work out what classification boundaries need implementing. In this context a classification boundary is the scope for applying a common set of classification and retention controls.

4.1.3.1 Single classification boundary

A single classification boundary can be used to cover an entire organisation. At this level, all settings are done at an M365 tenant level and will apply to every area. Any retention labels, retention policies, and classification schemes are applied to all agencies and functions within the organisation.

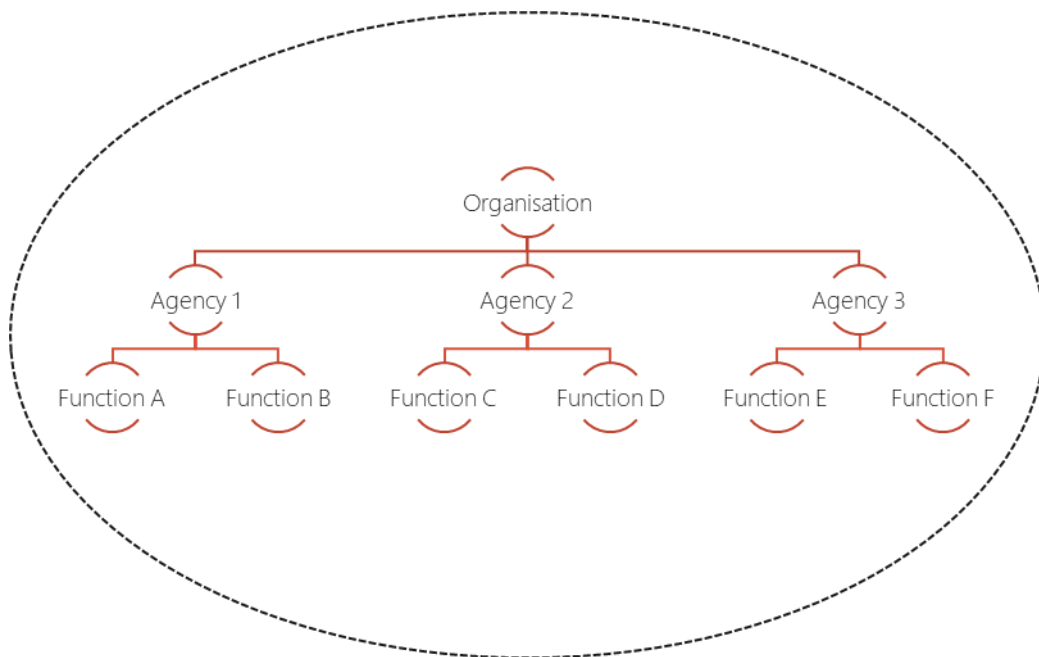


Figure 4 - A single classification boundary that aligns with the whole organisation and M365 tenant.

A single boundary can deliver the following benefits:

- **Reduced administration overheads** – most records and information management set up is undertaken globally, reducing the need for specialist roles within each area of the organisation.

- **Cross agency and function compatibility** – having a single classification and retention approach means any changes to organisational structure (such as machinery of government changes for public organisations) do not require reclassification of items.
- **Simplified information management training** – The consistent approach means any training is applicable across the whole organisation.
- **Global application of retention** – applying retention across tenant wide containers means the risk of items being deleted in error is reduced.

For it to be successful the following should be considered:

- **Commitment to a universal classification and retention scheme** – making a simple set of labels and classification terms to cover the whole organisation can be daunting, but keeping it simple makes it easier for end users
- **Difficult to tailor to wide functional areas** – It is possible to have some customisation, but this requires specialist skills within the functional areas.

Single classification boundary set ups work effectively for small organisations or those that see records and information management as a strategic priority.

4.1.3.2 Multiple classification boundaries

Where an organisation is made up of disparate agencies or functions it is useful to consider multiple classification boundaries. Whilst there may be some global retention policies to act as a safety net, the majority of activity occurs at a lower level.

