Government of Jamaica
RECORDS AND INFORMATION MANAGEMENT
PROCEDURES MANUAL

Prepared
by:
The Ministry of
Education,
Youth and
Information

July 2018

Technical Support provided by the Public Sector Transformation and Modernisation Programme, Office of the Cabinet.

TABLE OF CONTENTS

ANNEXURES

CHAPTER 1 BACKGROUND AND INTRODUCTION

1.1 Structure of the Procedures Manual

This Procedures Manual has been prepared to give broad guidance to Ministries, Departments and Agencies (MDAs) on the management of their records and information. For most of the RIM processes, the manual provides the broad principles to be followed. However, for key aspects of RIM such as classification, storage systems, records appraisal and RIM ICT systems, more detailed guidance is provided to ensure uniformity of practice across the GoJ. Detailed procedures are also given in those cases where the MDAs interface with the Jamaica Archives and Records Department.

MDAs are required to prepare their own institution specific RIM Procedures Manuals which must, however, be in alignment with this manual. While MDAs share many common practices, the circumstances of one MDA may differ from those of the next. As an example, while one MDA may need procedures to regulate the handling of mail from the post office, another MDA, under a shared services arrangement may not have direct interface with the post office as this is done for it by the other MDA. Equally, many instructions will be determined by several other varied factors such as the size of the institution, the location of the Documentation Centre/Registry, the location of the operational units, the established organisational norms and practices, the preferences of the decision makers etc. etc

The extract below, from the Filing Operations Manual of the Ministry of Labour and Social Security[1] shows some of the institution specific practices that each MDA will need to embed in their own MDA Manual. In respect of retrieving files in the Documentation Centre, the manual directs as follows:

> *Remove the file from the filing rack, cabinet or cupboard.*
>
> *Remove the Charge-Out card from the file.*
>
> *Using blue or black ink pen, write the name of the requesting officer and the date in the next available space in the appropriate area or file ladder on the front of the file jacket.*
>
> *Using blue or black ink, write the date.......*

To cater for these institutional differences, therefore, this manual is not totally prescriptive but spells out the broad areas that must be covered by the institutional RIM Policy as well as the minimum standards that must be adhered to. It is then up to each MDA to domesticate these requirements, in line with its own particular circumstances and to prepare a manual that suits its own circumstances.

This procedures manual is supported by more detailed topic specific guidelines which are issued by JARD from time to time.

[1] Filing Operations Manual, Ministry of Labour and Social Security, June 2010, page 21

1.2 Roles and Responsibilities

The GoJ RIM Policy assigns responsibility for RIM in MDAs as follows:

Responsibility Level	RIM Policy Requirements	Implications for MDAs
Institutional Responsibility	*"The implementation of this policy within all MDAs shall rest with the Accounting Officers of the Ministry/institution concerned (i.e Permanent Secretaries or Chief Executive Officers/Managing Directors of the institutions as may be applicable), through the RIM Committee."*	All MDAs are required to constitute and activate Records Management Committees. The mandatory annual returns submitted by MDAs to JARD should also be submitted under signature of the Accounting Officers
	In each Ministry, direct responsibility shall be vested with the DDIAS, who shall also be responsible for the Departments and Agencies of the Ministry for implementation of the RIM Programme.	The proper management of records of Departments and Agencies should be a Key Result Area for the DDIAS
	In each Department and Agency, direct responsibility shall rest with the Records Manager or equivalent officer.	The PMAS of the Records Manager must reflect clear outputs and performance indicators
Responsibility and Accountability of Individuals	*All employees shall be accountable for the records which they create, use or manage and, regardless of their level, must be aware of their responsibilities to manage the records created or used by them, or those under their control or custody.*	The accountability of staff for records should be included in the contracts and key result areas of staff, at all levels
	All employees shall be responsible and accountable for maintaining adequate and complete records necessary to fully document the business functions, activities, transactions, decisions and operations.	Random audits should be conducted to ascertain that staff are maintaining complete records
	All MDA employees leaving the service of the GoJ and its Departments and Agencies shall surrender all or any record in their custody, to their immediate supervisors.	Handover/takeover procedures for records must be reflected in the administrative procedures of MDAs
Responsibility of ICT Departments/ Units	*ICT staff are responsible for ensuring that ICT systems have records management functionality and maintaining the technology including appropriate system accessibility, security and back up. ICT staff shall ensure that any actions, such as removing data from systems or folders, are undertaken in accordance with this policy. ICT and records and information management staff have joint responsibility in ensuring that records generated by ICT systems are appropriately managed.*	RIM and the ICT departments must hold quarterly meetings to review compliance of ICT to records management functionality and to discuss any ICT developments so as to ensure that records management functionality is embedded in all systems.

1.3 The Policy and Legislative Framework for RIM

The management of records and information in MDAs is guided by national and international policies and legislation on records and archives including:

a) The Government of Jamaica Records and Information Management Policy, 2016

b) The Archives Act (1982), The Archives (Official Records) Regulations, 1988 and other related legislation

c) The Access to Information Act, 2004

d) ISO 15489 and other related international standards.

It is important that MDAs familiarise with these policies and legislative instruments and that they also have a clear understanding of the role and functions of the Jamaica Archives and Records Department (JARD).

1.3.1 The Record Office Act, 1879

The Record Office Act of 1879, even though many parts have been superseded, is still in force and assigns the statutory responsibility for keeping public records to the Keeper of Public Records, a position held by the Chief Justice of Jamaica. The Registrar General is the Deputy Keeper of the Records. The Keeper of Records also chairs the Archives Advisory Committee.

1.3.2 The Archives Act, 1982

The principal legislation under which JARD operates is The Archives Act, 1982. Key provisions of the Act include the following:

4.1For the purposes of this Act there is hereby established an office to be known as the Jamaica Archives with as many branches as the Minister may deem necessary or convenient and in which should be preserved such archives as are transferred there or acquired by the Archivist under the provisions of this Act.

"official records" means all papers, documents, records, registers, printed material, maps, plans, drawings, photographs, microfilms, cinematograph films and sound recordings of any kind whatever, officially received or produced by any public organization for the conduct of its affairs or by any officer or employee of a public organization in the course of his official duties.

*"public organization" means any **ministry,** department, commission, committee, board, corporation, agency or other **organization** of the Government*

The responsibilities of the Archivist are stated as follows:

6.-(1) There should be an Archivist for the purposes of this Act, who should be a public officer.

(2) The Archivist should be responsible for-

(a) the custody, preservation, arrangement, repair and rehabilitation of archives;

(b) such duplication and reproduction of archives as may be necessary or appropriate; and

(c) the preparation and publication of inventories, indexes, catalogues and other finding-aides or guides facilitating the use of archives.

The Archives Act is the principal pillar on which JARD derives its mandate and authority. The Act provides for an Archives Advisory Committee consisting of the following:

1.(1) The Archives Advisory Committee should consist of the following members-

(a) the Keeper of the Records;

(b) the Deputy Keeper of the Records:

(c) the Registrar of the Supreme Court.

(d) the Registrar of Titles;

(e) the Archivist, who should be secretary:

(v) the Chief Architect in the Ministry of Construction (Works):

(g) not more than ten members (hereinafter referred to as Appointed members) appointed by the Minister, including one representative from each of the following:-

(i) the Ministry responsible for the Public Service:
(ii) the Institute of Jamaica;
(iii) the University of the West Indies;
(iv) the Jamaica Historical MDA;
(v) the National Council on Libraries, Archives and Documentation Services.

A sub-committee of the Archives Advisory Committee receives and reviews records retention/disposal schedules that are submitted by the MDAs. The recommendations of the sub-committee are submitted to the Archives Advisory Committee for its review and adoption.

1.3.3 The Archives (Official Records) Regulations, 1988

The Archives (Official Records) Regulations, 1988 provide guidance for the management of records in public organisations and direct as follows:

> ***3. (1)****The Records Officer, acting in accordance with the advice of the Archivist, should establish and maintain a system for the proper care and control of official records within his custody and for this purpose the Archivist may issue guidelines to be followed from time to time.*
>
> ***(2).****The system established should-*
>
> *(a) make provision for the standards, procedures and techniques to be applied for the management of official records:*
>
> *(b) promote the maintenance, storage and security of official records selected for preservation as archives until these are transferred to the Archives;*
>
> *(c) facilitate the categorisation and segregation of official records; and*
>
> *(d) provide a programme for the disposition of official records including their transfer to the Jamaica Archives, or such other place under the charge and control of the Archivist.*
>
> ***4.*** *The Records Officer should establish safeguards against the unlawful removal or loss of official records within his custody.*
>
> ***5.*** *No official record should be disposed of without the prior approval of the Committee.*(i.e the Archives Advisory Committee).

The regulations also give guidance for Records Officers (in MDAs) who need to dispose of records that are no longer needed by their organisations and also require that records inventories be conducted regularly:

> *9.-- 1 The Records Officer should prepare and keep up-to-date, under the guidance of the Archivist, an inventory of official records in his custody.*
>
> *(2) On the basis of this inventory the Records Officer should compile schedules of these records showing, in the form approved by the Archivist, their retention periods.*
>
> *(3) These schedules should be submitted to the Archivist for the approval of the Committee.*
>
> *(4) The Records Officer should compile an annual summary of official records in his custody for submission to the Archivist not later than the 31st March each year.*

In conformance with the above, the GoJ RIM Policy requires MDAs to compile and submit to JARD by the 31st of March each year, annual summaries of official records.

1.3.4 Key Related Legislation

There are a number of other legislations which impact RIM and which MDAs should be familiar with.

The Access to Information Act, 2004: The Access to Information Act, 2004, provides access to official records as follows:

> *2.The objects of this Act are to reinforce and give further effect to certain fundamental principles underlying the system of constitutional democracy, namely-*
> *(a) governmental accountability;*
> *(b) transparency; and*
> *(c) public participation in national decision-making,*
> *by granting to the public a general right of access to official documents held by public authorities, subject to exemptions which balance that right against the public interest in exempting from disclosure governmental, commercial or personal information of a sensitive nature.*
>
> *5.--(1)Subject to subsection (2), this Act applies to-*
> *(a) public authorities which are specified by the Minister by order within eighteen months after the appointed day; and*
> *(b) all other public authorities immediately after the (expiration of the period of eighteen months referred to in paragraph (a);*
> *(c) official documents created by or held by a public authority not earlier than thirty years immediately preceding the appointed day.*
> *(2) The Minister may, by order subject to negative resolution, declare that this Act shall apply to official documents created by or held by a public authority at such date, being earlier than the thirty years referred to in subsection (1) (c), as may be specified in that order.*
>
> *6.-(1) Subject to the provisions of this Act, every person shall have a right to obtain access to an official document, other than an exempt document.*
> *(2) The exemption of an official document or part thereof from disclosure shall not apply after the document has been in existence for twenty years, or such shorter or longer period as the Minister may specify by order, subject to affirmative resolution.*

The Financial Administration and Audit Act, 1959: In terms of the Financial Administration and Audit Act, 1959, the Minister may issue directions and make regulations respecting the keeping of Government accounts and other records. The Minister,

> *or any officer authorized by him shall be entitled to inspect such offices and to have such access to official books, documents and other records as may be necessary for the exercise of his functions under this Act.*

The Auditor General is authorised to act as follows:

> *(3) For the purpose of the examination of any account the Auditor-General shall be entitled at all reasonable times-*
> *(a) to have access to all books, records, vouchers, documents, returns, reports, information storage devices, cash, stamps, securities, stores or other Government property in the possession of any officer;*
> *(b) to request in writing and he given custody, for such time as he may require, of any books, accounts, vouchers or papers under the control of any officer relating to or concerning public accounts, so, however, that the Auditor-General shall give to that officer a written receipt acknowledging delivery of such accounts, vouchers or papers;*

The Electronic Transactions Act, 2007: The Electronic Transactions Act has a number of provisions that are important for records. These include the following:

> *6. For the purposes of any law, information shall not be invalid or inadmissible solely on the ground that the information-*
> *(a) is created, stored or communicated electronically; or*

> *(b) is referred to but is not contained in an electronic document, if the information being referred to is known to and accepted by the party against whom it is relied upon.*
> *7.-(1) Where any law requires, or refers to, the giving of information in writing, information that is given electronically shall be taken to be given in writing if- .*
> *(a) when the information was given, it was reasonable to expect that the information would be readily accessible to, and capable of retention for subsequent reference by, the addressee;*
> *(b) where the information is to be given to the Government and the Government requires-*
> *(i) that the information be given in a particular way in accordance with particular technology requirements; or*
> *(ii) that particular action be taken to verify the receipt of the information, the Government's requirement has been met;*

The Act also deals with the admissibility of electronic information as evidence.

> *12.-(1) In any legal proceedings, nothing in the rules of evidence shall apply so as to deny the admissibility in evidence of any information given electronically*
> *(a) solely on the ground that the information is given electronically; or*
> *(b) if the information is the best evidence that the person adducing it could reasonably be expected to obtain, on the ground that the information is not in its original form.*
>
> *(2) In assessing the evidential weight of information given electronically, regard shall be had to-*
> *(a) the reliability of the manner in which the information was generated, stored or communicated;*
> *(b) the reliability of the manner in which the integrity of the information was maintained;*
> *(c) the manner in which the originator was identified; and*
> *(d) any other relevant factor.*

1.4 The Government of Jamaica RIM Policy

The Government of Jamaica Records and Information Management Policy (the Policy) was issued in 2016.

The Policy provides the framework for the standardized management of official records in the Government of Jamaica (GoJ) so that all activities and decisions of the GoJ are fully and accurately documented, managed and monitored in accordance with the regulatory framework and the life cycle principles of records creation, maintenance, use and disposal.

The Policy aims to:

- promote the accessibility and timely sharing of information within and across government;
- protection of confidential information;
- adherence to existing records and archives legislation;
- provision of requisite infrastructure, human and material resources, for the effective and efficient management of the records and information assets of the GoJ, and
- the acquisition and preservation of records created by non-public sector entities which have informational and historical value for the nation.

The Policy is based on and is primarily aligned to *ISO 15489-Information and documentation-Records Management.* However, it also takes into account several other related international standards including:

ISO 14721:2012-Space data and information transfer systems - Open archival information system (OAIS)-Reference model
ISO 27002:2013 -Information technology - Security techniques - Code of practice for information security management
ISO/TRI 18492-Long term preservation of electronic document - based information
ISO 9001: 2015-Quality Management System
ISO 15836: Information and documentation-the Dublin Core metadata element set

MDAs are required to acquaint themselves and be familiar with these standards.

Vision Statement: The vision statement of the RIM Policy reads as follows:

> *"An integrated, standardised and secure RIM system which facilitates access to Government information and archival material; preserves and leverages Jamaica's historical, information and cultural assets; as well as enables efficient service delivery, enhanced decision making and overall attainment of national developmental goals."*

Policy Scope: The Policy applies to employees/public officials of MDAs, (including local authorities and the judiciary) relative to the management of official records and archives held by MDAs, regardless of medium or format.

Policy Principles: The Policy is governed by the following principles:

- Accountability
- Integrity
- Protection of records
- Compliance
- Availability
- Retention and disposition
- Government-wide RIM systems
- Transparency.

Developmental issues covered by the Policy include the following:

- Policy, legislative and regulatory framework and enforcement
- Organisational structures and human resources for RIM
- Reform of JARD's institutional framework and infrastructure.

In line with ISO15489, the Policy covers the following technical aspects of RIM:

- Creation, capture and registration of records
- Classification and Indexing
- Storage and maintenance
- Security, access, use and tracking of records
- Records disposition
- Email management
- Information sharing
- ICT for RIM.

1.5 The Jamaica Archives and Records Department

As JARD is the principal player in the management of records and information in MDAs, it is necessary that MDAs also acquaint themselves with its origins and history so that they can put its role into context.

Briefly, JARD is a Department in the Office of the Prime Minister (OPM). The Department had its beginnings in the Island Secretary’s Office (ISO) established in 1659 as the administrative and record keeping arm of the Colonial Government. As a Government Department, the Jamaica Archives began in 1955 with the establishment of an Archives Section in the Island Records Office and the appointment of a Government Archivist.

JARD remained a part of the Island Records Office until 1982 when it became a Department in its own right following the passage of the Archives Act, 1982. Headed by the Government Archivist, JARD operates from three locations – the Archives Unit in Spanish Town, the Audiovisual Unit at Halfway Tree and the Government Records Centre in downtown Kingston.

JARD serves as the main repository for the preservation of government records in paper, audiovisual and electronic formats, relating to the country's history and heritage.

As per the legislative mandates discussed earlier, JARD collects archival materials relating to Jamaica produced by government ministries, agencies and department and persons of national importance as well as churches, charities and other organisations to ensure that primary materials of cultural value to Jamaica are preserved. It provides a research and reference service to the public and disseminates information on the collections to promote interest and knowledge of the nation's history and culture.

JARD also establishes standards and procedures for the efficient and effective management of official records in public sector entities, at all stages of their life cycles. It provides consulting services and training in records and information management to government ministries and departments, and provides storage facilities for non-current government records awaiting final disposition in keeping with their retention schedules.

CHAPTER 2 ORGANISATIONAL STRUCTURES AND HUMAN RESOURCES FOR RIM

GoJ RIM Policy Requirements for MDAs: *RIM Committees shall be constituted at Ministry level, chaired by a senior member of the management team.*

The core terms of reference of the Committees shall be set out by administrative circular issued by JARD from time to time.

Each Department or Agency shall have its own RIM Committee which shall liaise with the portfolio RIM Committee.

The RIM Committees shall meet at least twice a year and shall keep minutes of the meetings. Once a year, a meeting shall be convened by the chair of the Ministry RIM Committee and shall be attended by representatives from all the Departments and Agencies in the Ministry.

