Manitoba

Records and Information Management Framework

Government Records Office
Archives of Manitoba

Version Control

Initiated	July 2017
Final Draft	February 2018
Endorsed by the Archivist of Manitoba	April 2018
Published	May 2018

Authority

This framework is issued under section 8 (a) of *The Archives and Recordkeeping Act* which enables the Archives of Manitoba to establish government-wide policies, standards and guidelines for recordkeeping based on professional standards and best practices.

Acknowledgements

This framework is based on the State Records Authority of New South Wales' *Standard on records management* (2015) and *Implementation Guide* (2015) and the Archives of New Zealand's *Information and records management standard* (2016) and *Implementation Guide* (2017).

References

This framework is in accordance with the International Standards Organization (ISO) group of standards, technical reports and codes of best practice on Archives/records management - ISO/TC 46/SC 11.

Contents

Introduction

Records and information are key strategic assets of government and are the evidence of government business. In the Manitoba government, records and information help departments and agencies plan for and achieve short-term and long-term outcomes that benefit citizens, business and government.

Ensuring that evidence of government business is created, captured and managed is not simply about legislative compliance. A well-managed information base is the foundation of responsible, accountable government. It is also the underpinning of public service transformation and innovation strategies such as data-driven evaluation and evidence-based decision-making.

Records and information:

- provide the foundation for sustainable and effective programs, products and services
- support decision-making
- outline responsibilities
- document rights and entitlements
- drive collaboration and communication
- facilitate and enable transformation, creativity and growth
- preserve public knowledge for discovery and reuse
- make up the corporate memory of an organization
- support transparency and accountability

To provide these benefits, records and information need to be:

- routinely created and captured
- trustworthy
- available when needed, understandable and usable
- secured and protected
- valued as critical to business operations
- part of an organization's approach to risk management
- maintained and disposed of in an authorized way
- managed effectively and responsibly

Purpose / Scope

This framework sets out three high-level principles and corresponding requirements for effective records and information management in the Manitoba government. It is designed to help departments and agencies understand their records management responsibilities and meet their obligations under *The Archives and Recordkeeping Act*.

This framework covers records and information in all formats, including both digital and physical records, and focuses attention on digital recordkeeping as the Government of Manitoba continues its transition to digital business processes.

The purpose of the framework is to ensure that in complex business and information environments, business is supported by sound, integrated records and information management.

The framework is applicable to all Manitoba government bodies, as defined in *The Archives and Recordkeeping Act.* It should be read in conjunction with instructions, directions, and any other standards or guidance issued by the Archives of Manitoba under the authority of the Act.

Benefits of using this framework

Departments and agencies that meet the requirements in this framework will:

- create trustworthy, useful and accountable records and information in evolving business environments
- ensure that meaningful, accurate, reliable and useable records and information are available whenever required for government business
- sustain and secure the records and information needed to support short and long-term business outcomes
- enable the reliable sharing of relevant records and information
- minimise records and information volumes, preventing unnecessary digital and physical storage and management costs
- proactively protect and manage the records and information that provide ongoing value to government business and to the public
- meet obligations and requirements of *The Archives and Recordkeeping Act*

Further information

An implementation guide to support departments/agencies in meeting the requirements is in development. Contact GRO@gov.mb.ca.

Principle 1: Departments are responsible for records and information management

To ensure records and information are able to support all business functions and operations departments must:

- Assign responsibilities and allocate resources
- Develop business-specific strategies and priorities directing how records and information will be managed
- Communicate responsibilities, strategies and priorities throughout the department
- Monitor records and information management activities, systems, and processes

Minimum requirements	Explanation	Examples demonstrating compliance
1.1 Records and information management (RIM) is the responsibility of senior management.	Ultimate responsibility for records and information management lies with senior management. They must provide direction and support and ensure RIM meets legislative and business requirements in their department. Visible senior management commitment and support sets the expectation for staff to conduct business according to accepted standards of practice. Responsibility for RIM is cascaded down throughout the department, to various levels of management.	• Responsibility is identified in department strategies and policies. • An executive lead is assigned by the Deputy Minister and this role is identified in RIM strategies and policies. • Senior management is meeting requirements under the ARA. • RIM is a regular agenda item in management committee meetings.
1.2 RIM must be directed by department-focused strategy and policy.	Governance frameworks are critical to effective records and information management (RIM). Departments must set high-level strategy and policy for managing records and information. The administrative head of the organization must endorse the policy and it must be communicated and implemented at all levels.	• An organization-wide directive on RIM is adopted and communicated.