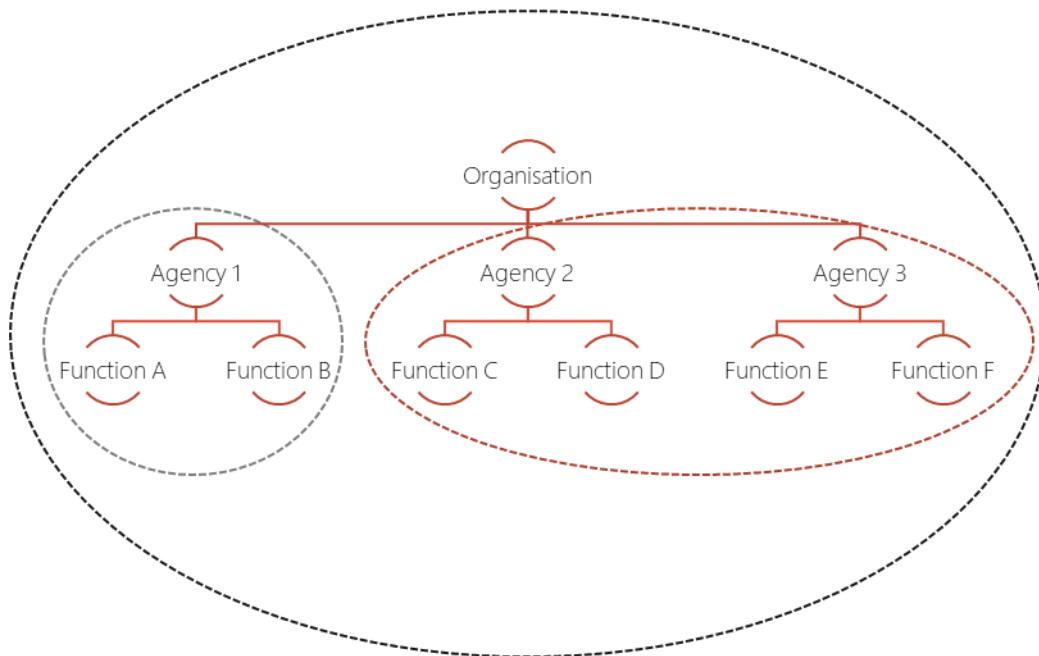


Figure 5 - A multiple classification boundary organisation with specific classifications and retentions applied to different areas.

Multiple classification boundaries can have the following benefits:

- **Flexible classification** – different classification schemes can be deployed to reflect different needs. This also potentially reduces the number of selections users must make in any given function.
- **Default labelling more targeted** – Applying classification and retention to items can be made easier for users by setting appropriate defaults that reflect an area’s needs.

A successful multiple classification boundary set up requires the following considerations:

- **Area level record or information management skills required** – With multiple classifications and varying retention, comes the need to have local skills to help manage the set up and support.
- **Restructuring is difficult** - Different retention labels and classification mean it can be hard to move items if reporting lines change.
- **Governance needs to be in place** – With multiple stakeholders, governance needs to be in place to work through different requirements.
- **Local level reporting** – with different classifications, reporting on exceptions or eDiscovery work needs to be undertaken at the local level.

4.1.4 Licencing

The features and capabilities that allow the full implementation of three lines of defence approach are made possible with Microsoft 365 E5 or the sub- component Microsoft E5 Compliance licensing.

Using Microsoft 365 E3 licencing does allow some records and information management functionality. However, much of the automation and default classification functions are not available. This means classification and labelling relies on user behaviour and inputs, and there is limited monitoring and management capability. This ultimately means the risk of unclassified and unmanaged records and information remains. Key features are compared below.

Feature	Microsoft 365 E5 / Microsoft 365 E5 Compliance	Microsoft 365 E3
Content and Activity Explorer	✓	✓
Classify data automatically based on Machine learning (training classifiers)	✓	X
Manually apply sensitivity labels in Microsoft 365 Apps (Office 365 ProPlus/Business client apps) using built-in labelling	✓	✓
Manually apply non-records retention labels	✓	✓
Apply a default retention label for SharePoint Libraries, folders, and document sets	✓	X
Apply a basic retention policy by workloads, specific locations or users	✓	✓

Automatically apply retention policies based on specific conditions (e.g., keywords or sensitive information)	✓	X
Automatically apply retention policies based on Machine Learning (trainable classifiers)	✓	X
Records Management (record labels, file plan manager, records versioning, regulatory record label)	✓	X
Retention labels disposition review	✓	X

Where Microsoft 365 E5 licencing is in place, there are numerous additional benefits over Microsoft 365 E3 licencing.