It shall be mandatory for RIM staff to have formal qualifications in records and information management.

Career pathways for RIM shall be provided.

The RIM job functions, including the DDIAS positions, shall be streamlined in terms of job qualifications and pay scales.

The position of DDIAS (or its equivalent) shall be no lower than the third tier in the organisation structure.

2.1 MDA RIM Committees

All MDAs are required to constitute and activate Records and Information Management (RIM) Committees. The terms of reference of the Committees are at Annexure 1.

All MDAs are expected to follow the guidelines below in constituting their RIM Committees so that there is uniformity and standardization across the GoJ:

(a) A Senior Member of the Management Team designated by the Permanent Secretary or head of the Department/Agency to chair the committee
(b) The DDIAS/Records Manager (as the case may be) to perform the secretariat functions of the Committee.
(c) A representative of the MDA’s legal department/a legal officer
(d) A representative of the IT department
(e) An Officer to represent all the administrative departments
(f) An Officer to represent all the technical departments.

The Terms of Reference of the RIM Committees include the following:

- Support the Director, Documentation, Information and Access Services (DDIAS) in the development of internal RIM Policies and RIM procedural manuals (to include the treatment of e-RIM and audio visual records) and submit to the Permanent Secretary/Head of Department for approval;

- Support the DDIAS in the development of retention and disposal schedules and submit to the Permanent Secretary for approval;
- Support the DDIAS in the development of internal classification protocols which are compatible with the established GoJ classification scheme as existing from time to time;
- Provide advice, as needed, with respect to the provision of access to official records to the public in accordance with the Access to Information (ATI) Act, 2002 and any other law;
- Provide advice on the roles and responsibilities to be ascribed various categories of staff;
- Oversight of MDA's compliance with GoJ and internal RIM policy and procedural manuals; and
- Serve as a point of contact for JARD on RIM matters, particularly, the implementation of the GoJ RIM Programme.
- Review and endorse all disposition requests prior to signoff by the Permanent Secretary/Head of Department and submission to the Archives Advisory Committee for approval.
- Review the Ministry's Portfolio entities RIM Quarterly Reports and provide comments to the Permanent Secretary on the status of RIM within the Ministry's Portfolio

The Ministry RIM Committee, over and above its responsibility for the records of the Ministry, also has a duty to liaise with the RIM Committees of the Departments and Agencies under the Ministry and, as required by the RIM Policy, at least once a year, to organise a meeting to be attended by representatives from all the portfolio Departments and Agencies in the Ministry.

JARD will periodically mount training programmes for the RIM Committees, including induction workshops for staff newly assigned to the responsibility.

2.2 Staffing: Standardised Job Classification and Play Scales

The implementation of the GoJ RIM Policy requires adequate human resources to be able to discharge the mandated responsibilities adequately. As stated by the RIM Policy, it will be mandatory for RIM staff to have RIM qualifications and, at the point of introduction of the Policy, staff not having the requisite qualifications will be given a period of time to acquire these qualifications.

The Strategic Human Resource Management Division (SHRMD) of the GoJ will periodically carry out reviews of the human resources available for the RIM function in the GoJ and will make provision for career structures and pathways that cater for the RIM profession in Jamaica. The capacity audits will enable MDAs to plan for the resources required to support the RIM function.

As mandated by the GoJ RIM Policy, the positions of DDIAS in MDAs shall be no lower than the third tier.

2.3 MDA Staff Skills for e-RIM

The role assigned to the Documentation Centres/Registries with respect to ICT requires that they ensure that the staff at their disposal is able to support the RIM ICT requirements that ensure that ICT systems in the MDA have records management functionality. The staff should also be able to periodically conduct RIM ICT Maturity Level Assessments, to be involved in the development of ICT systems and in their procurement, to be able to advise the MDA staff on the management of their electronic records.

The GoJ RIM Policy recognises several categories of skills required to run an optimal RIM enterprise. For MDAs there are two critical categories required for (a) the registry and (b) the records centre or records storeroom as the case may be. Figure 1 below tabulates the supporting skills required for each category and highlights those in blue as new skills required for e-RIM environments.

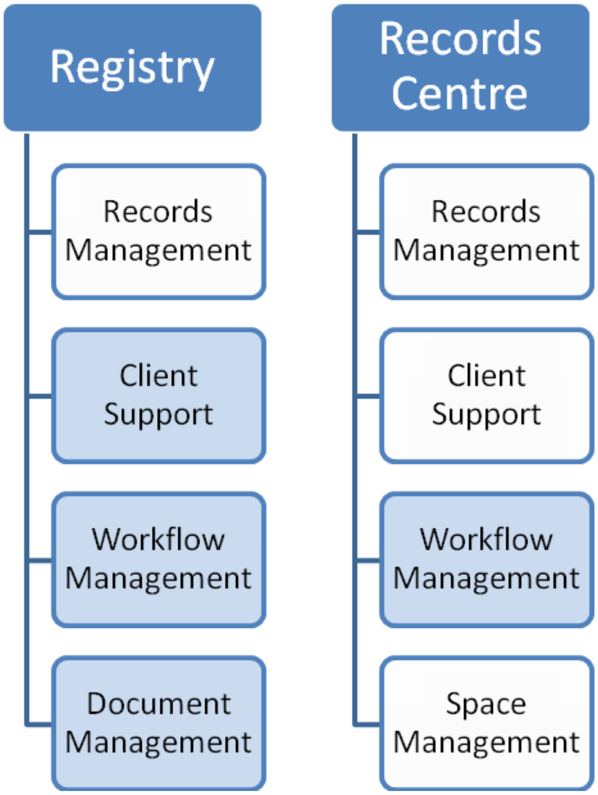


Figure 1: e-RIM Skills Matrix

MDAs are required to ensure that their staff have acquired these critical skills.

CHAPTER 3 CREATION, CAPTURE AND REGISTRATION OF RECORDS

GoJ RIM Policy Requirements: *All records created or received in the normal course of business by any Government Institution or employee shall be the property of the GoJ and shall be captured and registered into a recordkeeping system. This shall include electronic and audio-visual records.*

3.1 Mail Handling

- The Documentation Centre/Registry is accountable for all paper mail received or sent out by the MDA.
- All mail, including hand deliveries, should be received or dispatched through the Documentation Centre/Registry.
- All incoming mail should be opened, date stamped and registered in the Documentation Centre/Registry before it is sent,(filed or unfiled), to the addressees.
- Only mail classified “secret” or “top secret” is exempt from this requirement
- Security classified mail, including other categories such as “confidential”, is personally handled by the DDIAS/Records Manager.
- In MDAs with ECMs, the mail is date stamped, registered, scanned into the workflow and electronically forwarded to the addressees, with the original filed in the Documentation Centre/Registry.
- Minimum details to be registered include the following:
    - Date received
    - Name and organisation of sender
    - Date of communication
    - Subject of communication
    - Addressee
- Electronically received mail shall be dealt with under the Capstone approach where emails of designated accounts shall, after weeding of peripheral information, be preserved in totality
- Staff with non-designated email accounts shall be required to identify emails that have record value and preserve them in accordance with the Retention Schedule of the MDA.
- All outgoing mail shall be routed through the Documentation Centre/Registry where it shall be registered before dispatch

3.2 Creation of Electronic Records

RIM Policy Requirements: *Officers shall be required to work on the network drives and save the information either in the shared folders or individual folders on the network as determined by MDA’s e-RIM policies and procedural manuals.*

Document naming conventions shall be used for electronic records as per the guidelines that will be issued by JARD from time to time.

3.2.1 Network Drives

MDAs shall ensure that ICT systems have capacity to allow staff to work on their network drives rather than on their "C" drives.

Documentation Centre/Registry staff shall periodically examine computers to ensure that "records" are being saved into the network drives.

3.2.2 Document Naming Conventions

Document naming conventions should be adopted and used by MDAs so that staff, when naming electronic documents:

(a) Give document names that are brief, descriptive and as unique as possible
(b) Give document names that are consistent, simple, understandable and meaningful.
(c) Give names which are meaningful name and which closely reflect the document's contents.
(d) Express elements of the document name in a structured and predictable manner.
(e) Give similarly structured and worded names to documents which are linked.
(f) Avoid the use of generic names which are only meaningful in a personal context.
(g) Avoid the use of non-standard abbreviations and words that add no value.

The following guidelines are also useful regarding document naming conventions:

Naming Attribute	Advice
Abbreviations	Abbreviations, if at all used in naming documents, should be those that all staff are familiar with e.g. MDA
Dating	If dates are used as part of the document name, then year, month, day format should be used so that the documents will sort in chronological order: <yyyy-mm-dd>
Jargon and Slang	Jargon, nicknames and slang should be avoided.
Key Words	Document names should use keywords and avoid additional secondary words like "and", "if", "or" etc. This is because such words do not add value to the name and clog the storage space. If a must, use a dash (-) or underscore (_). Do not begin document names with "The", "a" or "an"
Letter Case and Font size	When naming documents, avoid all upper or all lower case. For example: " Salary Advance" is easier to read than "SALARY ADVANCE"
Punctuation & Special Characters	Punctuations and special characters like *, @, #, should not be used when naming documents because they affect the ability to search for and retrieve documents.
Use of Space	Place only one space between words to enable faster retrieval of the documents

3.2.3 Metadata

Metadata contains the document's particular characteristics which distinguish it as a unique object from other documents as well as information relating to the content, structure and context of the document as a record.

The Dublin Core Metadata Element Set should be used by MDAs to select data elements which should be included in document descriptions so that, for each document, minimum metadata can be recorded. The metadata element set comprises a set of 15 elements such as author/creator, access rights, dates of creation/amendment, document type, format, history, language etc. It is up to each institution to decide which minimum elements to capture so that the metadata is automatically captured as electronic records are created.

The Documentation Centre/Registry should build the capacity of users to adopt uniform nomenclatures for controlling metadata vocabulary so that there is consistency across the organization in the way metadata is recorded in order to facilitate the retrieval of documents.

3.2.4 Version Control

While electronic systems and especially ECMs have their own in-built version identification and control systems which provide an audit trail it is not always apparent how many versions were created or which is the latest or most authoritative version. Those handling paper copies of the document may also not be sure which version they are dealing with if the version identifier has not been indicated on the document (e.g. as a footnote or on the cover pages).

It is recommended that, over and above the electronic system version controls, MDAs also implement manual version controls for certain documents and processes to reduce the risks of people working from and updating wrong versions of documents or sending out wrong versions.

Each MDA should decide on the additional version control information that must be recorded for specified categories of documents such as reports and manuals.

3.2.5 Capture of Records

For paper records, documents are "captured" as records at the point at which they are put into a file, where, thereafter, they become accountable assets which can only be disposed of in accordance with the applicable retention schedules

In the electronic environment, it is more difficult to regulate the capture of records and thus it very important to be clear about the transition from a "document" to a "record"

- During the time in which a document is a "work item", it is treated as a "document", capable of being changed, commented and collaborated on.

- The document becomes a "record" when it is either (a) communicated to others or (b) used for decision making, at which point the document becomes a "record" which can no longer be changed or tampered with but must be maintained as evidence of the particular transaction, preferably in an edit locked format such as PDF.

- It is important to recognize this critical point at which a "document" is captured as a "record" and that, once designated as a record, the document no longer belongs to the creator but to the organisation, and becomes a part of the corporate information assets which can only be deleted or disposed of as per the MDA's records retention and disposal schedules.

- The capture of the document and change of status into a record is necessary in order to safeguard the authenticity of the record and the degree to which the record can be used for legal and accountability purposes.

- Should further work be required, new and related versions should be created by making and editing a copy and saving the latter as a new document.

3.2.5 Handling of Non-Records

JARD has issued a circular Ref # JARD/2015/01 regarding the treatment of non-records.

MDAs should follow the guidelines contained in the circular and ensure that non-records are not mixed with the records.

3.2.6 Filing

There are certain minimum standards that should be observed regarding filing.

(a) Minute sheets should be attached to the inside of the front cover to record items added to the file.

(b) To enhance document security, documents in files should be given a folio number which is a running sequence of numbers, starting at number one in each file, given as each item is placed on the file. The folio numbers help to secure the communications against unauthorised removal.

(c) There should be a system for recording and tracking files on issue.

CHAPTER 4 CLASSIFICATION

GoJ RIM Policy Requirements: *All MDAs shall adopt and use the GoJ Function Based Classification Scheme based on the classification of the business activities of the entity. However, for purposes of uniformity, all MDAs will be required to start with the common types of functions before the institution specific functions.*

The classification schemes shall be used to develop institutional Master File Classification Schemes which shall apply to both paper and electronic records.

The Master File Classification Schemes shall be prepared at records series and sub-series levels and shall mirror the main functions and sub-functions of the organization

4.1 Function Based Classification

The File Classification System for the GoJ is **function based** and supports classification grounded in analysis of an organisation's business activities and processes. It is built around the functions which the GoJ MDAs are mandated to execute and thus mirrors the records that each institution generates as a result of carrying out these functions. The adoption of the function based classification is in line with the international standard ISO 15498: Records Management which stipulates thus: *"Classification systems reflect the business of the organization from which they derive and are normally based on an analysis of the organization's business activities".*

The function based classification system adopted by the GoJ combines the methodologies pioneered by the Australian Standard for Records Management, AS ISO 15489 (through the DIRKS[2] methodology) and the Business Activity Structure Classification System (BASCS) developed by the Library and Archives of Canada. Classification by functions is based on the *context* of a record's creation and use, rather than on the *content* of the record itself. This means the record is classified according to why it exists i.e. its function rather than what it is about, i.e. its subject.

The classification of business functions recognises three classification levels as follows:
Level 1: Functions
Level 2: Activities (or sub-functions under BASCS)
Level 3: Transactions

The first two levels are used to constitute the ***File Classification Scheme*** for the organization and are controlled levels which must be uniform throughout the organization and which must be submitted to JARD for approval. At the first two levels, there are no records: these are headings and sub-headings of the file classification scheme.

The classification scheme is used as the framework for constructing ***File Plans*** starting at level three and reflecting the transactions of the records generated or accumulated by the entity or

[2] DIRKS - Developing and Implementing a Records Keeping System

individual officer. There is flexibility from this third level down and thus the level may still represent transactions before the records series or may actually be the records series.

4.2 Identifying MDA Functions

The first step in preparing the classification scheme is to conduct a business function analysis. The organizational chart, as well as any function schedules that may exist, is used to identify the main functions of the organization which will also constitute the first level of the file classification scheme.

The main functions of an MDA can generally be divided into two groups:

(a) Administrative/support functions (which tend to be common to all institutions)

(b) Institution specific functions.

The file classification schemes of MDAs thus comprise two sections as follows (a) the first section comprises those records which are common across all institutions while (b) the second part comprises the institution specific records. In all MDAs the first section of the File Classification Scheme will be the same.

4.2.1 Common Administrative/Support Functions

The administrative and support functions in MDAs are generally the same even if they might be organized in different combinations in each MDA or some functions may not exist independently.

The common functions found in most MDAs are as follows:

Function Description
Corporate Planning & Governance
Finance and Accounts
Administration
Human Resources Management
Property Management
Information Systems and Technology
Legal, Compliance and Regulatory

Or alternatively:

Function Description
Corporate Planning
Governance
Finance & Accounts
Properties & Buildings
Equipment
Legal, Compliance and Regulatory Affairs
Supplies
Transport
Human Resources Management

Public Relations & External Relations
Information Services
Information Systems & Technology
Security
Audit

(N.B. Decision to be made on which of the above to adopt)

These functions have been constituted into a common classification scheme that should comprise the first part of all file classification schemes in MDAs in the GoJ and that can only be changed by JARD. All MDA classification schemes must include this first part unaltered.

It should be noted that:

(a) In the actual organisational structures of each MDA, the "common" functions can either be executed individually, e.g. finance and accounts being separate functions under separate jurisdictions (departments/divisions), administered under one jurisdiction or even combined with another totally different function

(b) These common functions can also either be executed by the MDA itself or may be shared with other entities, e.g. OPM and OoC share the following services: Finance, Human Resources Management and Property Management.

The functions identified are then structured into a file classification scheme that is numeric in structure and comprises of records groups at intervals of 100. Using this process, the common functions have been constituted into the first level of the File Classification Scheme for the GoJ as shown below.

Function Level 1	Activity Level 2	Transaction Level 3	Function Description
Common Functions			
100			Corporate Planning & Governance
200			Finance and Accounts
300			Administration
400			Human Resources Management
500			Property Management
600			Information Technology
700			Legal, Compliance & Regulatory
MDA Specific Functions			
800			
900			
etc			

The above file classification structure must be used by all MDAs irrespective of how the actual organization structure of the MDA is or the portfolios under which the various functions fall. This is because the organizational structures containing the above functions can differ from one MDA to another and within the MDA, and can change from time to time. Irrespective of the organizational arrangements, the records should be arranged as per the classification schedule above and thus, for instance, all financial records found in any MDA should be under the 200 function group while human resources records should be under the 400 function group.

It should be noted that each function group is capable of accommodating up to 99 sub-functions, thus providing more than sufficient room for expansion.

4.2.2 Institution Specific Functions

Beyond the administrative/support functions, there are MDA specific functions. These are usually executed by divisions, departments, sections and units and, as can be expected, these functions generate records which differ from institution to institution. It is generally around these specific functions that the main accumulations of records as well as specialised ICT applications are to be found, e.g audit records in the Auditor General's Department.

Each MDA has specific functions which are different from the functions of other MDAs and thus creates records which are unique to it. Each MDA must thus identify its institution specific functions according to its particular mandate.

While the organisation chart is used to provide guidance in identifying the functions, the actual functions may need to be expressed differently in order to capture the actual essence of the function. The examples below illustrate how functions are identified from the organisational structures and are, as necessary, edited to reflect the function represented rather than the actual title of division/department.