Minimum requirements	Explanation	Examples demonstrating compliance
1.3 Organizations must have skilled RIM staff or access to appropriate skills.	Records management professionals are responsible for working with program managers and allied information professionals to lead or support such activities as records scheduling, development of records classification systems, analysis of recordkeeping requirements in business processes, design and implementation of records systems, and delivery of role-specific training. An organization must be able to access records and information management skills through recruitment, service providers, and by networking with other organizations.	• Departments have a RIM expert. • The role is identified in strategies and policies on RIM and communicated throughout the organization. • The responsibilities, skills and capabilities are defined in job descriptions and performance plans. • The RIM expert is consulted in all business process transformation and system design projects. • The RIM expert is in regular contact with the GRO.
1.4 Division, branch, and program area management must take responsibility for integrating RIM into work processes, systems, and services.	This requirement places responsibilities more broadly within the department. It reflects a business manager's detailed understanding of the records and information produced by and necessary to perform their work, and their responsibility for ensuring its management. Cascading responsibility to different business areas of the organization lets business unit staff and records and information staff work together to ensure that RIM is integrated into business processes, systems, and services. Organizations with a strong capacity consider RIM requirements in departmental strategic planning, financial and human resources planning, risk management, and the development of policies, programs, services and systems. Business managers must be aware that RIM requirements are needed when they move to a new service environment; develop new business processes, systems or services; or improve on existing business processes, systems or services (see Principle 2).	• Responsibility is assigned and identified in a RIM directive. Roles and responsibilities are understood.

Minimum requirements	Explanation	Examples demonstrating compliance
	Business owners must demonstrate that they have considered RIM requirements and assessed risks as part of the business development process.	
1.5 All staff understand their recordkeeping responsibilities.	All staff, including contractors, must understand their RIM responsibilities. Policies, business rules and procedures must include clear requirements for creating and managing records and information. Roles and responsibilities for RIM must be defined, assigned and communicated throughout the department, so that those responsible have the authority required to carry out their duties and the appropriate position and expertise. These roles and responsibilities include: • Senior managers, who have overall program responsibility and are expected to promote program compliance and allocate resources/funding (see 1.1). • Records management professionals, who establish and implement policies, procedures and standards (see 1.3). • Program managers, who ensure that staff follow recordkeeping guidelines to create and keep records to document business processes (see 1.4). • All staff, who must create and keep records in accordance with RIM guidelines, policies and procedures.	• The RIM directive is communicated to all staff. • Policies and procedures outline staff responsibilities. • Orientation and training is tailored to the appropriate audience and supports the organization's RIM responsibilities and goals.
1.6 Contracts and agreements must consider RIM requirements.	Corporate policy and strategy should include responsibilities for ensuring that records and information requirements are identified and met. Organizations should undertake risk assessments and have RIM issues addressed in any agreed upon contractual arrangements. An organization must ensure that the portability of records and information and associated metadata is assessed and appropriately addressed in outsourcing and service contracts, instruments, and arrangements.	• RIM requirements have been analyzed and identified (see 2.1). • RIM requirements have been incorporated into contracts, agreements and service arrangements in consultation with Legal Services and the GRO.

Minimum requirements	Explanation	Examples demonstrating compliance
1.7 RIM must be monitored and reviewed.	Policies alone will not guarantee good RIM practices. Success requires active and visible support by senior management and a commitment to continuous improvement.	• All processes and systems are reviewed regularly to ensure they are meeting business requirements and RIM best practices. • Monitoring activities are documented.