Feature	Microsoft 365 E5	Microsoft 365 E3
Classify data automatically based on Exact Data Match	✓	X
Automatically apply retention policies based on event	✓	X
Automatically apply sensitivity labels in Microsoft 365 Apps (Office 365 ProPlus/Business client apps) based on sensitive information types	✓	X
Advanced eDiscovery (Custodian Management, Deep Indexing, Analytics and Export)	✓	X
Insider Risk Management	✓	X
Customer Lockbox	✓	X
Cloud App Security	✓	X

Comprehensive details on licencing for all Microsoft 365 components, including security and compliance, can be found on the [Microsoft 365 licensing guidance for security & compliance](#) webpage.

4.2 People considerations

Platform setup is only part of the solution. It's vital to consider how people interact with the system.

4.2.1 Roles

In addition to the role of general users of M365 in managing the information they create and use, feedback from the WA State Records Office suggests a few important supporting roles. These may be part of the function of individuals or teams in your organisation:

- **Systems Admin role** – With the highest level of access this role allocates functions to other roles and makes any tenant level changes to retention policy.
- **Senior Information Management role** – This role determines the scope of retention policies and administers any global classification schemes used to apply any automatic

retention labelling. This role may also have oversight of eDiscovery functions and content search.

- **Information Manager / FOI role** – At a more local level this role would set up and manage any SharePoint site specific classifications and default labels. This role would also have access to the content search and eDiscovery functions to undertake and request for information tasks and reporting.
- **Disposition / Records Management role** – Again a local level this role has access to manage any disposition reviews required after retention periods have elapsed. The role can apply any specialist labels or approve deletion of items that are no longer required.

Whilst more granular roles may be needed, keeping things simple is important. Where a self-service process model is used, general users would have access to create SharePoint sites via Teams, and so take on the ownership role.

Each of these roles can then be configured within M365 to give the relevant access to the necessary functions.

4.2.2 Change management.

Building confidence in the solution requires a change management approach. For example, building a test instance of the platform, with days replacing the years for retention means the process can be reviewed end to end quickly before roll-out. The key audience for the change management effort in this case is those managing records rather than general users. The change in this area relates to shifting the traditional view of record management professionals to the risk-based approach. Demonstrating that risk is reduced by adopting a simpler, less granular, classification is an important step to wider adoption.

However, the audience may be broader for other proposed changes. Focusing on the user experience helps shape the policies and processes needed, and ensures the system is configured in a way that is pragmatic. This in turn reduces the risk that users can't or won't use the system. To assist with this, creating a set of general records management scenarios allows people to run through how the new approach would work.

It is also important to note that the modern records management approach can be used in conjunction with more traditional platforms and systems. The reality is that the modern approach focusses on the items currently not being managed effectively. Those items and records that are currently being managed can continue in parallel to any improvements being driven by adopting M365.

Creating a change and adoption plan that considers the impact to users and builds awareness, desire, knowledge, ability within the impacted groups and then reinforces the change should be part of any project delivering modern records management with M365.

4.3 Processes

At a basic level, the main process for a records and information management system is the way users provision containers and classify their items. There are essentially two different approaches, and the favoured M365 governance approach.

Deciding which best suits your organisation requires the following considerations:

- the number of classification boundaries within an organisation
- the favoured M365 governance approach
- the level of resourcing available.

The two approaches are:

4.3.1 Self service

Many organisations are aiming to provide a fully self-service approach to their record management operations (RM Ops).

Where staff facilitate their own work containers, such as SharePoint Team Sites or MS Teams, it is possible to deliver a self-service approach.

For this to work with M365, there are some factors to consider:

- **Good information management knowledge in the main staff group** – As users are directly making decisions that affect their records and information, they should have a good level of understanding around the principles of information management.
- **Simple classification schemes help** – The easier it is for users to select the right classification, the more likely it will happen. Generally self-service processes will need to be backed up by a single classification boundary to ensure items not classified or labelled are still retained.
- **Good access to Records Management support** – users will need to get support to answer their questions from subject matter experts. A central RM Team will still be needed to manage the broad, second line of defence, retention policies and to help users continually simplify their classification and retention schemes.
- **Monitoring exceptions is vital** – relying on end users increases the risk of incorrectly classified or labelled items. Records Management Teams will need to monitor regularly for exceptions.