Organisation Structure	Function
JARD	
Records Centre Unit	Records Management
Audio-visual Unit	Audio-visual Archives
Archives Unit	Public Archives
Office of Cabinet	
Public Sector Modernisation Division	Public Sector Modernisation
Strategic Human Resources Division	Strategic Human Resources Management
National Security Policy Coordination Unit	National Security Policy Coordination

It is thus important to note that while the functions are primarily extracted from the organization chart, they are expressed as functions and not by the given name of the operational entity or job title of the responsible officer.

It should also be noted that the "Strategic Human Resources" referred to above relate to the Office of Cabinet's institution specific responsibility for strategic human resources across the GoJ and not to the administrative management of the staff and human resources of the Office of Cabinet which are dealt with under the common functions.

The table below illustrates how the institution specific records series will differ from institution to institution.

Comparative Function Based Classification Schemes

Office of Cabinet (OoC)				ACCOUNTANT GENERAL'S DEPARTMENT (AuGD)			
Function Level 1	Sub-Function Level 2	Activities Level 3	Description	Function Level 1	Sub-Function Level 2	Activities Level 3	Description
COMMON FUNCTIONS							
100			Corporate Planning & Governance	100			Corporate Planning & Governance
200			Finance and Accounts	200			Finance and Accounts
300			Administration	300			Administration
40O			Human Resources	400			Human Resources
500			Property Management	500			Property Management
600			Information Systems & Technology	600			Information Systems & Technology
700			Legal, Compliance & Regulatory	700			Legal, Compliance & Regulatory
MDA SPECIFIC FUNCTIONS							
800			Public Sector Transformation	800			Economic Assessment
900			Public Sector Modernisation	900			Performance Audit
1000			Cabinet Support and Policy	1000			Information Technology Audit
1100			Strategic Human Resources	1100			Compliance Audit
1200			National Security Policy Coordination	1200			Financial Audit
1300			Corporate Management Development	1300			Quality Assurance

While the organization chart is used as a general guide in creating the classification scheme, and generally you identify the main functions from the higher levels of the organization, it is not necessarily always the case that the organizational levels are taken as the level one functions. Thus, for instance, in the comparative schedule above, three audit functions comprising (a) information technology audit (b) compliance audit and (c) financial audit fall under the General Assurance Audit which is under the Deputy Auditor General Assurance Audit. As will be noted however, they have been classified at the first level because they are fully fledged functions on their own similar to the Performance Audit which is organisationally placed at a higher level. With the above in mind, therefore, MDAs must use their discretion in identifying the main functions of the organization.

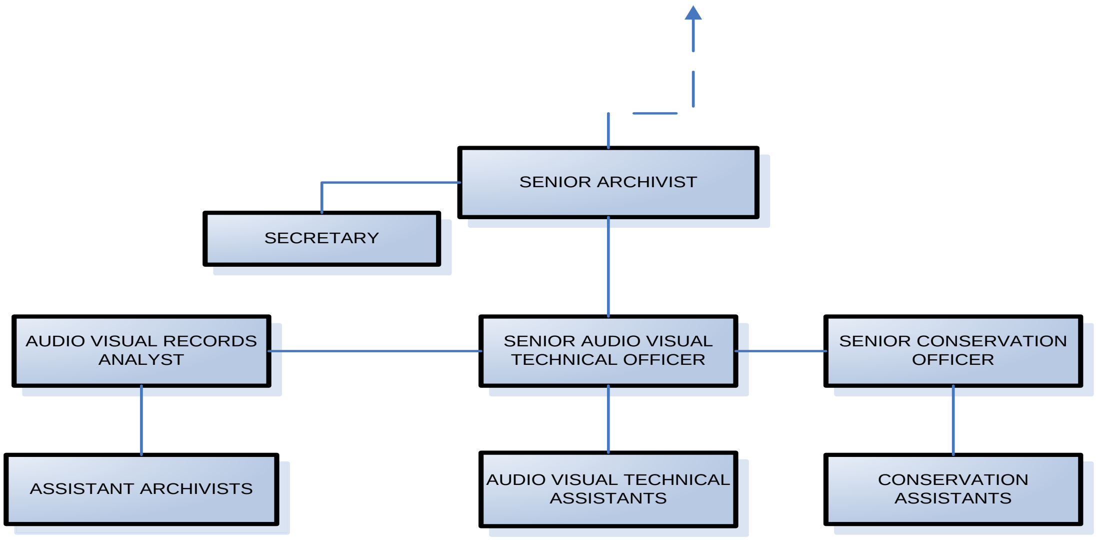
4.2.3 Activities/Sub-functions (Level 2)

The organization charts, function schedules and procedures manuals are used to help identify the activities/sub-functions under each function.

The table below illustrates how this second level may differ from MDA to MDA.

Jamaica Archives & Records Department (JARD)				ACCOUNTANT GENERAL'S DEPARTMENT (AuGD)			
Function Level 1	Sub-Function Level 2	Activities Level 3	Description	Function Level 1	Sub-Function Level 2	Activities Level 3	Description
COMMON FUNCTIONS							
100			Corporate Planning & Governance	100			Corporate Planning & Governance
					101		Corporate Planning
					102		Public Education
200			Finance and Accounts	200			Finance and Accounts
					201		Accounting
300			Administration	300			Administration
					301		Administration
					302		Telephone Operations
40O			Human Resources	400			Human Resources
					401		Human Resource Management
					402		Human Resource Development
500			Property Management	500			Property Management
	501		Facilities Management				
600			Information Systems & Technology	600			Information Systems & Technology
	601		Automated Systems Management		601		Records Management
700			Legal, Compliance & Regulatory	700			Legal, Compliance & Regulatory
					701		Internal Audit
MDA SPECIFIC FUNCTIONS							

The organization chart below, representing the Audio-visual Unit at JARD, illustrates how the organization chart can be used to identify the activities/sub-functions for the second level of the classification scheme.


SENIOR ARCHIVIST
SECRETARY
AUDIO VISUAL RECORDS ANALYST
SENIOR AUDIO VISUAL TECHNICAL OFFICER
SENIOR CONSERVATION OFFICER
ASSISTANT ARCHIVISTS
AUDIO VISUAL TECHNICAL ASSISTANTS
CONSERVATION ASSISTANTS

In the organogram above, there are three major sub-functions represented by (a) Audio visual Records Analyst (b) Senior Audio visual Technical Officer and (c) Senior Conservation Officer. These are then used to demarcate the three activities/sub-functions in audio-visual records and archives as follows:

(a) Records analysis

(b) Technical services

(c) Conservation.

The above thus constitute the second level of the classification scheme in relation to the function of audio-visual archives within the classification scheme for JARD.

As will be noted, Sub-functions do not appear in relation to the organogram and it will be necessary to consult other sources such as function schedules and procedures manuals to obtain the required information. In the above case, reviewing the procedures manuals shows that conservation includes the following activities:

(i) Preservation

(ii) Conservation

(iii) Disaster management

(iv) Digitisation.

In summary, therefore, the identification of the full range of functions and sub-functions which constitute the first two levels of the classification scheme requires the review of several sources of information including the organization charts, function schedules and procedures manuals.

4.2.4 Transactions (Level 3: Records Series)

At the first two levels there are no files. These constitute the headings and sub-headings of the classification scheme. Records and records series, sub-series and files are found from the third(transaction) level onwards. The third level represents the transactions which are conducted in relation to the activities identified at level 2 and it is, starting at this level, that records disposition decisions can be made. There is flexibility in terms of the sequencing from level 3 onwards, thus, while level 4 may represent a records sub-series, in other cases it may be the actual file. Equally, while level 5 might be a file, in other cases, it might still be a sub-heading/sub-series before the actual file which will be at the next level.

The table below illustrates how classification schemes for common records may differ from institution to institution from the second level onwards. The key issue and point of uniformity is that all records relating to administration will be found under 300 whichever MDA you go to.

Institution A					Institution B			
100	Corporate Planning & Governance				100	Corporate Planning & Governance		
200	Finance and Accounts				200	Finance and Accounts		
300	Administration				300	Administration		
	301	Transport				301	Logistics	
	302	Procurement				302	Customer Care	
		302/1	Tender Advertisements				302/1	Customer Feedback
		302/2	Tender Committee				302/2	Customer Rewards
			302/2/1	Appointment of Committee Members				
			302/2/2	Minutes of Committee Meetings				
400	Human Resources				400	Human Resources		
500	Property Management				500	Property Management		
600	Information Systems & Technology				600	Information Systems & Technology		
700	Legal, Compliance & Regulatory				700	Legal, Compliance & Regulatory		

As can be seen from the example at 302/2 above, the system allows for infinite expansion of the records series and sub-series as necessary, although it is not advisable to go beyond five levels. Note also that while in institution A, 302/1 on Tender Advertisements which is at the third level can be at file level, below that, 302/2, Tender Committee is a sub-heading with the actual files a level lower at 302/2/1 and 302/2/2.

The system is flexible and applicable to all MDAs and, within these, to all divisions, sections, units and offices in that each is able, within the framework of the broad classification scheme provided, to structure the File Plan to suit individual needs as well as complexity and quantities of records involved.

Different users will make greater use of those parts of the classification scheme where they have responsibility and thus create records under that particular function/sub-function. For instance, while the corporate services of JARD are handled at OPM, and therefore the main human resources records are resident at OPM, nevertheless JARD will still have its own limited human resources records including its own copies of personal files. As with OPM as well as all other MDAs, these records will be filed under records series 400. The difference will be that while at OPM the 400 level will be very extensive and expansive with many series and sub-sub-series, at JARD, it will be just a few series with a small number of files. But both will be classified under the same records function.

4.3 File Plans

The File Classification Scheme is used as the basis for creating File Plans. The File Plans are constructed starting at level three of the File Classification Scheme and comprise the actual transactions/records series and files held under the File Classification Scheme. The number of

File Plans in an MDA depends on the extent to which the RIM system is centralized or decentralized.

The primary File Plans will be found in the Documentation Centre/Registry. Other File Plans will then be found in sub-registries which may exist and in offices. All officers who generate records, whether in paper form or electronically are required to develop their own File Plans for the records held by them..

Electronically, shared drives should have their own File Plans depending on the function served by the users of that shared drive. Electronic records (with the exception of data bases and specialized/function specific software applications) should be filed under File Plans that are aligned to the File Classification Scheme of the MDA.

4.4 Institutional Identity

As all MDAs use the common numeric file classification scheme there can be difficulties in determining the origin of communications received from other MDAs. To overcome this problem MDAs, when communicating with other external entities, should affix an institutional identifier to the records classification.

Thus, all files begin with the truncation of the institution’s name followed by the file reference number. If we take as an example a file in JARD numbered 202/2/1, the file reference will now be JARD/102/3/2/1 thereby distinguishing it from a file in OPM of the same number which will be referenced as OPM/102/3/2/1.

Please note that it is advisable to use the institutional identifier only when recording the reference number or when sending out mail and other communications to other institutions. In the system itself, the classification system is better identified numerically without the institutional identifier. This is not only to make it easier for users, but, when adding new files or sub-files, the computer will also be able to sort the files in numerical sequence.

4.5 Approval of File Classification Scheme

All MDAs must undertake the above activity and establish the first two levels of the classification scheme. This file classification scheme, accompanied by the organization charts and function schedules shall be submitted to JARD for approval. Thereafter, changes to the scheme have to be advised to JARD for approval before implementation.

4.6 Security Classification

The security classifications of records under which various permissions and restrictions of access are regulated sit on top of the records classification procedures mentioned above and are considerably facilitated by the latter classification system as access controls, permissions and restrictions, can be built around the records series and sub-series as classified.

4.7 Classification of Case Files

Case files are those files which are similar in content but differ in that they relate to different cases, items, people etc. They include personal files, stand files, patient files and student files. Case files usually have their own numbering system and there is flexibility on whether they should be included in the above filing system or cross-referenced and filed outside this system. Thus, for instance, personal files can be arranged alphabetically or numerically by employee number, the latter which might be system generated within the human resources management system.

Several categories of financial and other records also do not need to be included in the file classification schemes. These include serially numbered types of records such as purchase order books, invoice books, or other papers which are self identifying or are batched together for processing. It is not practical that such records be given reference numbers under the filing scheme.

4.8 Classification of Electronic Records

4.8.1 File Classification Scheme and Directory/Folder Structure

While modern computerised systems and databases are capable of retrieving information randomly through powerful search engines, it is often difficult to re-call all items related to a particular activity or transaction so as to thread together the context of the issue. Electronic records should thus also be organised as per the File Classification Scheme to facilitate retrieval and so that there is alignment between the paper and electronic records.

Where there is no automated records management system such as an Enterprise Content Management (ECM) system, the directory/folder structure should be used as the basis of the electronic File Classification Scheme.

The advantages of using the File Classification Scheme in filing electronic documents include:

- Ensuring a complete recall of all records which relate to a particular activity or topic.
- Ensuring that records are presented in an order which shows the narrative development of the activity to which they relate.
- Providing an opportunity for aligning the electronic filing system with the paper filing system.
- Enabling electronic records to be appraised together in context and to be systematically and consistently scheduled and disposed of, so that associated records are retained for the same length of time and are destroyed or transferred together.
- Presenting a familiar face to the user, when filing or retrieving records, through a File Classification Scheme and a File Plan which reflects the organisational or business functions and which can easily be understood and navigated.

4.8.2 Setting up the Electronic Classification Scheme and File Plan

The File Plans should be based on the directory/folder structure and should be as per the approved File Classification Scheme of the institution. The Documentation Centre/Registry staff will assist officers to create their electronic File Plans, using the directory/folder system.

Each new document created should be saved into its appropriate directory/folder of the File Plan so that all documents on the same subject are kept together.

4.8.3 Electronic Filing Guidelines for Networked Systems without ECMs

For offices which are linked to a network but do not have an ECM, the File Classification Schemes should be set up on the central server in order to create shared drives that can be used and shared by network users and accessed according to agreed access rules and restrictions.

Those connected to the network should observe the following rules when creating and saving documents:

- No official documents or records should be saved on the hard disks of the computers of the individual officers without being copied onto the network folders (individual or shared drive). As necessary, personal folders should be set up on the network (and within ECM if existent) to cater for individual needs.
- As a rule, network users should log on to the network and create documents which are saved directly in their personal folders on the central server. The system administrators should make arrangements to have the files password protected according to levels of access.
- Documents identified as being of record value should be captured into the records management system by being saved into the personal or shared drives as "read only" versions which are thus “write” protected. This will ensure that other network users do not access the documents and alter or update them.
- As it is critical for information sharing and back up security that official information be handled within the central servers and that RIM staff should, from time to time, check the hard drives of officers to ensure that no official documents are being kept outside the central server without also being saved in the network. Officials found violating this should be subject to disciplinary procedures.

4.8.4 Electronic Filing Guidelines for Institutions with ECMs

- All documents created within the ECM should be classified and filed as per the institutional File Classification Scheme.
- All users who receive or generate documents in the ECM must have their own File Plans based on the institutional File Classification Scheme.
- The File Plans of each institution and each office that keeps its own records should reflect the actual electronic and paper files created and maintained by that institution/office.
- Both documents and records are classified and filed into the ECM as per the File Classification Scheme.

- During the time in which a document is a “work item” in the workflow, it is treated as a “document”, capable of being changed, commented and collaborated on.

- The document becomes a “record” when the “archive” functionality of ECM is activated at which point the document becomes a “record” which can no longer be changed or tampered with but must be maintained as evidence of the particular transaction.

4.9 General Guidance on Function Based Filing

4.9.1 Identifying the Function

In determining the appropriate file series and sub-series, and in order to decide where to save a particular document, you should consider the following questions:

What function does it relate to? Is it finance and accounts, human resources management or information systems and technology? As is evident, one will be asking which of the main functions, activities and records series the document relates to.

Having identified the records series, one then asks which of the sub-series it fits into. In other words, you begin at the broadest level and keep narrowing down until you have identified the correct sub-series and the actual file.

Ensure that, as much as possible, ***filing by source*** is eliminated**.** Filing by source means filing a communication according to where it is coming from. The examples below illustrate this:

- JARD Correspondence
- Kingston Municipal Council
- Jamaica Revenue Authority
- Letters from Cabinet Office.

Filing by source creates problems. As an example, if one is filing by source, a letter from the Cabinet Office will be filed in a file titled " Cabinet Office Correspondence" and literally everything from the Cabinet Office will be expected to be filed there.

The problem with this is that there can now be ***Multi-Destination*** for this letter if there are also other relevant activity/transaction based files. In relation to the communication from Cabinet Office, if the communication is about public sector transformation and modernisation, and there is already a file on this, the communication can then be filed either file. ***Multi destination results in multi retrieval*** possibilities which make retrieval more difficult. The aim thus, as far as is possible, is to eliminate filing by source.

4.9.2 Filing by Format or Type of Communication

As a general rule, files titled according to their format or type should not be created. The files listed below should not be created or used:

- Incoming Correspondence

- Outgoing Correspondence
- Faxes In
- Faxes Out
- E-mail Messages

The problem with these files is that any item that comes in relates to some function, activity or transaction. If again, the communication mentioned above has been faxed, where should it now be filed, in the file on "Faxes In" or in the " subject " file. The response from Cabinet Office may well be in the form of an e-mail or letter and there would be difficulties in deciding where to file this response.

There are certain types of communications that create problems. These include reports, returns and statistics. The guiding rule is that they should be filed under the activity or transaction to which they relate. Filing them separately can result in incompleteness of records as users consult only those records which are in the particular records series without realising that there are related reports and other documents filed separately elsewhere.

4.9.3 File Titling

File titles which are too broad, have no meaning or are misleading, such as the examples below, should be avoided:

- General
- Miscellaneous
- Various Correspondences
- Office General
- Sundry Correspondence
- Supervisor's File
- Administration Documents
- Various Reports.