Principle 2: Recordkeeping requirements are linked to business requirements

Records and information management (RIM) is a corporate activity designed to ensure the systematic creation, maintenance, usability and sustainability of records needed for business operations. RIM must be planned by management and linked to business requirements. Program areas need to:

- Analyze and define their key records and information requirements
- Design and embed requirements into business processes and systems

Minimum requirements	Explanation	Examples demonstrating compliance
2.1 Records and information needed to support business must be identified and documented.	This requirement provides the foundation for managing records and information in all environments. By analyzing and documenting functions and activities, an organization can identify what records and information it needs to support business. Decisions on what records and information are required should be documented in business rules, policies and procedures, and should also be incorporated in system specifications and metadata schema (see 2.3). An organization must embody these decisions in records schedules (see 2.4).	• Functions and activities of the organization are analyzed to determine what records are required to document activities. • RIM requirements are integrated into documented business rules. • Up-to-date records schedules are in place and regularly reviewed.
2.2 High-risk/high-value areas of business and the records and information needed to support them must be identified.	High-risk/high-value functions include those that: • Protect the rights and entitlements of citizens • Protect public safety or health • Collect and use sensitive personal information • Are subject to close scrutiny by the public or oversight bodies • Allocate or spend large amounts of money • Require long-term retention of records and information By identifying high-value records and information at creation, an organization can better manage and use these core assets. Better management can increase the value of information.	• Risks are identified, managed or mitigated. • Systems managing high-risk/high-value records are protected by business continuity strategies and plans.

Minimum requirements	Explanation	Examples demonstrating compliance
	Departments must identify the potential risks to records and information and mange or mitigate them. This includes protecting the systems that manage records and information that are high-risk/high-value from loss and damage. Departments should set up appropriate security measures and business continuity strategies and plans.	
2.3 RIM must be an essential consideration in design of all systems where high-risk/high-value business is undertaken.	In complex business and systems environments, it is important to build in RIM requirements from the start (see Principle 3). This is particularly important where the business involves high-risk/high-value activities. Where systems supporting high-risk/high-value records and information have not included RIM requirements, mitigation strategies must be adopted.	• Systems specifications include RIM requirements. • Systems design and configuration is documented and maintained. Systems that do not meet requirements: • Are identified • Risks are mitigated • Are redesigned to include requirements.
2.4 Records and information are managed comprehensively across all operating environments.	Regardless of format, records that relate to the same transaction, case or business event/decision should be managed comprehensively, so that they can easily be identified, retrieved or disposed of. Records schedules are a basic mechanism for managing business records. They identify records held by government and provide an important inventory for planning, protecting and providing access (see 3.6). Under the *Archives and Recordkeeping Act*, all government records must be scheduled, regardless of how long they need to be kept or what format they are in.	• Internal inventories, policies, procedures, and processes document where records are created and held, and in what form. • Records schedules are prepared and approved.

Minimum requirements	Explanation	Examples demonstrating compliance
2.5 RIM is designed to safeguard records and information with long-term value.	This requirement ensures that the Archives of Manitoba can identify which systems and service environments hold records and information with long-term or archival value. This requirement builds on minimum compliance requirements 2.1, 2.2 and 2.4 and works in conjunction with approved records schedules. Records and information designated as having archival value must be safeguarded and managed appropriately over time to ensure authenticity, reliability, trustworthiness and accessibility. Permanent or long-term records and information will outlive the systems in which they currently reside and will also outlive outsourcing arrangements and contracts with service providers. Organizations must ensure that they plan and manage the protection of permanent or long-term records and information through transitions of systems (system migration, conversion, and/or decommissioning) and changes to service arrangements (termination of services, new outsourcing arrangements). Permanent and long-term records must also be protected during and after administration and machinery of government changes. This includes records and information that must be transferred between organizations and also records that may remain with the creating organization.	• Program areas work with the Archives of Manitoba to develop records schedules, the means by which the Archives identifies records with long-term value. • Records are kept in accordance with approved records schedules.
2.6 Records and information requirements are maintained through systems and service transformations.	Rapid changes in information technology can leave critical business records and information inaccessible. Many government records need to be kept for longer than the expected lifespan of the systems they depend on. Ensuring continued access to electronic records requires inclusion of retention requirements in system design and a planned approach to migration. An organization must have documented migration strategies, and appropriate planning and testing processes. These must ensure that records and information are not 'left behind' or disposed of unlawfully.	• A migration strategy is implemented and regularly reviewed. • The process of migrating or converting records, information, and metadata from one system to another is managed to ensure records remain trustworthy and accessible.