RM Self service

A limited records management function relies on the configuration of information governance controls within the platform and staff to appropriately classify information.

Staff facilitate their own provision of the containers the need (MS Teams or SharePoint site), the container is provisioned with the means necessary for classifying records but is not pre-configured.

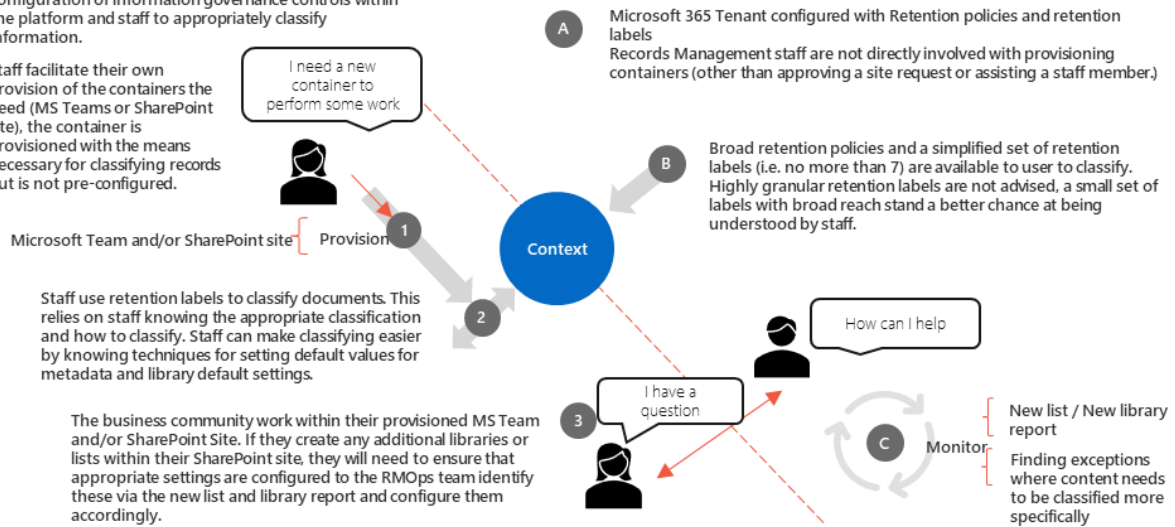


Figure 6 – Self-service records management process

4.3.2 Record Management Operations (RM Ops)

Taking a more supported record management operations (RM Ops) approach requires the RM team to take a more proactive approach in the provisioning of containers for users. Governance around the creation of SharePoint sites and MS Teams is recommended as this puts the decision making within the realm of the RM Ops Team. This is much more suited to an organisation that has multiple classification boundaries.

A request process can mean it takes longer to provision what users need but does mean the various services such as MS Teams or SharePoint have good default classification or retention labels applied. This ultimately makes it easier for users and reduces the risk that items use a second line of defence container retention policy, or don't have any labels applied at all.

For successful RM Ops to work with M365 there are some considerations:

- **A well-resourced RM Ops Team** – areas with major records demand will need to be supported with RM roles that can provision and configure the necessary containers.
- **Good governance structures** – governance of M365 and what users can create needs to be clear.
- **Records Management community of practice** – with likely multiple RM Teams and practitioners a strong community of practice helps with governance and consistency of approach.

RM Operations Model

A Records Management Operations RMOps model sees an organisation with an established Records Management function who provide advice and configuration for staff.

The RMOps team provide a bureau service taking requests for new information containers, provision and configure the new location with default values that mean that the end user doesn't have to worry about classifying content on an item-by-item basis.

The business community work within their provisioned MS Team and/or SharePoint Site. If they create any additional libraries or lists within their SharePoint site, the RMOps team identify these via the new list and library report and configure them accordingly.