Do not have too many subjects in one file and avoid long file titles such as the examples below:

- Meetings, Workshops, Seminars, Conferences and Visits by Overseas Technicians and Consultants.
- Motor Vehicle Maintenance, Fuel, Repairs, Insurance and Accidents.

4.9.4 Filing of Periodicals

Periodicals i.e. magazines, bulletins, newsletters and other materials printed and published at regular intervals should not be put into the filing system.

4.9.5 Filing of Audio Visual Records

Audio visual records need special treatment and separate storage. The main requirement is that their existence and storage location should be recorded somewhere so that they are retrievable. If many such items are found in a Department, an Audio Visual Register should be created and maintained.

Such items include:

- Photographs

- Films
- Videos and sound recordings.

4.9.6 Daily Filing

Please note that daily filing is a strict requirement of these procedures. There should be no accumulations of un-filed papers in the in-trays, whether in the Documentation Centres/Registries or in the offices. Departments and offices that are allowed to accumulate and keep their own records must also be prepared to accept the obligation to abide by this rule.

CHAPTER 5 INDEXING SYSTEM

GoJ RIM Policy Requirement: *Records shall be indexed as per the guidelines provided in the RIM Procedures Manual of the GoJ and the MDA*.

5.1 Scope of the Indexing System

Indexing systems are not new to MDAs and many of them still have and use large and heavy index books dating back to when the MDAs were established. While powerful search engines now make it infinitely easier to retrieve information, manual indexing still has a role to play especially in those MDAs that have not yet automated their RIM systems or have limited ICT applications.

The main objective of the indexing system is to provide a tool that will facilitate the identification and retrieval of records and information required for the execution of the MDA's business, wherever that information may be held within the MDA.

The indexing system must be designed in a way that makes it possible to index the files and records in both the formalised and structured registry system as well as the files and records in the subsidiary, formal and informal filing systems as may be found in other units and offices.

The indexing system is meant to facilitate the retrieval of information. The purpose of creating records is not only to document the activities of the organisation but to provide a body of information which can be used by the organisation for the carrying out of its duties and functions. Organising information without a means of retrieving the information serves no purpose. One of the mechanisms that facilitates the retrieval of this information is the index which can be described as a pointer, indicator or systematic guide to the items or information contained in a filing system or database.

The structure of the indexing system must be such as to facilitate the retrieval of information. Different people wishing to retrieve information will have different reasons for retrieving the information and are likely to approach the retrieval process differently. There is also the likelihood that they will specify their requirements differently. While some of the users will know what they are looking for, others will have only vague notions of what information sources are most useful to meet their needs. The indexing system must be designed so that it is able to support both types of users.

The indexing system should, as a minimum, cover various categories of records:

- Files contained in both the formal registries as well as the subsidiary systems
- Files in the records storerooms
- Registers
- Case files, e.g. personal files.

5.2 Indexes to the File Lists

As most MDAs have multiple records sites, a major instrument for the identification and retrieval of information in the MDA will be a consolidated file index that will also include records held outside the Documentation Centre/Registry.

For MDAs that do not have ECMs, there are two ways in which the indexing can be done.

Excel Spreadsheets: Excel spreadsheets can be used to enter the titles of the files, registers and other records contained in the MDA. The consolidated lists compiled will then enable searches to be conducted on the spreadsheets and sorting to be done by various criteria.

Keyword Indexing: A significant number of MDAs still have index books created in days gone by. Some MDAs may prefer to continue with usage of this manual indexing system which has its own advantage. For those wishing to continue with the manual indexing system, the guidance below can be followed using the keyword indexing system.

The keyword indexing system involves the indexing of the file titles and descriptors of the documents or records, and gives information on the whereabouts of the information being sought, leading the searcher to the required file. The system is developed on the premise that file and record titles, and specifically the words in the titles, convey the subject content of the document to which the title pertains.

The keyword indexing system that can be used is a simplified version of indexing systems which are commonly used by librarians to index information on book titles. Keywords comprise those words within a file title or records descriptor that can be used by someone seeking information on a particular issue or subject.

Each word that could be used by a searcher seeking information becomes a keyword that is indexed, with an entry being created for it and linked to the file title, classification number and location. The index does not give the user the actual information contained in the files but merely directs the person to the location/owner of the file.

From an information sharing perspective, the index will make it possible for the MDA, at appropriately authorised levels, to have an overview of all the records held in the MDA.

The following example illustrates how the indexing is done.

File Reference Number	**File Title**
406.1	Training of Staff

For the above file, two index entries will be created as follows:

Index Entry 1.

TRAINING, of Staff	
File Ref. No. 406.1	Location: Registry, shelf 892

Index Entry 2.

STAFF, Training of Staff	
File Ref. No. 406.1	Location: Registry, shelf 892

Notice that on each of the entries, the title of the file is indicated. In the case of the first file, the file title was indicated by merely completing the remaining parts of the file title. On the second entry, after putting the main entry, the full file title is then repeated. In all cases, the file reference number is shown in full, so that, whichever of the entries a user consults, he/she is guided back to the same file. The location of the file is also shown. This is because, the index entries may cover the records in several offices and sections within the MDA and it is thus necessary to indicate the place where the records are physically located.

The word "of" is not indexed as it is not a keyword. What this means is that, it is not expected that a user will come and look for information under "of". It is expected that the user will think either of TRAINING or STAFF, not "OF".

The following rules should be observed in determining what should be indexed:-

Files: The file titles should be indexed. File is used here to denote various types of file covers including file folders of the manila type, lever arch files, box files and accessible files.

Registers: The name of the register constitutes the title. Examples are:-

- Incoming Mail Register
- Personal File(PF) Register
- Advances Register
- Remittances Register, etc.

The titles of the above registers are the ones that would be indexed. It is again important to draw attention to the fact that the index is an index to the register titles and not to the actual individual contents in the register. There may actually exist other indexes specific to the contents of the register.

Books: Books such as are used in certain cases should also be indexed. The books referred to here are those that are used to record information, not published books. Examples of such books are Minute Books and Delivery Books.

Other types of records: There are other types of records which do not have titles as such. These include financial records of various types and their identification is usually according to what they are. Examples include vouchers, goods received notes, requisitions, and ledgers. It is these descriptors that are indexed.

When the indexing exercise has been completed, covering all offices and records in the MDA, all the entries are input into a database using Excel spreadsheets (or, if so desired, a card catalogue with the cards arranged in the alphabetical order of the first word on each card).

The above indexing system, based on file and document titles, has the advantage that it is simple and easy to understand and can be produced relatively cheaply and quickly whether manually or through a computer. The index entries are based on the words in the title itself, thereby removing the necessity for human interpretation of the indexing terms. The language of the index therefore mirrors the terminology of the filing system itself. The integration and accumulation of the entries from different filing units is also relatively simple.

There are, however, some limitations which must be understood and appreciated. The title index is really a crude form of indexing and can demand a great deal of imagination and searching skills on the part of the users. The file titles do not always constitute an accurate summary of the contents of a file or document. The title is also a summarization at the highest aggregated level and does not represent the sub themes and other subjects represented in the file or document. The lack of control over indexing language can also be a drawback.

5.3 Indexes to Personal Files

Where there is no automated system, the following rules can be used when creating alphabetic indexes for personal files.

- A register or index cards can be used. The names are then arranged in alphabetic order within the register or the cards. It is preferred that cards be used, since registers are inflexible in arranging the names within each alphabetic section. There are also problems in that it is difficult to forecast the rate at which each of the alphabetic sections will grow and therefore to leave sufficient room for each section.

- If a register is used, each letter of the alphabet should be allocated a separate section of the register with empty pages left in between sections to provide for expansion as new employees come on board.

- Within each alphabetic section, the names are then arranged in alphabetic sequence. In arranging the names within the section, the sequence of the names is decided by the alphabetic sequence of the letters coming after the first one.

- In this way, the second letter of the surname determines the precedence of the name. Thus, James comes before Jennifer, while the latter comes before John. If the first two letters are the same, then the sequence is determined by the third letter. Where these are again similar, the fourth letter is considered and so forth until a sequence can be determined.

- If the surnames are exactly the same, then the sequence is determined by the first names or the initials. Those whose names therefore start with a, b or c would come before those whose first names begin with x, y or z. If only the initials are available, the sequence of the first initial would also be the determining factor.

The personal files index can be simple or sophisticated depending on the administrative requirements of the MDA. A remarks column is useful to record comments on the employee, such as maiden or married name, and termination of employment.

5.4 Indexes to Registers

The MDA should decide on other indexes and databases that can be created to facilitate the retrieval of information. Each register is basically amenable to indexing, the only limitation being the validity or usefulness of the resulting index. Consider the usefulness of indexes to the following registers:

- Index of Register of Incoming Correspondence
- Index of Register of Outgoing Correspondence

However, the above registers, if in electronic form, e.g. Excel spreadsheet, can facilitate search and retrieval via various sorting parameters. The following are a few examples.

- Incoming correspondence sorted by Name of Sender
- Incoming Correspondence sorted by Name of Addressee
- Outgoing Correspondence sorted by Name of Addressee.

5.5 Computerised Indexing

MDAs have traditionally relied on paper filing systems for records storage and retrieval. However, paper records are extremely difficult to manage because they have to be stored in and retrieved from only one place, which is the Registry. Electronic content management systems (ECMs) solve many of the storage and retrieval problems inherent in paper filing systems while simultaneously reducing business costs. ECMs manage storage and retrieval of many different types of digital documents, including word processing files, spreadsheets, database files, e-mail, voice mail, scanned images, and Internet/intranet HTML documents.

While ECMs provide much faster access to and retrieval of records, the mere availability of a new technology does not justify its acquisition. Effective indexing would add value to the MDA far beyond mere speed of retrieval by enabling users to retrieve records in many different ways.

In the electronic domains records are part of a hierarchy of "containers" which include Folder, Section, Document, and Page etc. A folder can have many sections, and sections can contain many documents, and documents can consist of many pages. Yet traditional paper-based filing systems at the MDAs require staff to retrieve all information at the "Folder” level of the hierarchy. By contrast, ECMs allow information to be retrieved at many levels. This retrieval is built on indexing, the bedrock of ECMs. The accurate and consistent indexing of digital records and representations is absolutely critical to the success of the MDA.

5.5.1 Types of Indexing

Indexing can be field-based, full-text, or a combination of the two. Index field data makes unique identification of documents possible. Retrieval from index fields is consistent and accurate because it is based on a controlled search vocabulary. Ideally, field indexing should be performed at the point when business documents are created. Some field indexing can be done automatically, but human indexers are also required.

5.5.2 Full-text Indexes

Computer software in ECMS reads every word of every document in a database and creates an inverted index of words and their locations in the database. End-users would then search the database using any words they want to: the computer will find every match between the search term(s) and the text of the documents. Full-text searching makes it easy to locate documents when users are not exactly sure what they need, but it also finds a high number of irrelevant items (for example, Internet search engines are based on full-text indexes). In the interest of quick and accurate retrieval, some field-based indexing is recommended. Indexing digital documents exclusively with full-text indexes is not recommended.

All MDAs should benefit from some combination of field-based and full-text indexing, but determining what particular combination is most beneficial to a given organization is not easy and is a learnt process. Before MDAs can choose an ECM to manage digital documents, the indexing needs should be weighed against the benefits and costs of indexing. Different ECMs offer different types of indexing, and the MDA should be aware of their capabilities. MDAs have different indexing needs because their documents and their users vary, careful study is required before selecting and configuring an ECM.

CHAPTER 6 USE AND TRACKING OF RECORDS

GoJ RIM Policy Requirements: *Appropriate systems shall be developed and used for the tracking of paper and electronic documents and records. This shall include both action and location tracking.*

All e-RIM systems shall provide for audit trails and/or event logs to record all actions applied on e-records within the system, the time, dates and persons responsible for the actions.

6.1 File Retrieval, Issue and Tracking

Procedures for the issuing and tracking of files are largely applicable to the Documentation Centres/Registries. While there may be other files held in other departments/sections/units/offices, in these there is rather limited movement.

Files leave the Documentation Centre/Registry for a number of reasons including:-

- Routing a communication that has been received
- In response to a request for a file/files.

6.2 Outcard System

An outcarding system should be used to control file issues, even in those cases where the issuing system is electronic. A set of outcards is kept in the registry. No file should leave the registry unless an outcard has been filled or printed and inserted in the place on the shelf /cabinet or other storage place vacated by the file. The details that should be recorded include the following:

- File reference number
- File title
- Date issued
- Person issued to
- Date returned.

The important and critical aspect is that a dummy must be left in the place vacated by the retrieved file.

6.3 File Tracking

The tracking of the movement of files from one office to the next poses major challenges to Documentation Centres and Registries.

It is advisable to deploy electronic systems for the tracking of files and ECM systems, for instance, have document tracking and workflow management systems that do this well.

However, in the absence of automated tracking systems, it may be necessary to use manual and semi-automated tracking systems to control this process.

Electronically, the passing on of files from one office to another may be notified to the Documentation Centre/Registry by e-mail or through the Intranet. Where such facilities are not available, officers may be issued with pads of file pass-on slips. When an officer wishes to send a file to another officer without the file going back to registry, then the file pass-on-slips are used.

The slip is completed and given to the messenger to take back to registry which then amends the outcard as necessary.

However, manual/semi-automated tracking systems often face many challenges because the officers involved are too busy to attend to this “small” detail of sending an e-mail notification or filling and returning the slip to the Documentation Centre/Registry when they pass on the file.

If there is resistance to the use of file pass-on slips, then the alternative is to insist that files be moved from office to office by messenger. The files are then routed to the designated officer via the registry for update of the issue details. The messenger can also be given a register or forms to complete and return to registry for update of issue details.

6.4 File Bring-Up System

Officers to whom files have been issued may not be able to deal with the issue quickly. On the other hand they may want to hang on to the file to remind themselves to deal with the issue at some point.

The lengthy retention of files in offices creates problems for the registry as other communications come in and need to be filed. To encourage officers to return files to the registry if they are not dealing with the issue immediately, a File Bring Up System can be introduced.

The registry keeps a diary. An officer wishing to deal with the issue at a later date indicates this on the file and returns the file to the registry, with the date on which he/she wants the file to be brought back. The system can also be used in those cases where officers, in advance, know when they will want to have certain files and so make requests in advance.

In the registry, the file reference number and name of officer are entered into the diary and the file is sent back to the officer on the required date.

6.5 Temporary File System

There will be cases when a communication comes in and yet the file has been issued out. To ensure that such items are not held, a Temporary Files System is used. In this case, a temporary file is created and used and its details are recorded in a Temporary Files Register. The register makes it possible to control the number of such items issued out. Details recorded in the register include the following:

- Date created
- Subject
- Permanent file reference number
- Temporary file number
- Person issued to
- Date returned

CHAPTER 7 STORAGE AND MAINTENANCE

GoJ RIM Policy Requirements: *MDAs shall be provided with the buildings, office space, records storage space, shelving, RIM supplies, reprographic and conservation equipment, information communication technologies and other resources necessary for the safekeeping of the records and archives in keeping with the goals and the objectives of the RIM Programme.*

Records storage arrangements shall take into consideration the format, media, nature and use of the records, as well as migration requirements in the case of electronic and digital records.

Adequate storage space and facilities shall be provided to cater for current records in the registries and operational areas in the short term.

Each MDA shall provide appropriate storerooms and strongrooms, with appropriate shelving and other equipment for the storage and management of semi-current records.

MDAs do not, ordinarily, think of the long term needs of records and often do not pay attention to the preservation needs of records. However, apart from the fact that poor environmental conditions may render records unusable even in the short-to-medium term that they are in the MDA, a proportion of the records will have archival value and will need to survive in good condition so that they can be preserved in perpetuity when they reach JARD.

It is essential then that MDAs pay attention to the environmental conditions in which the store their records and must ensure that they provide suitable environmental conditions for the management and preservation of the records.

The guidelines below provide guidance on minimum environmental conditions that must be met. MDAs are required to elaborate them in relation to their own specific situation.

7.1 Temperature and Humidity Regulation

Very few MDAs will be able to provide environmentally controlled environments in which temperature and humidity are climatically controlled. However, they should be aware of the effect of these elements so that, as much as possible, they provide stable storage conditions that do not adversely affect the records.

Extreme temperatures and humidity (amount of moisture in air) contribute significantly to the degradation of records, both paper, audiovisual and electronic. Their effects on records are interdependent hence the need to consider them together.

High temperatures contribute to the accelerated oxidation of paper and microfilm that damages the documents while high humidity activates growth of mould on the records and archives, causes decomposition through hydrolysis, speeds formation of sulphuric, hydrochloric and other acids that destroy paper and ink, and also softens sizes and glues used for binding. A low humidity, meaning a drier environment, robs the paper of moisture which compromises the paper's flexibility and weakens inter-fibre links rendering cellulose more fragile.

A combination of high humidity and high temperatures activates spread of fungi, bacteria and insects, all of which are harmful to records and archives.

Sudden and continual fluctuations in temperature and humidity subject paper records and archives to great tensile and compressive strains that destroy the paper's structural links.

While MDAs are not expected to provide ideal environmental conditions for records, nevertheless they should seek to provide conditions that do not expose the records to these fluctuations and, if possible, should isolate records with permanent value and, from the very beginning, find sanctuary for them in separate units that are environmentally controlled.

For the generality of the records, it is often a question of ensuring that the points at which records are being stored do not expose them to extreme fluctuations and that, for instance, they are not placed in an area exposed to the sun. Equally, storage in trailer containers exposes them to extreme fluctuations as the temperatures rise rapidly during the day and go down at night.

