Functional Requirements for Managing Records in Microsoft 365

Digital Preservation Coalition – November 2023

adri Australasian Digital Recordkeeping Initiative

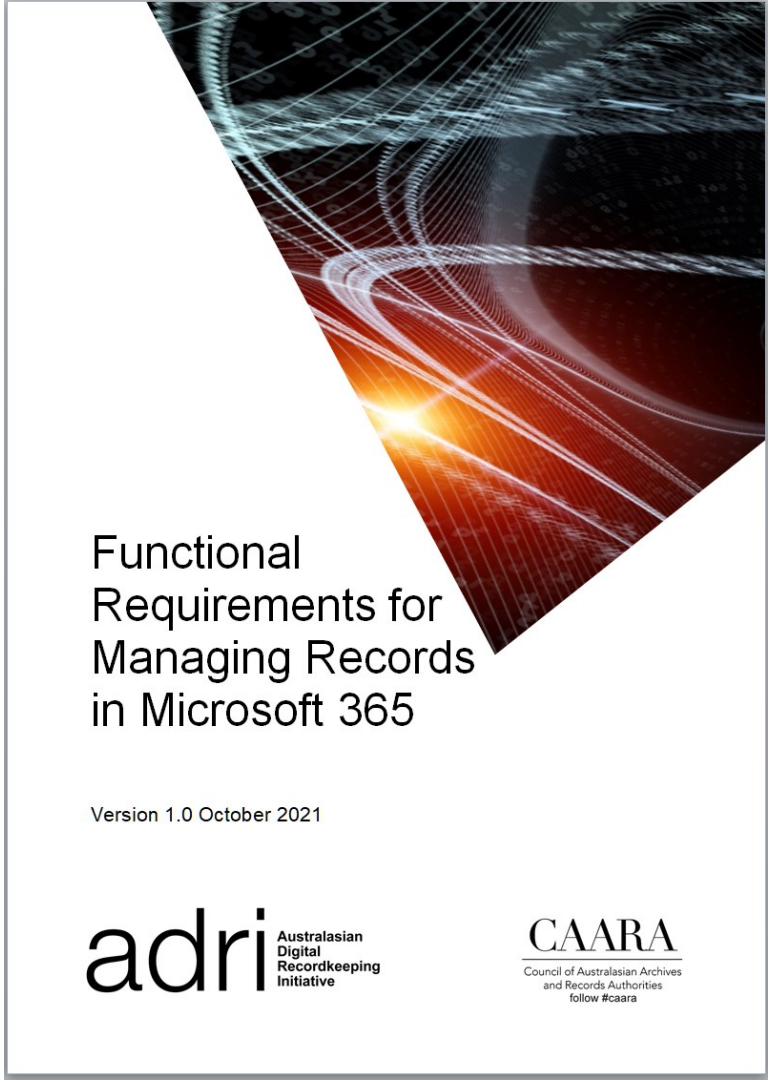
CAARA
Council of Australasian Archives and Records Authorities
follow #caara

Public Record Office Victoria

VICTORIA State Government

A resource for Australasian recordkeeping, *Functional Requirements for Managing Records in Microsoft 365*: https://www.caara.org.au/index.php/working-groups/adri/products/

It is a product of the Australasian Digital Recordkeeping Initiative (ADRI), a working group of the Council of Australasian Archives and Records Authorities (CAARA).



Public Record Office Victoria

CAARA members

National authorities
National Archives of Australia
Archives New Zealand

State and territory authorities
Library & Archives NT
Public Record Office Victoria
Queensland State Archives
State Archives and Records Authority of New South Wales
State Records Office of Western Australia
State Records of South Australia
Tasmanian Archives
Territory Records Office (ACT)

Motivation

Public sector agencies are increasingly using M365 to create and manage their records.

High volume of requests from agencies and service providers, frequently ‘is M365 compliant?’

So many factors to consider -

Licence, features, configuration, point in time, usage, governance and management – and the module being used and records being managed

Sources

The primary resources used in the development of the functional requirements are the standards and specifications set by ADRI member archival authorities.

Those standards and specifications are informed by Australian and International Standards, in particular:

- Creation, capture and management of records (e.g. ISO 15489)
- Functional requirements for records in business systems (e.g. ISO 16175 pt.3 2010)
- Functional requirements for digital records management systems (e.g. ISO 16175 pt.2 2011)

Additional SAAS-related requirements were drawn from the ADRI paper ‘Information Management Requirements for Software-as-a-Service’, v1.0 May 2020

Principle 1: Design and configuration of M365 implementations must include recordkeeping requirements

R1. The use of persistent metadata for records must be supported.

- The system should, as far as possible, support its routine capture (including a
  where this is possible).
- If the system is not able to ensure that persistent metadata is supported, th
  be moved to a system that can support it.

R2. Systems holding records must enable them to be identified, retrieved, and used for
of time they must be retained.

R3. The system must prevent the unauthorised or premature destruction of records (including contextual metadata).

R4. The system must protect metadata from unauthorised deletion or modification. The system should allow an authorised records or system administrator to alter the metadata of a record if required, such as, to allow finalisation or correction of the record profile. Any such action must be captured as additional records management metadata.

R5. The system must support the design and implementation of protection and security controls to ensure records are only accessed, amended, used, released, or disposed of as authorised. Access, security, and user permissions for systems managing records and information must be documented and implemented.

This work is about setting the bar

Principle 5: Access to records in M365 must be proactively managed from creation and capture to disposal

R16. Imported records must preserve the integrity of the record (content and metadata).

R17. All records must be maintained in a format that is expected to survive and remain accessible and readable using readily available software for the required life of the record.

R18. Bulk retrieval of content and metadata for secondary use in unrelated applications must be allowed.

R19. All information, including information created, accessed, or modified by contractors an party providers engaged in outsourcing arrangements, must be accessible when re agency must ensure that the records are not put at risk if the service provider is ac another organisation during the contract, and that records are returned to the age end of contract, including relevant metadata, in the form the agency specifies.

R20. The system must support the implementation of security classifications and requir are applicable to the sensitivity of the information. Records that carry security class (i.e., those requiring an elevated level of protection) must be handled and stored in co with the requirements of the classification.

Some are not strictly 'functional'

Scope

- Intended to enable application to systems in the broad sense and includes M365 plus any third-party integration or procedures. The focus is on outcomes not specific products.
- Applicable at any stage in procurement, implementation and management.
- Audience is broad – so specialised recordkeeping knowledge is not assumed.

If you have any questions or comments regarding this work, please contact peter.francis@prov.vic.gov.au

adri Australasian Digital Recordkeeping Initiative

CAARA
Council of Australasian Archives and Records Authorities
follow #caara

Public Record Office Victoria

VICTORIA State Government