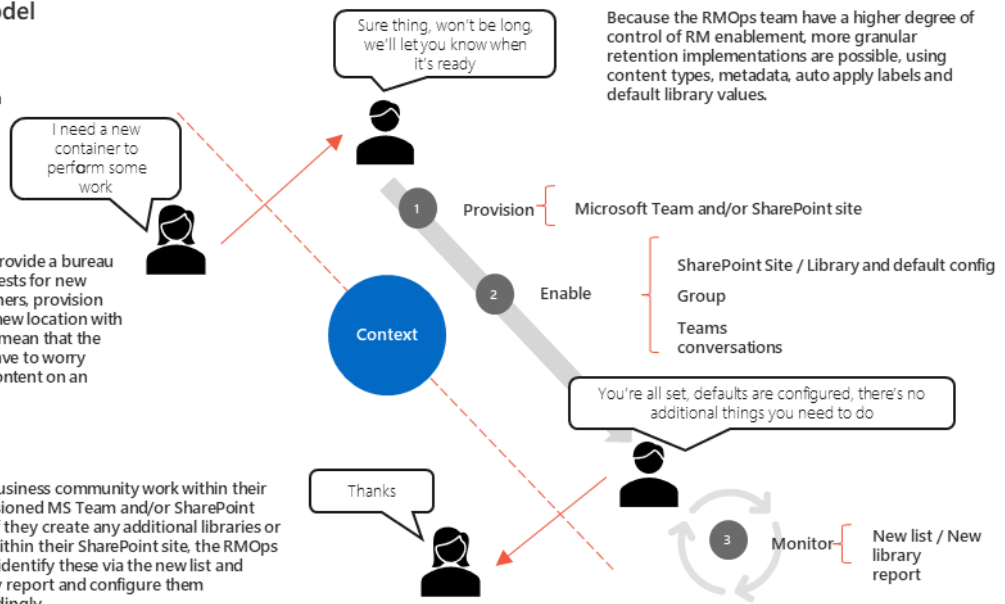


Figure 7 - RM Operations process model

4.4 Policies

The final piece of the solution for M365 modern records management is to develop a set of policies that meet the risk tolerance of the organisation, agency or function. The risk-based approach means the number of policies and depth of classification schemes should be as simple as possible.

A pragmatic approach could be considered the least-worse option, but it increases the likelihood of classification and retention taking place. Considering the risk relating to the content of items, means sensible policies can be created that protect against most risks. With RM Teams acting in a supervisory capacity, exceptions can be managed so high-risk content can get the additional focus it needs.

4.4.1 Classification schemes

Retention and disposal schemes (RDS) or retention and disposal authorities (RDA's) are common to provide a classification for information, an associated retention period and an action to take once that period elapses.

Setting up classification schemes in the M365 term store allows users and RM Teams to apply the metadata to items in document libraries, and then have M365 auto-apply the associated retention period and action.

When looking at classification schemes consider how they relate to risk:

- What are the high-risk categories?
- Do the subcategories make it clear for a user the difference between them?
- Are categories split with concepts like 'significant'?

Classification can then be collapsed by applying the highest risk of the subcategories to all items within the category.

For example, within the Western Australian General Disposal Authority for State Government (GDASG) there are three subcategories within the term Accidents / Emergencies / Incidents. These relate to the significance of the accident and if injury or death happens. Each subcategory has a different retention requirement.

NUMBER	TERMS	DESCRIPTION	CUSTODY
1	ACCIDENTS / EMERGENCIES / INCIDENTS	Management of accidents, emergencies and incidents, including: Injury to staff. Injury to visitors / clients	
1.1	ACCIDENTS / EMERGENCIES / INCIDENTS	Records of significant accidents, emergencies or incidents, including incidents that cause death or permanent disability. Records include notification, investigation, response, management and reporting.	Retain 5 years after action completed, then transfer to the SRO.
1.2	ACCIDENTS / EMERGENCIES / INCIDENTS	Records of accidents, emergencies or incidents which are not included in Section 1.1 and which impact the environment (e.g. oil / chemical spills). Records include notification, investigation, response, management and reporting.	Retain 20 years after action completed, then destroy.
1.3	ACCIDENTS / EMERGENCIES / INCIDENTS	Records of accidents, emergencies or incidents not included in Sections 1.1 or 1.2. Records include notification, investigation, response, management and reporting.	Retain 7 years after action completed, then destroy.