7.2 Other Environmental Considerations

Dust: Exposure of records to dust not only compromises the cleanliness of the records but also results in their degradation. Dust provides grounds for proliferation of insects, bacteria and other pests which do not only eat up the records but also creates dirt and results in scratches to digital media thus posing readability challenges.

Constant Cleaning: Using vacuum cleaners and general wiping of shelves - should be conducted to eliminate dust in the records storerooms.

Protection from Magnetic Fields: Electronic, audiovisual and digital records (both analogue and digital) should be kept away from magnetic gadgets because this can result in disorientation of magnetic fields which damage them. Consequently, such media should not be kept close to electronic gadgets like computers, radios and should not be placed on top of each other.

Fire Protection: Electrical wiring should be professionally done and constantly inspected to ensure safety. Automatic circuit breakers should be used to allow auto-power disconnection in case of electrical mishaps.

Hand-held fire extinguishers for foam, carbon dioxide, halogenated hydrocarbons and powder should be placed at strategic places in the Documentation Centre/Registry areas.

Physical Security: Suitable arrangements for the physical security of the Documentation Centre/Registry should be put in place to safeguard the records and archives. Windows and doors should be burglar proofed. As a general rule, non-Documentation Centre/Registry staff should not be allowed inside and should be served from a counter.

Protection of Vital Records: Vital and high value records in vaults and other controlled areas should be accessed through dual controls and such access should be recorded and documented.

Pest Management: The Documentation Centres/Registries and records storerooms should be protected from rodents and insects such as cockroaches, silver fish, bookworms, beetles, booklice and termites which feed mainly on cellulose, paste, glue and wood and whose growth is encouraged by warm and humid environments, darkness and poor ventilation.

The pests should be managed through consistent fumigation of the buildings and use of uncontaminated materials in the storage and processing of records.

Cleanliness: Basic cleaning, using vacuum cleaners, fumigation and general hand cleaning should be done regularly.

Eating and Drinking: Eating or drinking in the records storerooms is not be allowed. Smoking within the Documentation Centre/Registry and records storerooms is also prohibited at all times.

Maintenance of Strong Rooms: Each MDA should have a strong room/s to store highly confidential records.

- The strong rooms should not be open access to staff and specific officers should be given responsibility for the strong rooms.
- The keys/access codes should be kept secure and access should be under strict supervision from the responsible officers.
- In addition, the records boxes should also be sealed if the degree of confidentiality is very high.

7.3 Disaster Management

- Each MDA shall have a Disaster Management Plan which shall be reviewed at regular intervals.

- Appropriate in-house and offsite backup systems should be installed to provide backup to all electronic documents within the MDA.

- Records of what is backed up and where should be maintained.

- Copies of the backup media, together with the backup record, should be stored safely in a remote location and JARD should be consulted in this regard.

- Regular tests for restoring documents from the backup copies should be undertaken, to ensure that the backups can indeed be relied upon for use in an emergency.

CHAPTER 8 RIM ICT

GoJ RIM Policy Requirements: *MDAs procuring ECM will select from designated software packages identified by e-Gov (e.g. three or four packages) for use by MDAs.*

MDAs are required to deposit all audio visual materials, which are official records, to both JARD and the National Library, whether or not the works are published or non –published.

MDAs shall put in place the five categories of skills required to run an optimal RIM enterprise, specifically: Registry, Records Centre, Paper Archive, Digital Archive and Audio Visual Archive.

Changes to the RIM enterprise ICT environment shall be implemented in a timely manner.

Recoverability, redundancy, continuity and sustainability of RIM in ICT systems shall be addressed at the time of design and must be fully integrated across the entire organisation as a required managed process.

Affected MDAs shall employ Collaborative Case Management (CCM) approaches, which leverage the core components of RIM including online links to case documents for rapid retrieval and review.

MDAs shall complement perimeter security with a measured approach to managing internal information security by developing prescribed standards to manage and secure content using access controls and audit trails.

RIM ICT initiatives shall be conducted in accordance with the enterprise plan promulgated by JARD.

Individual MDAs shall pursue RIM ICT initiatives which conform to the blueprints and priorities established at the enterprise level.

8.1 Adoption and Use of International Standards

The GoJ has adopted various international standards to guide the management ICT generated records. These include the DoD 5012 and ISO 15489 as well as the other complementary RIM standards shown in diagram on Figure 2 below.

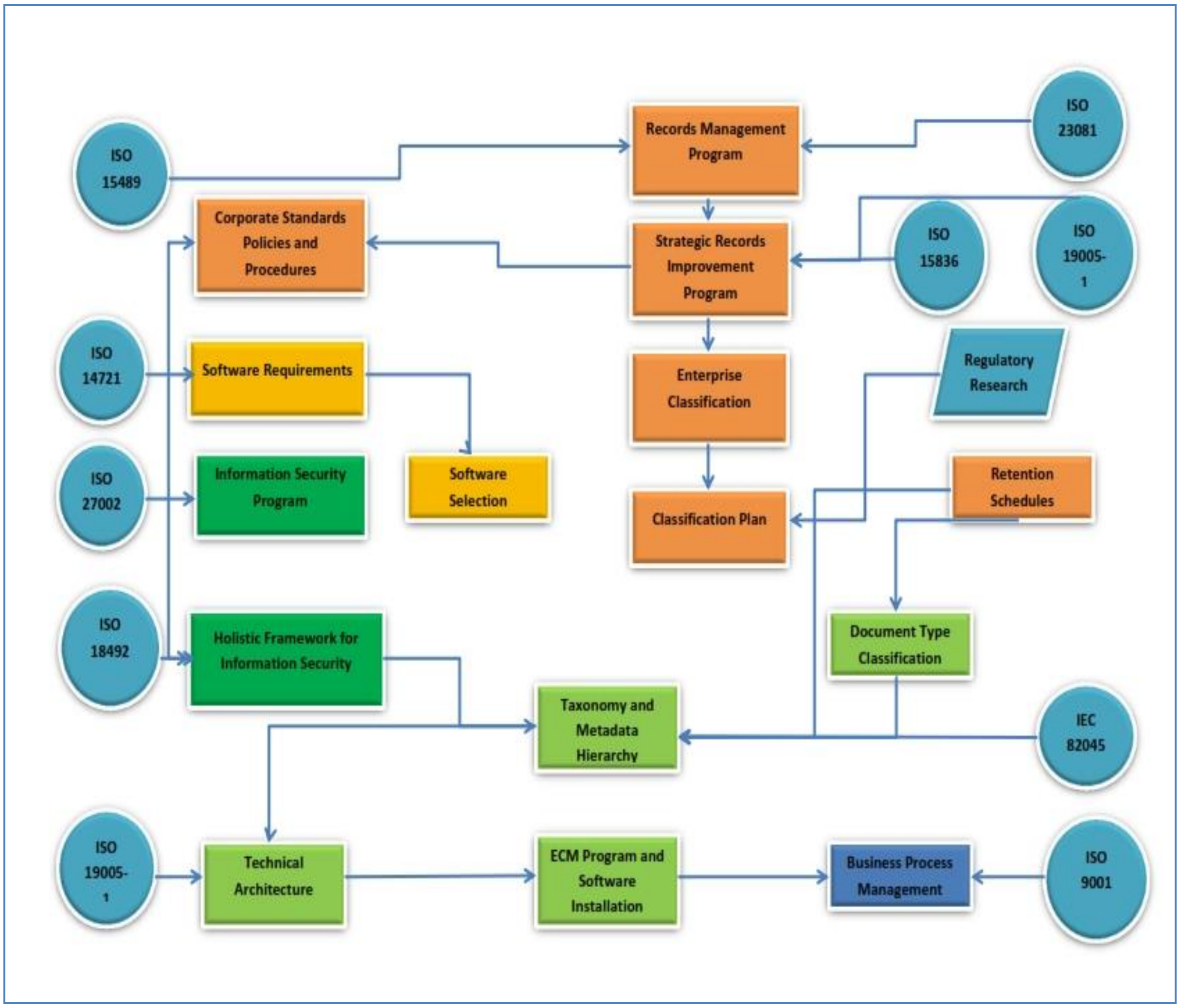

Records Management Program
ISO 15489
ISO 23081
Corporate Standards Policies and Procedures
Strategic Records Improvement Program
ISO 15836
ISO 19005-1
ISO 14721
Software Requirements
Enterprise Classification
Regulatory Research
ISO 27002
Information Security Program
Software Selection
Retention Schedules
Classification Plan
ISO 18492
Holistic Framework for Information Security
Document Type Classification
Taxonomy and Metadata Hierarchy
IEC 82045
ISO 19005-1
Technical Architecture
ECM Program and Software Installation
Business Process Management
ISO 9001

Figure 2 RIM Standards

8.2 Guidelines and Standards for Software that meets RIM Requirements

While the acquisition and management of ICT systems is the full responsibility of MSTEM, JARD has a responsibility to ensure that the systems that are introduced meet RIM requirements so that the records generated can be managed as records in accordance with the applicable legislation and regulations. To assure this, from time to time, JARD will issue guidelines on RIM requirements for ECM for use by MDAs.

The guidelines for the acquisition of ECMs are based on the categorization of MDAs according to their RIM ICT maturity level so that MDAs can make sound decisions. The DDIAS/Records Manager in the MDA owns the resultant specifications and is responsible to ensure that the IT Department is aware of the RIM specific requirements applicable to the MDA before purchase or development of the ECM tools. The DDIAS/Records Manager also provides input whenever there is a need to develop or acquire ICT systems.

To discharge this mandate, the DDIAS/Records Manager should participate in the review and approval of ICT Business Cases for introduction and/or development of ICT capabilities and in any ICT governance board that approves decisions that impact ECM.

8.3 RIM ICT Capability Maturity Assessment Model

JARD has a primary responsibility to ensure that records generated by ICT systems are appropriately catered for. In collaboration with MSTEM, JARD will support MDAs to ensure that ICT systems being procured have records management functionality and are also appropriate to the MDAs RIM ICT maturity level.

A RIM ICT Capability Maturity Assessment Model has been developed by JARD for use by MDAs in assessing their RIM ICT Capability Maturity levels so that they can procure and install ICT systems that are in line with their level of RIM ICT maturity. The model specifies the minimum requirements that should be catered for by an ICT system in order to assure the records management functionality.

The "Where are we now?" question is answered through performing baseline assessments such as the RIM ICT maturity level assessment. This assessment measures the organization in an objective manner to provide a basis for comparison later.

The Maturity Level Assessment Model is designed to help MDAs and government agencies using or desiring to introduce ICT capabilities in the management of electronic records. Whilst the techniques for managing physical records have existed for many years, MDAs still face challenges when it comes to deploying ICT capabilities to manage electronic records. The Maturity Level Assessment Model therefore identifies selected factors that are required to exercise an ICT capability in records management functions.

The MDA's ability to execute specific factors provides a measure of maturity and can be used to recommend a series of sequential steps to improve RIM ICT capability. It is an assessment that gives stakeholders an insight into pragmatically improving working in the electronic records environment. This model is developed from combining aspects of the records management standard ISO 15489 and ITIL 2011 practices for IT Service Management (ITSM) that focuses on aligning ICT services with the needs of organisations.

The information below provides an overview of the RIM ICT Maturity Level Assessment tool. The full model is available from JARD.

Structure of the Assessment Model: The Model provides measures that assess 4 levels of 'maturity' against 32 aspects of what constitutes effective use of ICT capabilities in electronic records management programmes in MDAs. The 4 levels are:

Lacking (0) – MDA shows no evidence of awareness of the need to take a strategic approach in the use of ICT capabilities in the management of electronic records.

Aware (1) – Uncoordinated internal attempts to use ICT capabilities to improve records management reactively.

Defined (2) – Coordinated attempts to improve ICT capabilities for records management underway across the MDA

Aligned (3) – The effective use of ICT capabilities for the management of records is aligned and fully integrated within the MDA's strategic and operational activities.

The situation in many MDAs is already complex when it comes to the use of ICTs and therefore each description of maturity is designed to be an honest representation, capturing the main characteristics of an MDA at a specific level of 'maturity' in the use of ICTs for its electronic records management functions.

Approach: For each of the 4 levels provided in the 32 measures, a decision needs to be reached as to which is the closest to the current situation within the MDA. Attempts should not be made to be overly fixated on the individual points of detail but to aim at good general approximation of the current situation.

Due to the fact that the model covers many areas of the organisation, it is recommended to use a collaborative effort of more than one person to complete the template in any given MDA. However, it is also recommended that the final collation of data be completed by a small team of staff to ensure a consistency of approach and understanding.

Any MDA using the model is encouraged to repeat the exercise at regular intervals so as to allow the organisation to measure its progress over time.

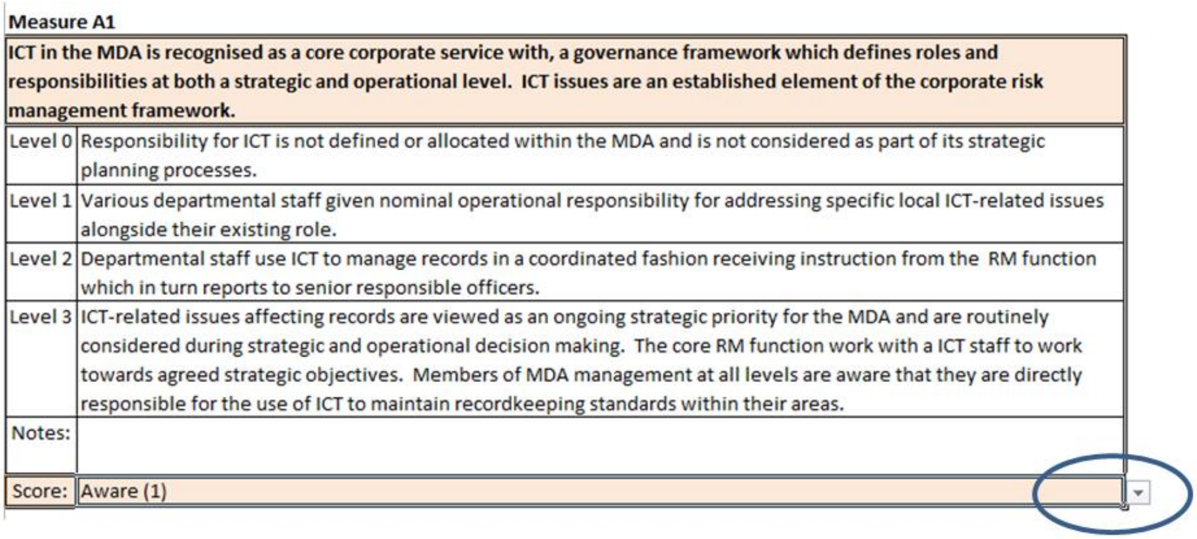
8.4 Using the Maturity Level Assessment Model

The Model is divided into 9 sections. Each Section has its own worksheet in the excel template provided.

Each worksheet has a section title and description. For example:

A	**Organisational arrangements to support ICT for records management**
	MDAs should have in place organisational arrangements that support ICT capability for records management.

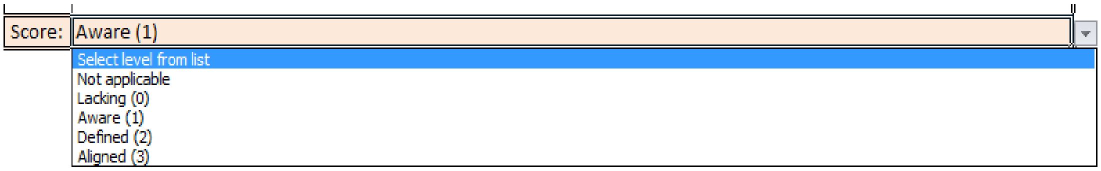
Each measure within the section is displayed. For each measure there is an identifier (e.g. A1), the statement itself and four descriptions: one for each level of maturity specific to the measure.



Measure A1

ICT in the MDA is recognised as a core corporate service with, a governance framework which defines roles and responsibilities at both a strategic and operational level. ICT issues are an established element of the corporate risk management framework.	
Level 0	Responsibility for ICT is not defined or allocated within the MDA and is not considered as part of its strategic planning processes.
Level 1	Various departmental staff given nominal operational responsibility for addressing specific local ICT-related issues alongside their existing role.
Level 2	Departmental staff use ICT to manage records in a coordinated fashion receiving instruction from the RM function which in turn reports to senior responsible officers.
Level 3	ICT-related issues affecting records are viewed as an ongoing strategic priority for the MDA and are routinely considered during strategic and operational decision making. The core RM function work with a ICT staff to work towards agreed strategic objectives. Members of MDA management at all levels are aware that they are directly responsible for the use of ICT to maintain recordkeeping standards within their areas.
Notes:	
Score:	Aware (1)

MDAs are required to select a level of maturity for each measure. By clicking on the field to the right of 'Score:' the field displaying 'Select level from list' in the above example, a drop-down icon is shown on the right. Clicking on the drop-down produces a list of levels. The appropriate maturity level is selected by clicking it.



Score: Aware (1)

Select level from list
Not applicable
Lacking (0)
Aware (1)
Defined (2)
Aligned (3)

Each measure also has a 'Notes' section allowing the MDA to optionally make notes regarding the score that they feel best represents their organisation.

Working through the 32 measures, selecting the level of maturity that best represents the MDA at the point in time by using the drop down list automatically populates the results in the Summary Score worksheet.