Minimum requirements	Explanation	Examples demonstrating compliance
	An organization must use a migration, conversion, and/or decommissioning process that ensures that records and information are kept for as long as needed	• The portability of records and information and associated metadata is addressed in outsourcing or service arrangements. • The decommissioning of systems follows the requirements for disposing of records and information. • System documentation is maintained.

Principle 3: Records and information are well managed

Effective records and information management (RIM) is based on trustworthy and reliable records and information that are accessible, reliable, and maintained for as long as they are needed to meet business requirements. This extends to all records formats, in all business environments, and in all types of systems.

Minimum requirements	Explanations	Examples demonstrating compliance
3.1 Records and information must be created and managed as part of normal business activities.	Decisions about what records to create are business decisions that must be based on the requirements and obligations of the organization. Policy, rules and processes articulate and inform the organization and its staff of the requirements and responsibilities for creation, capture and management of records supporting the organization's business processes. An organization must identify, assess the risk, resolve or mitigate, and document any exceptions that affect the creation, integrity, accessibility and usability of its records and information. An organization's staff and contractors must conform to policies, business rules and procedures, to ensure records and information are routinely created and managed.	• Policies, business rules and procedures articulate staff requirements and responsibilities for the creation, capture and management of records. • Assessments or audits demonstrate that systems operate routinely. • Exceptions to routine operations that affect information integrity, usability or accessibility are identified, resolved and documented.
3.2 Records and information must be reliable and trustworthy.	A key purpose of records is to provide evidence of business activities. The value of records as evidence depends on the organization's ability to demonstrate that the records have not been modified or altered. Demonstrating this requirement is accomplished by ensuring that records have adequate metadata to provide meaning and context, and that the metadata remains associated with the record.	• Systems are in place that create and capture adequate metadata. • System audits are able to test management controls of systems, including information integrity. • Appropriate systems, processes, and documentation are in place to ensure metadata demonstrates reliability and trustworthiness.

Minimum requirements	Explanations	Examples demonstrating compliance
3.3 Records and information must be identifiable, retrievable, accessible, and usable.	An organization must associate or link appropriate minimum metadata to records or information to ensure the records and information can be identified, retrieved and shared. To maintain the accessibility and usability of digital records and information, an organization must ensure it regularly migrates or moves them from one system or platform to another (see 2.5 and 2.6). An organization must regularly test systems and perform assessments or audits to demonstrate that the systems can locate and produce records and information that can be read and understood. To maintain the accessibility and usability of physical records and information, an organization must keep them in appropriate storage areas and conditions.	• Testing is able to verify that systems can locate and produce records and information that are viewable and understandable. • Appropriate minimum metadata is in place. • To maintain the accessibility and usability of digital records and information, an organization must ensure it regularly migrates or moves them from one system or platform to another. • Appropriate storage of physical records is deployed in the active phase (in office) and the Government Records Centre is used to store semi-active records.
3.4 Records and information must be protected from unauthorized access, alteration, loss, deletion and/or destruction.	Records and information must be protected. Clearly defined, documented and distributed guidance and procedures are essential and an organization must implement an information security policy and appropriate security mechanisms. The policy must cover records and information held physically and/or digitally. Security measures should include: • access and use permissions in systems • processes to protect records and information no matter where they are located, including in transit and outside the workplace • secure physical storage facilities Undertaking regular assessments or audits will help an organization verify that access controls have been implemented and are working.	• Information security and protection mechanisms are in place. • Records and information are protected wherever they are located, including in transit, outside the workplace, and on removable storage media or mobile devices. • Assessments or audits can test that access controls are implemented and maintained.