Figure 8 - extract from the WA-GDASG

Reviewing the subcategories shows that the most high-risk items should be retained as a state record after 5 years. Applying this approach to the other subcategories would mean that all items in this classification would be retained for a minimum of 5 years and then be sent for a disposition review. At this point an item can be relabelled by the reviewer to either be kept indefinitely as a state record, have an additional period retention applied, or be destroyed.

Pragmatically, any item that could be one of the subcategories could be handled with limited risk is the retain for 5 years and review is applied. The significance of the incident can be reviewed after 5 years rather than trying to apply a subcategory at the time items are created.

Following a similar process means a complex term set can be significantly reduced along with the number of retention labels that are associated.

4.4.2 Retention labels

Retention labels fall into one of three categories that can then be added into the M365 compliance center.

The first is the set of labels that are published for users to select (if appropriate). Considering the risk, it is possible to create a set that covers most needs. Using simple language these are broken into short term, operational business, operational business followed by a review, long term, evidential and litigation, retain in archive.

The second set is a repeat, but these are used to auto-apply based on the classification scheme and are not published for users to select.

The third set is for disposition reviewers to apply once an initial retention period has elapsed, and the item is reviewed.

Example user selectable labels

Name	Retention period	Trigger	Post retention action	Notes
Retain Short Term then delete	3 years	From last modified	Automatically deleted	Replaces the need for all items from 0-3 years
Retain Operational Business then delete	7 years	From last modified	Automatically deleted	Covers everything 4-7 years that has no need of a disposition review
Review after Operational Business	7 years	From last modified	Sent for disposition review	Records supervisor to review and either delete or apply new label
Review after Long Term	25 years	From last modified	Sent for disposition review	Records supervisor to review and either delete or apply new label - covers items that need to have a longer operational business retention
Retain for evidential litigation	75 years	From last modified	Sent for disposition review	Used for personal records or those involving incidents or hazardous materials
Retain to State Archive	5 years	From last modified	Sent for disposition review	For those items that may be required for State Archives. A review is triggered after 5 years to determine if needed for archive and the applicable label then applied or deleted

Example auto-apply labels.

Name	Retention period	Trigger	Post retention action	Notes
AA-Retain Short Term then delete	3 years	From last modified	Automatically deleted	Replaces the need for all items from 0-3 years
AA-Retain Operational Business then delete	7 years	From last modified	Automatically deleted	Covers everything 4-7 years that has no need of a disposition review
AA-Review after Operational Business	7 years	From last modified	Sent for disposition review	Records supervisor to review and either delete or apply new label
AA-Review after Long Term	25 years	From last modified	Sent for disposition review	Records supervisor to review and either delete or apply new label - covers items that need to have a longer operational business retention
AA-Retain for evidential-litigation	75 years	From last modified	Sent for disposition review	Used for personal records or those involving incidents or hazardous materials

AA-Retain to State Archive	5 years	From last modified	Sent for disposition review	For those items that may be required for State Archives. A review is triggered after 5 years to determine if needed for archive. The applicable label is applied, the item is moved to an alternative archive or deleted
AA-Long Term Hazardous material	75 years	From last modified	Sent for disposition review	Search for hazardous material names such as asbestos and apply a long-term retention period

Example post-disposition labels (Disposal reviewers only)

Name	Retention period	Trigger	Post retention action	Notes
DIS - Retain Short Term then delete	3 years	From when label applied	Automatically deleted	Applied if following review an additional short time retention is required before deletion
DIS - Retain Long term then delete	25 years	From when label applied	Automatically deleted	Applied following a review if not needed to be archived, but a long-term retention applies - item not reviewed again
DIS Retain for evidential litigation then delete	75 years	From when label applied	Automatically deleted	Applied following a review if not needed to be archived, but an evidential retention applies - item not reviewed again
DIS - Archive in place	Forever	From when label applied	N/A	Used to mark an item as being needed in the State Archive, but being stored in place

By structuring labels in this way, items adopt a retention period that is 'rounded up'. The question to consider is "what is the risk of keeping the item for this length of time?". In general terms the risk is tolerable in the simplified set of labels, but any exceptions can still be applied if absolutely necessary. In the case of the example labels, any item is at least going to be kept for 3 years, but if not needed beyond this it will get deleted.