The results of the assessment help an MDA to obtain an accurate, reliable and honest measure of the current level of maturity of ICT capabilities for electronic records management within the organisation. This helps the MDA to:

1. identify its ICT capabilities, thereby providing evidence of the impact of previous/current investment in this area
2. identify areas of good practice which can act as catalysts to spur further development
3. provide evidence of its ability to comply with the RIM Policy

4. provide metrics for internal audit and quality assessment purposes
5. provide evidence to help inform risk management decisions
6. help identify gaps and weaknesses and thus where best to target resources and focus efforts
7. raise the overall profile of electronic records management as a strategic priority by leveraging ICT
8. measure progress in this area overtime through repeated application of the Model after set intervals
9. make objective comparisons between MDAs so as to pool resources for improvement for those at similar levels
10. allow for an enterprise view of the state of MDAs vis-à-vis ICT capabilities for electronic records management

8.5 Guidance for MDAs Procuring ECMs

To promote standardization of RIM ICT systems across the GoJ, JARD, in consultation with MSTEM, also periodically develops and issues three sets of lists:

(a) A list of ECMs under review: these are ECMs which are in the preliminary stage, or have been approved but not yet on the published list.

(b) A published list of approved and available ECMs, including those hosted by MSTEM, 3rd party vendors and those installed at the MDAs.

(c) A list of retired ECMs with information and reasons for their retirement.

MDAs should use the lists when identifying ECMs for procurement.

8.6 Information Security

MDAs should ensure that IT security and the security of the records are aligned and that the confidentiality, integrity and availability of the records, information, data and IT services always matches the agreed needs. Confidentiality is met when the records are accessed by or disclosed to only those who have a right to know. Integrity is met when the records are complete, accurate, and protected against unauthorized modification. Authenticity is met when the handling of transactions related to the records, as well as information exchanges between the MDA and its clients and sources can be trusted.

MDAs are required to complement perimeter security with measures to improve internal information security and to secure content using access controls and audit trails.

MDAs should develop management processes that have overall responsibility for maintaining the access to information and ICT systems through ensuring that access is granted only to people who require access for legitimate business reasons. Access management does not decide who has access but instead carries out the policies developed regarding access during the design stage of the ICT lifecycle.

Access management should be implemented to provide the right for users to be able to use an ICT system or group of ICT services. It is therefore the execution of policies and actions defined in information security management. Access management should execute the policies and actions defined in information security policies and regulations. It is these and related processes that determine what access should be provided and to whom it should be provided.

The objectives of access management should be to:

- Manage access to services based on policies and actions defined in information security management
- Efficiently respond to requests for granting access to services, changing access rights or restricting access, ensuring that the rights being provided or changed are properly granted
- Oversee access to services and ensure rights being provided are not improperly used.

Access management should assist with the overall security of the environment and its information. The value to business is that the MDA can be assured that its information is secure and access is provided to those who require it. With proper access management, the MDA can be assured that access to confidential information is controlled, employees have the appropriate level of access, and that access can be audited if necessary.

8.7 Disaster Recovery

MDAs should ensure that they have put in place a process to support the overall continuity of records management by managing the risks that could seriously affect the ICT system. To ensure disaster recovery at acceptable levels the MDAs should:

- Produce and maintain a set of ICT continuity plans that support the overall continuity of records management.
- Complete regular impact assessment exercises to ensure that all continuity plans are maintained in line with changing environments and requirements.
- Conduct regular risk assessment and management exercises to manage the ICT system within an agreed level of business risk in conjunction with the business and the IT team.
- Assess the impact on records of all changes on the ICT system and supporting methods and procedures
- Ensure that proactive measures to improve the availability of records are implemented wherever it is cost-justifiable to do so

- Negotiate and agree contracts with suppliers for the provision of the necessary recovery capability to support all continuity plans.

8.8 Audio-visual Records

Taking a life cycle approach to digital preservation, MDAs should also identify and address risks associated with preserving digital content prior to ingest, and apply tools and workflows to manage these. Alongside the technical solutions, MDAs should work to embed digital sustainability as a key organizational principle underpinning all digital records activities across the MDA.

8.9 Implementation of Changes to the RIM Enterprise ICT Environment

MDAs will be expected to make changes to the RIM enterprise ICT environment in a timely manner.

MDAs should develop a change management process to control the lifecycle of all changes to the enterprise, enabling beneficial changes to be made with minimum disruption to IT services. Change management should also ensures that all changes to IT services and assets are recorded and tracked. All of these activities ensure that change management minimizes overall business risk.

A change management process should be established to:

- Respond to changing business requirements while maximizing value and reducing incidents, disruption and re-work
- Respond to the IT requests for change that will align the RIM requirement with the business needs
- Ensure that changes are recorded and evaluated, and that authorized changes are prioritized, planned, tested, implemented, documented and reviewed in a controlled manner
- Ensure that all changes to IT are recorded and tracked
- Optimize overall business risk.

8.10 Collaborative Case Management (CCM)

There are MDAs that may need to employ Collaborative Case Management approaches including use of online links for rapid retrieval of case documents.

Enterprise content management’s primary task is supporting business functions, by ensuring all information gets to users in the right context, at the right time. Case management on the other hand provides tools to integrate capabilities across different aspects of the business, allowing MDAs to deliver more efficient and beneficial outcomes for each customer’s ongoing ‘case’.

MDAs should use case management tools as a function of an ECM, to not only tailor their services to a customer's unique needs and history, but also derive more insights into the trends and processes which underpin their customer life cycles more broadly. This approach requires highly integrated platforms that capture, store and analyze content, backed by infrastructure which can handle each case as a discrete yet interlinked data entity.

Case management approaches benefit from rigorous implementation of ECM systems and policies. Ideally, the case management tools in use should be compatible with the database and archival processes of the ECM system used in an MDA. That way, automated and manual case management processes alike can draw on a far greater volume of content, with far faster response time, than if they were to operate in isolation from the ECM.

Ensuring continuity and consistency of service should be possible when case management tools distribute ECM-stored content throughout the MDA, so that a customer's preferences and history result in the most appropriate form of response at every point of interaction.

For many MDAs, these customized responses should be automated to a large degree. A strong case management system should not only link content within the ECM framework to a specific case, but identify the responses it believes would generate the most impact or positive sentiment in each area of business.

Case management and ECM systems should offer clear and real-time access to customer insights across the business. Each operator or decision-maker should be able to quickly access all relevant records or changes to a given customer's history; a strong analytics platform should deliver insights specific to each business unit based on the full range of available content in the system. Ideally, such insights can adapt as new content arrives from both internal and external sources, giving all staff the most up-to-date advice on the customer's situation at any point of service.

8.11 Classification Enabled Disposition of Digital Records

The linkage of the records classification system to the records disposition process considerably enhances the identification and disposition of records.

Deletion is not destruction and does not meet the disposition requirements for destruction of electronic and digital records. When digital records are deleted it is only the pointer to the record (such as the file name and directory path) that is deleted. The actual data objects are gradually overwritten in time by new data. However, until the data is completely overwritten, there remains a possibility that the information can be retrieved.

JARD will develop and issue guidelines and methods for destroying digital records that includes:

- digital file shredding

- degaussing – the process of demagnetizing magnetic media to erase recorded data
- physical destruction of storage media – such as pulverization, incineration or shredding
- reformatting – if it can be guaranteed that the process cannot be reversed.

To ensure the complete destruction of a digital record, all copies should be found and destroyed. This includes removing and destroying copies contained in system backups and offsite storage.

CHAPTER 9 MANAGEMENT OF EMAILS

GoJ RIM Policy Requirements for Email Management: *Emails that are used to conduct GoJ business are official records and shall be captured as records and managed in accordance with this Policy.*

All MDAs shall invest in email management systems that facilitate the capture and management of emails as official records of the GoJ. Such systems shall be deployed on government designated domains.

All emails held in the official GoJ email domain(s) are the property of the GoJ therefore users of GoJ email systems shall not have any expectations of privacy.

Use of personal email addresses by public officers for official business is prohibited. If, because of system constraints/crashes, public officers have to use alternate email addresses, these shall be in the name of the organization, not personal addresses.

RIM Committees in MDAs shall designate levels at which officer's e-mails are required to be archived and preserved as per the CAPSTONE approach.

All MDAs shall define categories of information that may not be transmitted via e-mail.

9.1 General Guidelines for Complying with the GoJ RIM Policy on Emails

- As a general rule, emails received by or initiated by public offices, including attachments, and which relate to the business activities of public offices and that have continuing administrative, evidential and informational value should be retained for as long as they are needed to meet administrative and legal requirements.
- Emails that are identified as constituting official records should be captured as records and should be managed as other records in accordance with this policy.
- All MDAs should invest in email management systems that facilitate the capture and management of emails as official records of the Government of Jamaica. Such systems should be deployed on government designated domains.
- Use of personal email addresses and public email systems by public officers for official business is prohibited.
- Email facilities are provided as a tool to assist public officers and offices in their day-to-day work and should be used for official communications only.
- Personal emails should not be considered as official records and should not be captured into the recordkeeping system.
- Emails that are deemed to have evidential value should remain intact in terms of their structure (layout or format and links to attachments and related documents), content (the information contained in the message) and context (information pertaining to the

sender and recipients as well as any header information and transmittal data such as time and date) to ensure they remain authentic and accurate for the entire duration they are serving business functions.

- Users of Government email systems should not have any expectations of privacy on their emails. All emails held in the official Government email domain(s) are the property of the Government of Jamaica.
- Access to emails is subject to established access controls regulating access to other records to protect against unauthorized or inappropriate access.
- Staff in MDAs must be aware that all email messages, including personal communications, may be subject to discovery proceedings in legal actions and all staff must be aware of the appropriate response in case of legal actions.
- Every MDA should define categories of information that may not be transmitted on email.

9.2 Management of Emails as Corporate Records

Not much attention is paid to managing emails as records. Under the RIM Policy, emails will be treated and accounted for in the same way that other organizational information assets are treated.

In addition to complying with legislative requirements relating to email, MDAs also need to ensure that appropriate business records are maintained for audit and accountability purposes.

It is important that MDAs recognize that emails should be treated as records of the business activity and that failure to capture and maintain these records could be problematic when providing evidence about how a business activity was conducted and why it was done in a particular way.

To ensure that appropriate email records are maintained JARD will, from time to time, issue guidelines on how emails should be managed. When providing these guidelines it should be recognized that different MDAs may use emails in different and possibly opposing ways.

9.3 Guidelines Regarding Use of Personal Emails

As a general rule, use of work email accounts for personal use is discouraged and the limitations on use of the MDA email for personal email use should be included in the terms and conditions of employment as a way of clarifying and enforcing what the MDA's expectations are in relation to employees using its email facilities. If staff are allowed to use work email accounts for personal use MDAs must be aware of their legal obligations as regards privacy matters.

Due to the personal nature of email communication, members of staff should be made aware that it is their decision to write an email message and that they are responsible for what they have written in an email message.

9.4 Email Accounts to be Preserved in Totality

Taking a leaf from the CAPSTONE approach used by the National Archives and Records Administration (NARA) of the United States of America, each MDA will identify and designate for preservation email accounts of senior officials. These email accounts, subject to being purged of ephemera, will be preserved in totality for designated periods of time, with the accounts of officers at the highest levels being designated for permanent preservation.

If the MDA wants to preserve such electronic versions of email records, but does not have an ECM, this could be done through saving email messages in .msg format on secured network drives. It would be necessary to explore the feasibility of these option before opting for it in terms of the protection available to the email records, for example how easily could the records be changed and can access to these batch of email records be restricted. Whichever option is chosen, whether it is strictly print to paper, or secured network drives, it is important that there is consistency throughout the MDA in how and where the email records are managed. It should be noted that even if the MDA does not have an ECM it is not advisable for email records to be stored in individual's personal mailboxes.

9.5 Retention of Emails of Non-designated Email Accounts

The emails of other officers (i.e. non-designated accounts) will be dealt with in accordance with the existing retention/disposal schedules of the MDA. The RIM function in the MDA will make provision for the application of the retention instructions and will ensure the periodic transfer of concerned emails to archival storage and preservation.

All members of staff must be able to identify which email messages should be preserved as a record in relation to their work. In this context preserving a record of work means locating the relevant email message with other records that relate to the same business activities, whether this be in an ECM or on a paper file. As the types of records produced by an MDA can be diverse it will be necessary to work closely with line managers to provide more specific guidance in different work areas about which email messages will constitute records.

As email messages can easily be sent to many people in an MDA. Staff members need to be given an indication about who is responsible for identifying and preserving email messages as records. The message that is conveyed will need to be consistent with the RIM Policy. It is not necessarily possible to give detailed generic guidance about managing email messages as records because email messages can be sent to many people and can form one or many long strings, which makes it difficult to know when an email message should be captured with the other business records.

However, it is advised that MDA business specific rules are created regarding who is responsible for capturing email messages according to whether the messages are internal or external together with some consideration for who is responsible for the area of work. There should also be some advice about when to capture a record of an email exchange that has formed a string and how previous iterations of the email string should be treated.

9.6 Responsibility for Recording Emails

As email messages can be sent to multiple recipients there are specific guidelines to indicate who is responsible for capturing an email as a record:

- For internal email messages, the sender of an email message, or initiator of an email dialogue that forms a string of email messages
- For messages sent externally, the sender of the email message
- For external messages received by one person, the recipient
- For external messages received by more than more person, the person responsible for the area of work relating to the message.

When an email message has been identified as a record of a business transaction it is important that the message is retained with other records relating to that particular business activity. This will mean moving the email from a staff's personal inbox and pointing it in the appointed records management system, this might be on an ECM, classified network folders or on a paper file. The point at which a record is put into the appointed records management system is sometimes referred to as the point at which the record is captured. It is important to ensure that records are captured within the appointed records management system as this is where members of staff will refer to when they want to know when, why and what decisions were made about any given business activity.

The management of encrypted emails over time is likely to be problematic. There is a danger that encrypted emails might become inaccessible over time as the method of encryption becomes obsolete. If an MDA does send or receive encrypted emails there is a need to consider how encrypted email records will continue to be accessed over time, for example de-encrypting email messages before they are captured as email records either in an ECM, on shared drives or public email folders.

9.7 General Access Guidelines, inclusive of Emails

As with other records, emails should be subject to the access rules of the MDA. Particular attention will need to be paid to this as electronic records tend to be more vulnerable than paper records.

Technical methods used to protect sensitive emails sent from another MDA should be considered carefully before they are implemented. For example, if it is decided that a method of encryption will be used it will be necessary to decide who will have access, the circumstances when encryption should be used and to ensure that the intended recipients have compatible systems.

Using a disclaimer is a frequent method used to protect organizations from legal action if inappropriate information is sent from an email address originating from an organization’s server. Although it may be prudent to use disclaimers as they may provide the MDA with some protection against potential legal action there is no guarantee that this will be the case. A more effective preventative measure against legal action would be to ensure that members of staff are made sufficiently aware about the types of information that should not be transmitted via email through an MDA specific email policy and training.

It should not be necessary to list every specific type of sensitive information, although enough information should be given about the different types of sensitive information the MDA holds so that members of staff can identify sensitive information and understand how it should probably be treated. It is important that members of staff are aware that it is their responsibility to treat and communicate sensitive information appropriately, ie decide whether or not it can be sent via email.

It is particularly important MDAs issue a clear message that members of staff need to be extra cautious when writing and sending email messages that include personal details or where comments are made of personal nature in reference to a specific staff member or a group of staff.

9.8 List of Information that may not be Transmitted by Email

There are certain categories of records which are not suitable, because of their confidential nature, for transmission via email. Each MDA will identify and prepare a list of those records that should not be transmitted through emails.

Information relating to some subjects is too sensitive to be sent via email. The precise nature of this information will vary according to the MDA concerned. There are three broad areas of sensitive information that close attention needs to be given: (a) information with National Security implications (b) information considered as commercial in confidence and (c) personal information. It is important that these types of information be handled with care because if these types of information are communicated to the wrong people it could result in the MDA and or members of staff concerned being involved in legal action or undesirable media attention.

When formulating specific guidelines for sensitive subjects it is necessary to ensure that there is consideration and alignment with the applicable classification relevant to all the main types of sensitive information an MDA holds. It should be noted that the three types of sensitive information mentioned earlier are illustrative, some MDAs may not hold all three types of sensitive information and some may hold other types of sensitive information not included here. A list of sensitive of the classified types of records should be published with MDA specific guidelines on the management of emails categorized therein.

Once the different types of sensitive information held by the MDA have been established, it will be necessary to decide the permissible ways of communicating each type of information by email. When considering how particular types of information should be communicated it will be necessary to consider if email is to be used, whether any additional protection is required, for example connecting to the a Secure Intranet, encryption methods and disclaimers. The decision about which type of protection is required should be made according to the nature and type of business that is conducted.

CHAPTER 10 INFORMATION SHARING

GoJ RIM Policy Requirements for Information Sharing: *The flow of information and sharing of data within and across public institutions shall be encouraged to promote common understanding and knowledge, inform decision making and improve service delivery.*

All MDAs shall identify and classify their information in terms of what can be shared within the institution, what can be shared with other public institutions, what can be shared with non-public institutions, what can be shared with the public (public information) and what should not be shared.

Provisions of various legislations governing disclosure of public information shall be complied with when sharing information with entities outside the MDA.

Adequate technological infrastructure including ICTs shall be deployed to facilitate sharing of information, including but not limited to online sharing. Such technologies shall provide adequate security for information being shared.

To promote information sharing and to enhance decision making within MDAs, a consolidated list of the file plans and titles of files in the Registry, departments and individual offices shall be compiled and published in keeping with the GoJ RIM Procedural Manual. Any information of public policy or other relevance or significance, collected through research or surveys and whose value has cross-cutting benefits across the public sector, shall be shared with relevant MDAs in keeping with this Policy and the provisions of a Data Sharing Policy to be developed.

RIM software and hardware shall conform to defined standards that promote interoperability for data, applications and technology.

10.1 Standards for Hardware, Software and Interoperability

JARD, in consultation with MSTEM, will from time to time, issue standards to ensure that software and hardware acquired by MDAs has records management functionality and promotes interoperability for data, applications and technology. Defining clear measures of interoperability will be key to success.