Minimum requirements	Explanations	Examples demonstrating compliance
3.5 Access to, use and sharing of records and information must be managed appropriately, in line with legal and business requirements.	An organization must ensure that access to, use and sharing of records and information are in compliance with legal requirements such as *The Freedom of Information and Protection of Privacy Act*, *The Personal Health Information Act*, *The Mental Health Act*, *The Child and Family Services Act*, *The Youth Criminal Justice Act,* etc. Undertaking regular assessments or audits of systems will help an organization verify that access to, use and sharing of records and information is managed in accordance with business requirements and legal obligations.	• Policies, business rules, and procedures identify how access, use, and appropriate sharing of information are managed. • Assessments and audits confirm access requirements.
3.6 Records and information are kept for as long as needed for business, legal, and accountability requirements.	Records schedules are a basic mechanism for managing business records. They establish minimum retention periods and are required to authorize disposal of all government records. Records schedules should be regularly reviewed to ensure they reflect current recordkeeping arrangements and needs. Records and information must be scheduled and disposed of according to the provisions of authorized records schedules. This includes records and information located in business systems, in outsourcing or service agreements, or in physical storage. An organization must implement policies, business rules and procedures to ensure that records and information are kept for as long as required.	• Retention requirements are identified and reflected in up-to-date, approved records schedules. • Policies, business rules, and procedures support retention requirements. • Records that have been designated as archival are protected and maintained according to the provisions of approved records schedules and the direction of the Archivist of Manitoba (see 2.5).
3.7 Records and information must be systematically disposed of when no longer required, and when authorized and legally appropriate to do so.	Physical records must be disposed of in accordance with approved records schedules and Government Records Office policies and procedures. To apply retention and disposal rules to electronic records, two things are needed: up-to-date records schedules that authorize retention periods and disposal actions for these records; and electronic recordkeeping systems that enable automated retention and disposition based on the records schedules.	• Disposal complies with authorized records schedules. • GRO procedures and processes for disposal of records and information are followed. • Disposal of records and information is documented.

Terms and definitions

activity – "major task performed by a business entity as part of a **function**." [ISO 15489-1:2016, 3.2]

ARA – *The Archives and Recordkeeping Act* (C.C.S.M. c. A132). The ARA was proclaimed in February 2003 and replaced Part II of the *Legislative Library Act, "*Public Records and Archives", which had been in force since 1967. The Act applies to records of all departments and agencies of the Government of Manitoba. It also provides for agreements respecting the management and preservation of records of the Courts and the Legislative Assembly and its offices.

The Act establishes a modern framework for managing the records of government and for the Archives' operation. The ARA:

- uses updated language to encompass records in all formats
- confirms the Archives' lead role in establishing policies, guidelines and services needed to promote good recordkeeping in government
- sets out the duty of government bodies to schedule records, and to retain and dispose of records in accordance with approved schedules
- confirms the Archivist of Manitoba's role in identifying records of lasting significance to government and society, and in working with government agencies to develop strategies for long-term preservation and use of the records.

Archives – the Archives of Manitoba.

conversion – "process of changing records from one format to another." [ISO 15489-1:2016, 3.6]

department - the framework refers to 'department' as a simplified term for all **government agencies** and **government bodies**. This framework uses the terms 'department', 'organization', 'business' and 'program area' interchangeably.

destruction – "process of eliminating or deleting a record, beyond any possible reconstruction." [ISO 15489-1:2016, 3.7]

disposal action – the action taken at the end of the total retention period: records are either designated as archival or designated for destruction. Also referred to as **disposition**. Disposal actions are documented and approved in **records schedules**.

disposition – see **disposal action**.

evidence – "documentation of a transaction. This is proof of a business transaction which can be shown to have been created in the normal course of business activity and which is inviolate and complete. It is not limited to the legal sense of the term." [ISO 15489-1:2016, 3.10]

function – "group of activities that fulfils the major responsibilities for achieving the strategic goals of a business entity." [ISO 15489-1:2016, 3.11]

government agency (as defined in the **ARA**):

> "(a) any board, commission, association, agency, or similar body, whether incorporated or unincorporated, all the members of which, or all the members of the board of management or board of directors or governing board of which, are appointed by an Act of the Legislature or by the Lieutenant Governor in Council, and
>
> (b) any other body designated as a government agency in the regulations."