The principle for the action after the retention period is the shorter the retention the more likely the item is automatically deleted. Therefore, the short-term label is followed by automatic deletion, the operational business label has both a delete and review version, and all other labels mean an item is always going to be reviewed.

A note on auto-applied labels

M365 allows for items to have retention labels applied based on auto-applied rules such as an associated classification term.

As a general principle, for rules that are set to retain information using a low confidence level for any match, such as 60%, means if there is doubt the item will be retained.

For rules that are set to delete information, using a high confidence level, such as 90%, before automatically deleting means if there is doubt, again, the item will be retained rather than deleted.

5 Conclusion

With the addition of the right licencing and set up, it is possible to effectively manage records and information through M365 that enables more information is appropriately accessible to more people in your organisation now and into the future; and enables compliance with the requirements of the relevant record keeping obligations (for example the State Records Act. For your location).

M365 is familiar to many through its Office applications, so making this the basis for an approach can simplify adoption across your organisation. Applying classification, sensitivity, and retention metadata within M365 rather than relying on the transfer to a separate record keeping tool will reduce the risk of information being unmanaged. Continuing to use existing approaches is unlikely to close the gap.

For it to be successful you do need to consider the other parts of your information management system – the processes, policies, and people. This involves working on reducing the granularity of classifications and retention options by considering the risks and your tolerance towards them. Reducing the overall risk of records and information being unmanaged is the aim rather than striving to have each and every record tagged to a deep and complex classification scheme.

Deciding on the level of self-service versus support will relate to the level of governance demand you place on general users or specific information management roles. It also determines what is set up at a tenant wide level and what is set up at a lower site or team level.

Adopting a risk-based approach to records and information management means the overall system is simplified for both users and administrators. This does involve accepting a certain tolerance for risk and being flexible in how granularly you apply your classification and retention schemes. However, the simplification means the overall risk of items remaining unmanaged is reduced.

5.1 Key Takeaways

- Using M365 for modern records management requires a mindset shift from the traditional approach used in many DRM Systems.
- Aiming to simplify the records and information management system for users requires significant effort from records management practitioners and teams.
- As a minimum M365 E5 compliance licencing is needed to maximise the risk reduction from taking a modern records management approach
- Using M365 for records and information management is not necessarily mutually exclusive of using other records management systems.

6 About the Authors

Engage Squared is on a mission to empower employees to enjoy work more - using Microsoft tools to make work more productive, collaborative and connected.

We work with large organisations to empower teams and individuals to use new technology to work productively (by migrating to O365, undertaking adoption and change management campaigns and / or configuring information and records management solutions), to help their leaders connect with their staff (by developing powerful new Intranets and digital workplaces built on modern SharePoint, and by rolling out Yammer), and to tailor Office 365 workloads to boost productivity (using all of the Microsoft 365 suite, including PowerApps and Power Automate).

As a Microsoft Preferred Partner for Content Services, Engage Squared is recognised for delivering enterprise content management solutions to serve modern customer needs – with solutions ranging across highly document-centric industries, to critical compliance-focused scenarios, and less structured collaborative organisations.

6.1 Andrew Jolly

Andrew is the Information Management Practice Lead at Engage Squared, he helps organisations craft systems to share information, manage documents and content, collaborate on projects, automate processes, and meet record keeping and compliance obligations; allowing everyone to make improved decisions, more effectively.



With over 15 years' experience with the Microsoft SharePoint and 365 platforms Andrew combines a pragmatic approach to modern records management means which his extensive knowledge of what information management and productivity mean when it comes to the Microsoft ecosystem.

Contact him at andrew.jolly@engagesq.com or on 0423 539 710.

6.2 Matt Dodd

Matt is a Digital Workplace Consultant at Engage Squared, he changes the way people work, create and connect through human centred approaches to culture, leadership and digital services. He combines design, empathy and systems thinking to deliver value to individuals and organisations.



Since 2004, he's been working in large organisations delivering digital based change. He's led programs enabling online services for local government and pioneering the use of social media platforms for customer and colleague engagement. He's spent the last few years' shaping the digital employee experience at CBA subsidiary Bankwest; delivering an award-winning Yammer enterprise social network along the way. At Engage Squared he's now working with Western Australian organisations to build digital capability and transformational experiences.

Contact him at matt.dodd@engagesq.com or on 0477 373 083.