It will be important that interoperability is refined so that it meets the needs of MDAs and/or extended enterprise in an unambiguous way. The refined interoperability measures should be part of or referred to the enterprise architecture strategic direction. These measures should be instituted within a transformation strategy that should be embedded within the Target Architecture definition and pragmatically implemented in the Transition plans.

Interoperability can be specified through the following four degrees:

- *Degree 1:* Unstructured Data Exchange that involves the exchange of human-interpretable unstructured data, such as the free text found in operational estimates, analysis, and papers.

- *Degree 2:* Structured Data Exchange that involves the exchange of human-interpretable structured data intended for manual and/or automated handling, but requires manual compilation, receipt, and/or message dispatch.
- *Degree 3:* Seamless Sharing of Data that involves the automated sharing of data amongst systems based on a common exchange model.
- *Degree 4:* Seamless Sharing of Information that is an extension of Degree 3 to the universal interpretation of information through data processing based on co-operating applications.

These degrees are very useful for specifying the way that information has to be exchanged between the various systems and provide critical direction to those implementing the systems.

10.2 MDA Schedules of Information/Data Handling Storage Points

Information can only be shared if its existence is known. The foundation of information sharing will be the identification, in each MDA, of the information and data handling and storage points. While in most MDAs the bulk of the information will be in the registries, there will be information held at other points whose existence will need to be logged and made known.

The bed-rock for effective information sharing lies in the realisation that all information and data have a lifecycle defining their point of origin, and point of disposition in the MDA. This lifecycle should be explicitly managed/controlled and not left to chance. Today, the volume of information that most MDAs need to manage is increasing continuously and exponentially. The ever-changing landscape of business and technological requirements presents new challenges to MDAs. Each MDA should therefore ensure that procedures and policies are developed to put technologies, processes, policies, and culture in place to ensure that information is treated as assets and cost-effectively managed throughout its lifecycle.

The approach should:

- Facilitate maturity based cost-effective access to business data and information
- Facilitate cost reduction of IT infrastructure by optimizing base on maturity level/capability
- Enable closer alignment of ICT to business processes
- Have reliable data storage, backup and recovery procedures
- Classify information and identify its value to the business as soon as possible
- Implementation and management of e-mail Management
- Reduce cost of ownership through data and information retentions and disposal policy
- Protect information assets from unplanned deletion or security violations

By explicitly managing the information lifecycle, MDAs can put in place an approach that proactively minimizes business risk. At the same time, it reduces technology infrastructure, and compliance and litigation costs.

10.3 MDA-wide Records Schedules

The next step will be to have schedules of records held in the MDA which can then be made accessible according to the access provisions of each institution. The guiding rule is that, at the very top, the existence of all information should be known (and accessible) and this will narrow as you go down the ladder.

A Records Retention Schedule is a document detailing the storage and appropriate disposition of all records within the organisation. These MDA specific schedules should be derived from a comprehensive analysis of all identified regulations, business operational processes, industry standards, and business obligations, both internal and external.

A robust Records Retention Schedule is a fundamental tool for the implementation of an information sharing strategy which will affect the way information is stored, referenced and how long it will remain available for access. The schedules should fit within the MDA-wide records management policies and processes that determine what defines a record, its lifecycle, and how it fits within the classification model. It is derived directly from records classification used to define the controls and processes to follow for sharing, securing, managing, and safely disposing records.

10.4 Schedules of Information that can be Shared

It is important that decisions are made regarding which information can be shared and with whom. This should be documented in the MDA's RIM Policy and procedures so that staff are guided accordingly.

All groups of stakeholders in the MDA will have security concerns when sharing information and it is therefore desirable to bring security procedures to the fore front as early as possible in the life-cycle. Throughout the life-cycle of information, guidance should be provided to staff on security-specific steps which should be taken.

The generally accepted areas of concern before establishing information sharing regimes are:

- Authentication: The substantiation of the identity of a person or entity related to the MDA that accesses shared information in some way.
- Authorization: The definition and enforcement of permitted capabilities for a person or entity whose identity has been established.
- Audit: The ability to provide forensic data attesting that the sharing and data access has been used in accordance with stated policies.
- Assurance: The ability to test and prove that the systems used have the security attributes required to uphold the stated security policies.
- Availability: The ability of the MDA to function without service interruption or depletion despite abnormal or malicious events.

- Information Protection: The protection of information assets from loss or unintended disclosure, and resources from unauthorized and unintended use.
- Administration: The ability to add and change policies, add or change how policies are implemented in the MDA and add or change the persons or entities related to the systems.
- Risk Management: The MDA's attitude and tolerance for risk.

10.5 Requisite ICT Infrastructure for Information Sharing

Access to information should be facilitated by the requisite infrastructure including, where feasible, digitization capability. Increasingly more and more information should be made available online and MDAs must strive to install the infrastructure needed to promote access to information.

The ICT Infrastructure is a prerequisite to the effective physical implementation of the information platform and its associated management functions. When designing the infrastructure, MDAs should seek MSTEM's support in the following areas:

- Security
- Archiving and backup of data
- Disaster recovery and restoring of data
- Monitoring data usage especially on public websites and portals.

The process to develop an effective ICT infrastructure should incorporate the following steps:

- Define a taxonomy of platform services and logical technology components (including standards)
- Identify relevant locations where technology is deployed (local, at MSTEM, Vendor, cloud etc)
- Carry out a physical inventory of deployed technology and abstract up to fit into the taxonomy
- Look at application and business requirements for technology
- Is the technology in place fit-for-purpose to meet new requirements (i.e., does it meet functional and non-functional requirements)?
    - Refine the taxonomy
    - Select product (including dependent products)
- Determine configuration of the selected technology
- Determine impact:
    - Sizing and costing
    - Capacity planning
    - Installation/governance/migration impacts

10.6 Guidelines for Sharing Research Information across the Public Service

In the public service, considerable resources are used to conduct research into different aspects. The results of this research often remain within the confines of the commissioning unit or the MDA and are rarely shared with other MDAs. MDAs will be required to identify research that can be shared with other MDAs and/or the general public and which should thus be made available through various channels, including online channels.

For members of the staff from different MDAs to have confidence that data sharing takes place legally, securely and within relevant guidance, all participating organizations need to have in place policies which meet the requirements for:

- Data Protection
- Confidentiality
- Information Security

These policies must cover manual, verbal and computer-based data; processes must be in place within MDAs to regularly monitor and improve the effectiveness of these policies.

All MDAs should ensure that secure solutions exist to support the safe transfer of data. Risk assessments should be carried out before the transfer of data is carried out and all reasonable steps to mitigate any risks identified taken.

Supporting documentation relating to the secure transfer, receipt, access to, storage and disposal of shared data should be made available to staff. Each MDA should keep a log of all requests for data sharing received. Each MDA should also instigate a system of reporting back to the originator of data where actions have been taken on the basis of the data shared.

MDAs should put into place policies, procedures or guidelines covering:

- Communication by fax
- Communication by phone
- Electronic communication
- Verbal communication
- Written communication
- Use of personal data for purposes other than that agreed
- Access arrangements to shared records and databases
- Secure storage and disposal of confidential data.

These policies, procedures or guidelines should be subject to regular monitoring and all MDAs should have evidence that they have checked that their shared data is being kept and processed correctly by any 3rd parties.

10.7 MDA Websites Containing Information that can be Accessed by Citizens

Websites and online channels should be utilized by the MDAs to share information with their clients as well as with the citizens in general.

MDAs should have their websites actively monitored and assessed: Ongoing monitoring, analysis and evaluation of websites is an important component of the website management lifecycle and is critical to improving performance and service delivery. It should be used to determine if the business objectives of the website are being met, to provide a basis for improving the website by understanding how citizens interact with it, and as a means of determining when a website or specific content within a website should be redeveloped or decommissioned.

MDAs should explore opportunities for collaboration: Before developing or redeveloping a website, MDAs should explore opportunities to collaborate with other MDAs to deliver a more complete view of the information and services available for a particular service/topic area or to make it easier for citizens to access a range of related services.

Searching online is a quick way to initially identify MDAs that have a shared interest in a particular area. Social media can also play a key role in bringing together people and ideas that spark collaborative opportunities and can also provide an effective means for MDAs to interact with and build a better understanding of citizen needs.

Responsible Management: Citizens must be able to trust that the MDA website they are interacting with complies with the law and protects their interests. MDAs must ensure that all online presences and online activity are managed appropriately. Website content owners must ensure that their content is managed appropriately and that citizens are informed about the website's conditions of use and, where relevant, how information about them will be used.

MDA websites must be identifiable: Citizens must be able to readily identify an MDAs website and confidently engage with the information and services provided by the website. MDA websites must effectively communicate their status and authority. Citizens should feel comfortable interacting with MDA websites and exchanging information should they choose to do so. They should also be able to find out more about the nature of the website and its context within the Government.

CHAPTER 11 RECORDS APPRAISAL AND DISPOSITION

GoJ RIM Policy Requirement: *No official records shall be destroyed without the approval of the AAC.*

The appraisal of records and the preparation of records retention/disposal schedules shall be done at the macro-level, i.e. at records series and sub-series levels.

Records retention/disposal schedules for categories of records that are common across the public service shall be prepared and issued by the AAC and shall be applied by all MDAs.

MDAs shall develop institution specific records retention/disposal schedules in compliance with the GoJ Procedural Manual and through consultation with the RIM Committee and JARD.

11.1 Records Appraisal: Definition and Scope

Appraisal is the act of determining the value of that information and for prescribing what should happen to the information. The records appraisal process makes it possible to identify the period of usefulness of the information, to give appropriate instructions as to the fate of the information, to provide a mechanism for assigning disposal/retention periods, and to provide a mechanism for carrying out the disposition instructions.

Appraisal also involves identification of those records that merit preservation as archives because they have an enduring value for purposes other than those for which they were created.

The retention/disposal decisions are reached by applying concrete records appraisal criteria which make it possible to make objective[3] decisions.

11.2 The Regulatory Framework

The retention and disposal of public records is governed by The Archives (Official Records) Regulations, 1988. According to the regulations: *"No official record shall be disposed of without the prior approval of the committee",* (i.e. of the Archives Advisory Committee).

The GoJ RIM Policy requires all MDAs to prepare and maintain records retention/disposal schedules approved by the Archives Advisory Committee.

11.3 MDA Records Appraisal Sub-Committees

The appraisal of an MDA's records is the responsibility of the MDA RIM Committee. However, the RIM Committee has many other responsibilities and might not be able to find the time required to conduct this exercise. Accordingly, to conduct the detailed and initial appraisal, MDAs are advised to constitute a Records Appraisal Sub-Committee which should include three key stakeholders:

DDIAS/Records Manager: The DDIAS/Records Manager/Registrar to chair the sub-committee and put the records being appraised within the context of the other records in the MDA.

[3] "Building Records Appraisal Systems", International Records Management Trust and International Council on Archives, 1999

Records Creators: A representative from the department whose records are being appraised to advise on the continuing utility of the records (i.e. on their primary value).

Legal Counsel: A representative from the legal department to advise on any legislative requirements for the retention of the records. If there is no legal officer in the MDA this can be someone from one of the other institutions in the Ministry cluster.

Longest Serving Officer: An officer who has been with the MDA the longest time to advise on possible historical value.

The above form the core of the Records Appraisal Sub-Committee and may be joined by other stakeholders brought in for one reason or another. For instance the sub-committee may bring in someone from Accounts to advise on the financial retention requirements. JARD may also be requested to send a representative.

The deliberations of the sub-committee are submitted to the RIM Committee for its consideration, endorsement and submission to the Archives Advisory Committee.

The Records Appraisal Sub-Committee should meet at least once every three years.

11.4 The Functional/Macro-appraisal Approach

The functional/macro-appraisal approach, combined with “values-based” analysis is used to appraise records in the GoJ.

- Functional appraisal is based on determining the functions of the institution, identifying the offices that create records in carrying out the functions and selecting the records that provide the most complete and concise documentation of the functions.
- The functional approach focuses on the functions and structures of the records creating agencies rather than the records themselves and is intended to reduce the need to examine the records themselves.
- The term macro-appraisal is used to denote the approach through which the appraisal is done at the higher level of records series and sub-series as opposed to the approach in which appraisal is done file by file. In the past, file by file appraisal used to be the standard records appraisal method. However, because of advances in information technology and the large accumulation of records that modern institutions have to deal with, it is no longer practical to use that approach.
- Using this methodology, records appraisal is done very early in the records life cycle, i.e during the period of currency and the schedules prepared are applicable to the existing accumulations of non-current records as well as the records being created at present and due to be retired in future.
- The appraisal and scheduling of records takes into account any existing administrative and legal instruments, national and institutional, that regulate the disposal of specified categories of records, e.g. financial records.

11.5 Records Appraisal Activities

There are a number of activities that are carried out in appraising records:

1) Research and analysis of the mandates and functions of the institution including the overall organisational structure, the operational departments and the functions of these departments.
2) Identification and confirmation of the activities, transactions, records series and sub-series of the institution.
3) Appraisal of the records using the functional macro-appraisal approach supported by value-based analysis.
4) Compilation of Records Retention/Disposal Schedules.
5) Submission of the schedules to the MDA RIM Committee and onto the Archives Advisory Committee
6) Approval and implementation of the schedules.

11.6 Research and Analysis of Organisational Mandate/Functions

Appraisals should not be based on intuition or arbitrary suppositions of retention needs but on thorough research and analysis of the institution, its given mandate and mission, the functions that it undertakes and the resultant records.

Analysis is based on getting an understanding of the administrative and operational procedures of the institution, relationships between the functions, activities, transactions and records series, a perspective of the entire documentation produced by the institution and on a scrutiny of the records series to determine their short or long term value.

The function based classification scheme of the MDA and its identified functions, activities and records series provide a vital input to the appraisal process. Further analysis of the functions is, however, undertaken at the point of records appraisal in order to provide the records appraisers with more detailed information about the functions and records to facilitate decision making.

11.6.1 Background and Organisational Mandate

The mandate of the institution is found in the legal instruments that established the institution including Acts of Parliament, Government Gazettes and other statutory instruments. The mandates of the institution are also articulated through vision and mission statements and through:

- Policy and procedures documents
- Annual reports
- Corporate plans and strategies

Interviews and consultations with key staff also provide valuable information and insights to validate the documentation as well as capture practices that may deviate from the laid down mandates.

To establish the context of the functions and the records, the mandate of the institution must also be reviewed within the overall context of the GoJ:

- What is it that makes the organisation unique?
- Does any other MDA or organisation perform similar functions?
- Is the organisation dependent on another organisation to complete work on its mandate?
- Does the organisation consult regularly with another entity in the fulfilment of its mandate?
- Are there other organisations which have responsibility in relation to legislation for the organisation?
- Are there any joint committees with other entities for the fulfilment of the mandate?

The analysis of the organisation's mandate is done once and the information gathered kept for use during subsequent records appraisals.

The information also enables the records appraisers to identify and distinguish between "offices of primary interest" and "offices of collateral interest". As defined by the Library and Archives of Canada[4], an "Office of Primary Interest" (OPI) is the --- government institution -- department, agency, board, office or commission -- to which the authority, responsibility and accountability to perform a particular function on behalf of the Government ---- has been specifically assigned by legislation, regulation, policy or mandate. The concept is useful in ensuring that records relating to the core responsibilities of an institution or to departments and units within an institution are preserved in contrast with related/duplicate records that may be found in other MDAs or in other functions within the institution.

As an example, records containing minutes of the institution's senior management team meetings will be found amongst the records of all those who attend the meetings. Faced, therefore, with identical file sub-series from several divisions/departments, the retention consideration will be to preserve the set of minutes belonging to the division/department that has primary responsibility for this function, i.e. the Office of Primary Interest.

11.6.2 Organisational Functions and Structure

The structure of the organisation is contained in the organisation charts or organograms. The organisation charts assist the Records Appraisal Committee to review the records in terms of the institution's management structure, reporting channels and levels of authority. Through the organisation charts, the functions of the institution and the relationships between groups of records are identified and mapped and it is possible to untangle the interrelationships within the records, identify records which are duplicate, determine which records should be the "record" for purposes of retention and to make disposal decisions.

11.7 Functional Analysis

Functional Analysis is then conducted. Each function and sub-function is scrutinised in detail. Questions that may be asked include the following:

[4] Library and Archives Canada, website

- What function is represented?
- How does the function relate to other functions in the organisation?
- What is the importance and ranking of the function within the organisation?
- What is the reporting structure of the function?
- What programmes are administered by the function?
- What types of decisions and policies are made by the function?
- What types of records document the policies and decisions of the function?
- Who receives copies of the decisions and policy documents?
- What types of reports are produced?
- What is the size, volume and arrangement of the records?

Information obtained should then be used to rank the functions and sub-functions in order of priority with eligibility for permanent retention rising in relation to the ranking of the function. As can also be expected, records created by higher offices/functions in the organisation are likely to merit permanent retention in relation to records created in the lower offices.

The ranking of the functions is done on a scale of 1-5, with 1 representing functions with high importance while 5 is for functions with low importance. Most of the records of the functions with high ranking are likely to merit permanent preservation while those of low ranked functions are likely to be of transient nature.

In determining the above, it may be necessary to identify and interview key stakeholders in the MDA. These include business area managers, legal staff, accounts staff, internal auditors and records users, especially those who have been with the organisation for a long time. These can provide key perspectives on functions and records that are deemed to have critical value. Information technology staff will also be useful in identifying the various business systems in which records might be held.

11.8 Records Series Identification

The functional analysis exercise is used to conduct the first part of the appraisal and is focused on ascertaining the value of the function and the function’s records. From the functional analysis, it is possible to draw broad conclusions on whether the records have a long term value or are of a transient nature. From the functional analysis alone, however, it may not be easy to decide with precision, how many years the transient records should be retained.