government body (as defined in the **ARA**):

> "(a) a **department**,
>
> (b) a **government agency**,
>
> (c) the Executive Council Office, and
>
> (d) the office of a minister."

government record (as defined in the **ARA**): "a record created or received by, or for, a government body in carrying out its activities." This definition emphasizes the purpose, rather than the physical form or medium of records. The definition includes traditional paper records and records in all other forms, including electronic. Government records are primary sources. They include unpublished documentation in any format, typically maintained in organized filing or other recordkeeping systems in government offices. Published books, library materials and artifacts are not government records.

Government Records Office (GRO) – a unit of the **Archives,** the GRO is the central agency responsible for promoting good recordkeeping in government. The GRO provides expert advice and support to government departments and agencies on recordkeeping best practices, requirements, issues and challenges including electronic recordkeeping, records scheduling, and a variety of program specific recordkeeping needs.

metadata for records – "structured or semi-structured information, which enables the creation, management, and use of records through time and within and across domains." [ISO 23081-2:2007, 3.7]

migration – "process of moving records from one hardware or software configuration to another without changing the format." [ISO 30300:2011, 3.3.8]

record (as defined in the **ARA**): "a record of information in any form, including electronic form, but does not include a mechanism or system for generating, sending, receiving, storing or otherwise processing information." Records are made up of information, but they are something more than information alone. Records are the product of activities - they are created or received in the normal course of business and deliberately captured and 'fixed'. They are defined in terms of their essential purpose and value - which is to provide needed **evidence** of actions and events.

record of archival value (as defined in the **ARA**): "a record of lasting significance to the government or society, such as a record:

(a) relating to the legal basis, origin, development, organization or activities of the government or its institutions,

(b) relating to the development or implementation of policies of the government,

(c) relating to the history of Manitoba, or

(d) having historical value."

These records are identified by the **Archives** when records are scheduled, and the **records schedule** authorizes their permanent preservation.

recordkeeping – refers to the entire range of functions involved in creating and managing records throughout their life cycle. It includes:

- creating / capturing adequate records
- maintaining them in trustworthy recordkeeping systems for defined retention periods
- enabling retrieval for use
- controlling access according to defined rules
- disposing of records that are no longer needed, according to formal retention and disposition rules
- maintaining and providing information about records holdings
- documenting recordkeeping practices and actions.

In this framework, the term **recordkeeping** is used interchangeably with the terms **records management** and **records and information management** (**RIM**).

records and information - in everyday language 'information' is often used to mean 'record'. The words can be used interchangeably. But 'information' can also refer to discrete pieces of information, or data, which are not the same thing as a record. Since records are made up of information, the quality of the information is also important. Managing information as records provides government with valuable evidence that can be used and re-used, protected, kept for as long as required and disposed of when no longer needed.

records and information management (RIM) - in this framework, the term is used interchangeably with the terms **records management** and **recordkeeping**.

records management - the systematic control of the creation, receipt, retention, use and disposition of records. It includes policies, practices and systems used for the management of records in an organization. In this framework, the term is used interchangeably with the terms **recordkeeping** and **records and information management (RIM)**.

records schedule (as defined in the **ARA**): "a formal plan that identifies government records, establishes their retention periods and provides for their disposition."

records system - system which captures, manages and provides access to records through time. A system may be manual or automated and includes the processes, procedures and business rules required to operate it.

retention period – the minimum time that records must be retained prior to **disposition**, as set out in a **records schedule**.

RIM – see **records and information management**.

schema – "logical plan showing the relationships between **metadata** elements, normally through establishing rules for the use and management of metadata specifically as regards the semantics, the syntax and the optionality (obligation level) of values." [ISO 23081-1:2006, 3.3]

transaction – "smallest unit of a **work process** consisting of an exchange between two or more participants or systems." [ISO/TR 26122:2012, 3.5]

work process – "one or more sequences of actions required to produce an outcome that complies with governing rules." [ISO/TR 26122:2012, 3.6]