To determine this with more precision, a macro-appraisal exercise is conducted at the records series and sub-series levels. The records series and sub-series are identified through the function based MDA’s classification scheme.

Series of records comprise those records which belong to clearly identifiable functions and that have a common bond. In general, each function is considered as a group/fonds and the main activities within each function comprise the sub-fonds. The major transactions within each activity (sub-fonds) represent the records series while the sub-transactions represent the sub-series.

Through the file classification system, functions which are common to all the departments will already have been identified. This should result in the development and issuing of a records retention/disposal schedule with two segments: the first part being for those records which are common to all departments and the second being for department specific records.

In general, retention schedules are constructed at records series level. However, there will be some cases where it is necessary to disaggregate the records for more specificity and, in such cases, the appraisal can also be done at the records sub-series level.

11.9 Assessing Primary and Secondary Values

To ascertain the retention period with precision, a second step is added to the appraisal process through appraisal of the primary and secondary values of the records. The Records Appraisal form at Annexure 2 is used for the exercise.

Generally information has two major values:

Primary value. All information has a primary value which stems from the primary reason for which it was created. This primary value ceases as soon as the primary purpose has been accomplished.

Secondary value*.* After the primary purpose has been served information could in fact be disposed of. However, this does not always happen because quite often the information must now serve a secondary purpose in so far as it is needed to satisfy other needs.

11.9.1 Primary Values

All information is created to serve a specific purpose. In serving this purpose, information has a primary value whose period of usefulness varies from just a few minutes to a few weeks, months, years or even eternity. There are three main categories of primary value and many series of records may have more than a single primary value.

Administrative Value

Records have this value if they help the institution to perform its current work. The time during which this value exists may be long or short, depending on the purpose it serves.

Records such as routine requisitions have a short-term value. Closed transaction files may pertain to long-term fiscal, regular or control operations and their administrative value may last over a long period. Directives, orders and regulations obviously have long-term administrative value.

Many records at operating levels have little administrative value because they are:-

- Duplicated elsewhere, as in correspondence or directives.
- Summarized at higher levels, as in reports.
- Temporary controls, such as log books.

Most housekeeping documents have short-term administrative value because they document routine transactions quickly completed. They may consist of requisitions, purchase orders, invoices, vehicle log books and the like.

Legal Value

Records have this value if they contain evidence of legally enforceable rights or obligations. Among these obligations are the legal rights of persons to make claims against the institution.

Among records having legal values are:-

- Documents involving legal agreements, such as leases, titles, and contracts.
- Evidence of actions in particular cases, such as claims papers.

The duration of legal value varies with the matter at hand.

Fiscal Value

Records having fiscal value relate to financial transactions. They may be budget records, which show how expenditures were planned, they may be vouchers or expenditure files of several kinds, which document the purposes for which funds were spent, or they may be accounting records. Records relating to the development of fiscal policy should not be confused with those of fiscal transactions. Fiscal policy files may have long term value while the transaction papers have only short term value.

11.9.2 Secondary Values

Secondary values go beyond primary needs and interests, and are of two types:-

- **Evidential values:** These give evidence about the existence and functioning of the institution.
- **Information values:** These give information about persons, things, problems and conditions with which the institution dealt.

Evidential value means that the records give evidence of organisational structures and functions. Some records which contain such evidence have archival value. Such records are needed as evidence of the organisation's responsibilities and how it discharged them. They are needed so that the experiences of the organisation can be examined later.

Records that contain evidence of an organisation's functions, policies, decisions, procedures, operations, or other activities should thus be preserved as archives. These records give indication of the organisation's origins, its structure, the policies it followed, the reasons for their adoption, and the procedures used to implement the policies.

Evidential records provide precedents so that when quick decisions are needed by the organisation, much planning effort can be avoided.

In general, the records kept should show the organisation's plans, methods and techniques used to carry on its business. The ease in locating policy and procedure material depends on the quality of the organisation's documentation. Quality, in turn, depends largely on how well decisions are recorded and on whether or not the records are filed separately from temporary materials.

Sources of policy and procedures records include the following:-

- Directives, manuals together with related endorsed comments.

- Organization charts and directories provide important documentation of the structure of the organisation. Master sets should be earmarked for preservation.
- Narrative and statistical reports on accomplishments at divisional or higher organizational levels are important. Often there exist summary narrative accounts of the direction and execution of the organisation's programmes which have been prepared for annual reports or for other purposes.
- Publicity materials, in the form of press releases, official speeches, charts and posters, showing the actual administration of programmes.

Records of top management, and of management offices at various levels of the institution, should generally be retained. These may include the correspondence files, minutes of meetings, memoranda, directives and other evidence of official action. In general, the records of offices decrease in value as the administrative ladder goes down.

Informational values relate to the information that is created as a result of the organisation's activities. In looking for informational values, appraisal is concerned with the information in them. The information may relate to persons, things, places, and phenomena. There are three tests for informational values:

Uniqueness: This means that the information in the records cannot be found elsewhere in as complete and usable a form.

Form: This mainly concerns the degree to which the information is concentrated. It relates also to the physical nature of the records. Ease of access to the data often needs to be considered when choices must be made between two series, arranged differently, containing virtually the same information. Choices may have to be made between paper records, electronic and digital records, or records stored or processed on other media, but data concentration and ease of access are still the important tests.

Possible Research Value: The research importance of a records series is an educated guess by an appraiser. Such decisions are generally based on a broad understanding of the business of the institution, technological advances taking place and the areas in which future research is likely to focus on.

In determining secondary values of records, the advice of the International Records Management Trust and the International Council on Archives quoted below also provides useful guidance:

"The archivist identifies those records that provide the most complete and concise documentation of significant functions. The following types of records may be targeted:

- *record sets of minutes, papers and reports of internal committees and of inter-ministerial or inter-departmental committees for which the agency provided the secretariat*
- *records relating to the formulation of legislation and policy arising from the core functions of the agency, including both successful and unsuccessful programmes*

- *records that document precedents or major developments in the functions, organisation, working procedures, activities, accommodation and staffing of the agency*
- *record sets of reports, directives, forms, manuals, official publications (including non-sale items)*
- *information that is not unique but is more comprehensive or in a more convenient form than that in other records of the agency or in the records of other agencies*
- *records already identified as of long-term utility to the agency, such as records that must be preserved under any statutory provision; records documenting rights or obligations of the state and so on."*

Additionally, it is also useful to follow the appraisal practices of the National Archives of Australia in which records which have permanent value are seen as fulfilling all or some of the five objectives stated below:

Objective 1: To preserve concise evidence of the deliberations, decisions and actions of the Government and its institutions relating to key functions and programmes and significant issues faced in governing the country. Major decisions in relation to a function, especially those decisions made on behalf of the nation, have national application or implication, signal a new or changed policy or involve substantial expenditure.

Objective 2: To preserve evidence of the source of authority, foundation and machinery of the Government and its institutions.

Objective 3: To preserve information that is considered as essential for the protection and future well-being of country's people and their environment

Objective 4: To preserve records that illustrate the condition and status of the country and its people, the impact of the Government's activities on them and the interaction of people with the Government

Objective 5: To preserve records that have substantial capacity to enrich knowledge and understanding of aspects of the country's history, culture and people.

11.10 Other Appraisal Considerations: Sampling

There are certain categories of records which, because of their bulk, are difficult to preserve in their entirety. When this is the case, sampling becomes a useful technique to use. The primary requirement is that the sample size and technique should be agreed beforehand. Sampling may consist of no more than keeping files at pre-determined intervals, such as keeping every 50th file. This is known as serial sampling. Such sampling may, however, not be suitable if other considerations such as geographical or time representation have to be taken into account.

When deciding on the sampling method to be used, as well as the sample size, it is important to foresee the possible uses to which the materials will be put in future and thus to ensure that the method and size of sample have sufficient validity to be of use to those who will need to use the materials later. Some methods might render the preserved samples useless.

Sampling may be one of the conditions stipulated in the retention/disposal schedule.

11.11 Guidelines for Making Retention Decisions

The following guidelines can facilitate the making of valid retention decisions:

- Avoid the "every conceivable contingency syndrome" - a records retention programme cannot and should not be designed to accommodate every conceivable need for information at any future time, however remote the probability might be. Virtually every piece of paper generated in an organisation has some future use for someone, somewhere. The reality, however, is that it is not possible to preserve everything and therefore tough disposal/retention decisions must be made.
- Information should be retained if there is a reasonable probability that it will be needed at some future time to support some legitimate legal or business objectives and the consequences of its absence would be substantial.
- Records retention policies should generally be conservative in the sense that they do not expose the organisation to an inordinate degree of risk. If the only benefit of a short retention period is a saving in space, a substantial degree of risk is usually not justified to attain this reward.
- Those involved in records appraisal must be mindful of the fact that the presence or absence of information can be either helpful or harmful to the institution depending on the specific legal or business contingencies that may arise at any time in the life of the institution. It is difficult to predict the occurrence of these contingencies with any certainty. The best way to minimize the risks associated with records retention is to provide for their systematic disposal immediately after the expiration of their value for legal and business purposes.
- A retention period is most likely to be valid if it is based on a professional consensus of the opinions of persons most knowledgeable about the value of the information and the costs, risks and benefits of its disposal after varying periods of time.

ANNEXURES

Annexure 1 TERMS OF REFERENCE-MDA RIM COMMITTEES

TERMS OF REFERENCE

RECORDS AND INFORMATION MANAGEMENT(RIM) COMMITTEE

1. Background

The Government of Jamaica through the Modernisation Vision and Strategy 2002-2012, Ministry Paper 56/02 articulates the importance for accurate and accessible data in carrying out the functions of government and highlights the need to 'improve the collection, management, analysis and use of data/ information within ministries and agencies and electronically link institutions across the island.' Further in 2013, the Public Sector Transformation and Modernisation Programme (2013-2018) administered by the Office of the Cabinet (OoC), provided for the development of "an Integrated Records and Information Management Policy (RIM) for the GoJ and provide necessary digitising capacity to Jamaica Archives and Records Department (JARD) to ensure that records and information collected, are stored and managed in a consistent manner across the public sector to enhance accessibility of Government data and information for efficient service delivery."

A key element of the RIM Policy framework requires all Ministries, Departments and Agencies (MDA's) to establish a RIM Committee (the Committee) to direct and oversee the implementation and monitoring of the RIM Policy within each MDA.

2. Purpose of the RIM Committee

The purpose of the RIM Committee is to provide:

- advice to the Permanent Secretary on the status of Records and Information Management (RIM) across the Ministry and its Portfolio entities,
- support the Documentation Centre in carrying out its legislative function in managing the Ministry's electronic and physical records and information assets.
- General advice and guidance to the Permanent Secretary in the management of electronic and physical records and information.

3. Responsibilities of the RIM Committee

In guiding the implementation of the GoJ RIM Policy in the Ministry, the core Terms of Reference for the Committees shall be set out by Administrative Circular to be issued by JARD from time to time, in consultation with the MDAs, to include the following minimum functions:

- Support for the Director, Documentation, Information and Access Services (DDIAS) in the development of internal RIM Policies and RIM procedural manuals (to include the treatment of e-RIM and audio visual records) and submit to the Permanent Secretary/Head of Department for approval;
- Support the DDIAS in the development of retention and disposal schedules and submit to the Permanent Secretary for approval;

- Support the DDIAS in the development of internal classification protocols which are compatible with the established GoJ classification scheme as existing from time to time;
- Provide advice, as needed, with respect to the provision of access to official records to the public in accordance with the Access to Information (ATI) Act, 2002 and any other law;
- Provide advice on the roles and responsibilities to be ascribed various categories of staff;
- Oversight of MDA's compliance with GoJ and internal RIM policy and procedural manuals; and
- Serve as a point of contact for JARD on RIM matters, particularly, the implementation of the GoJ RIM Programme.
- Review and endorse all disposition requests prior to signoff by the Permanent Secretary/Head of Department and submission to the Archives Advisory Committee for approval.
- Review the Ministry's Portfolio entities RIM Quarterly Reports and provide comments to the Permanent Secretary on the status of RIM within the Ministry's Portfolio.

4. Membership

At the Ministry level, RIM Committees shall be constituted and chaired by a member of the Senior Management Team designated by the Permanent Secretary.

The Committees shall include the following representatives:

(a) A Senior Member of the Management Team designated by the Permanent Secretary or head of the Department/Agency to chair the committee
(b) The DDIAS/Records Manager (as the case may be) to perform the secretariat functions of the Committee.
(c) A representative of the MDA's legal department/a legal officer
(d) A representative of the IT department
(e) An Officer to represent all the administrative departments
(f) An Officer to represent all the technical departments.

The committee may establish Working Groups/sub-committees from time to time to executive it functions. This may include a Records Appraisal Sub-Committee to review the MDA's records for disposition.

5. Secretariat Support To The Committee

The DDIAS of the Ministry shall perform the secretariat functions of the Committee. The responsible officer will prepare in advance of each Committee meeting, summary documents which allow the Committee to make informed decisions on all matters to be discussed at the meeting. This will be circulated and form the basis for discussions at the meeting.

Documentation of each meeting will be circulated to each member of the RIM Committee within three working days of the meeting, indicating the issues raised, agreements made and actions to be taken.

The DDIAS will be responsible for arranging the time/date/location of meetings. He or she will also be responsible for collecting agenda items, issuing an agenda and circulating supporting papers at least five days in advance of each meeting.

6. Tenure of RIM Committee

The RIM Committee will be established by the Permanent Secretary/Head of Department and shall be required to meet as least once per quarter in compliance with the GoJ RIM Policy. The work of the Committee is ongoing and its constitution will remain unchanged unless advised by the Jamaica Archives and Records Department.

7. Quorum Requirements

A minimum of fifty percent plus 1 will be required for each meeting to be recognised as an authorised meeting for the recommendations or decisions to be valid.

8. Alternates

Members of the RIM Committee shall nominate a suitable alternate to attend a meeting if and when the member is unable to attend. The nominated alternate shall have voting rights at the attended meeting. The alternate shall be knowledgeableof the function and requirements of the areas he/she represents

The Chair should be informed of the substitution prior to the scheduled meeting.

ANNEXURE 2 RECORDS APPRAISAL FORMS

PART A Research on Functions of the Organisation

ID	SUB-ISSUE	FINDINGS	
1	What is the function and what is its mandate?		
2	What activities are involved?		
3	Does any other entity in the organisation have a similar mandate?		
4	How complex is the function relative to other functions in the organisation? (e.g. number of staff, units and sub-units, size of budget)	Score	Scale: (1) not complex – (5) extremely complex
5	How significant is the impact of the function on the people of Jamaica?	Score	Scale: (1) insignificant–(5) very significant
6	What is the degree of influence of the function on the rest of the institution	Score	Scale: (1) no influence –(5) very influential
7	What is the importance accorded to the function in the annual reports of the institution?	Score	Scale: (1) no importance – (5) High importance
8	What are the work processes involved and what is the flow of data between these?		

PART B Function/Records Occurrence Analysis Sheet

(To determine where else in the MDA similar/related records are found)

Function	Activity/Sub -Function	Records Series	Records Summary	Dept/Unit with Primary Responsibility	Records Occurrence in other Divisions, Sections, Units (Indicate actual names)				
					Dept 1	Dept 2	Dept 3	Dept 4	Etc »»

PART C Records Appraisal Form

RECORDS APPRAISAL FORM	
PART A FUNCTION IDENTITY	
Function	
Activities	
Records Series	
Scope Note	
Records Sub – Series	
PART B: ASSESSMENT OF FUNCTIONAL VALUES:	
Do records created by the function have short or long term value	
If the value is short term, what is the recommended retention period	
PART C: ASSESSMENT OF PRIMARY VALUES	
What is the primary purpose of the function/activity and records?	
For how long does this primary purpose exist?	
What is earliest point at which the records can be disposed of without secondary considerations?	
Do the records have any financial value? If yes, for how long?	
Do the records have any legal value? If yes, for how long?	
Is the disposal of the records bound by any legislation?	

PART D ASSESSMENT OF SECONDARY VALUES

Are there any secondary considerations that should be considered before the records can be destroyed?

Secondary Considerations	**Period for which records should be retained**

Do the records created by this function contain any of the following information on or about the institution?

Type of Information	**Yes**	**No**	**Type of Information**	**Yes**	**No**
Origins or history			Precedents		
Functions			Contracts		
Structure and organisation			Assets		
Policies			Important events in the Institution		
Strategic decisions			Procedures		

APPRAISAL RECOMMENDATION

Recommendation	**Conditions/Qualifiers**

Comments			
Date Prepared		**Signature of Approving Officer**	
Date Approved		**Designation**	

Annexure 3 Internal MDA Records Transfer Form

INTERNAL MDA RECORDS TRANSFER FORM					Deposit No.		
Division/Department/Unit/Office:					Page No.		
Box/Bundle No.	Description of Records	Covering Dates		Destroy/ Transfer Date	**For Records Storeroom Use**		
		From	To		Box No.	Location No.	Date Destroyed/ Transferred to RC
Records Deposited by:		**Records Received by(Name)**					
Signature:		**Signature:**					
Date:		**Date:**					

Notes:

1. **Deposit No.** Number each deposit made by your unit/office starting from No. 1 for that particular year, e.g 1/2016, 2/2016 etc
2. **Page No**. Number each page of that particular deposit from page 1
3. **Box/Bundle Number**: For each deposit, number the boxes or bundles from 1
4. **Destroy/Transfer date (5th column):** Refers to the date the records can be destroyed according to the MDA Records Retention Schedule or the date for transfer to the JARD Records Centre.
5. In the storeroom, the boxes are given unique and unrepeatable storeroom box numbers taken from the Storeroom Register.