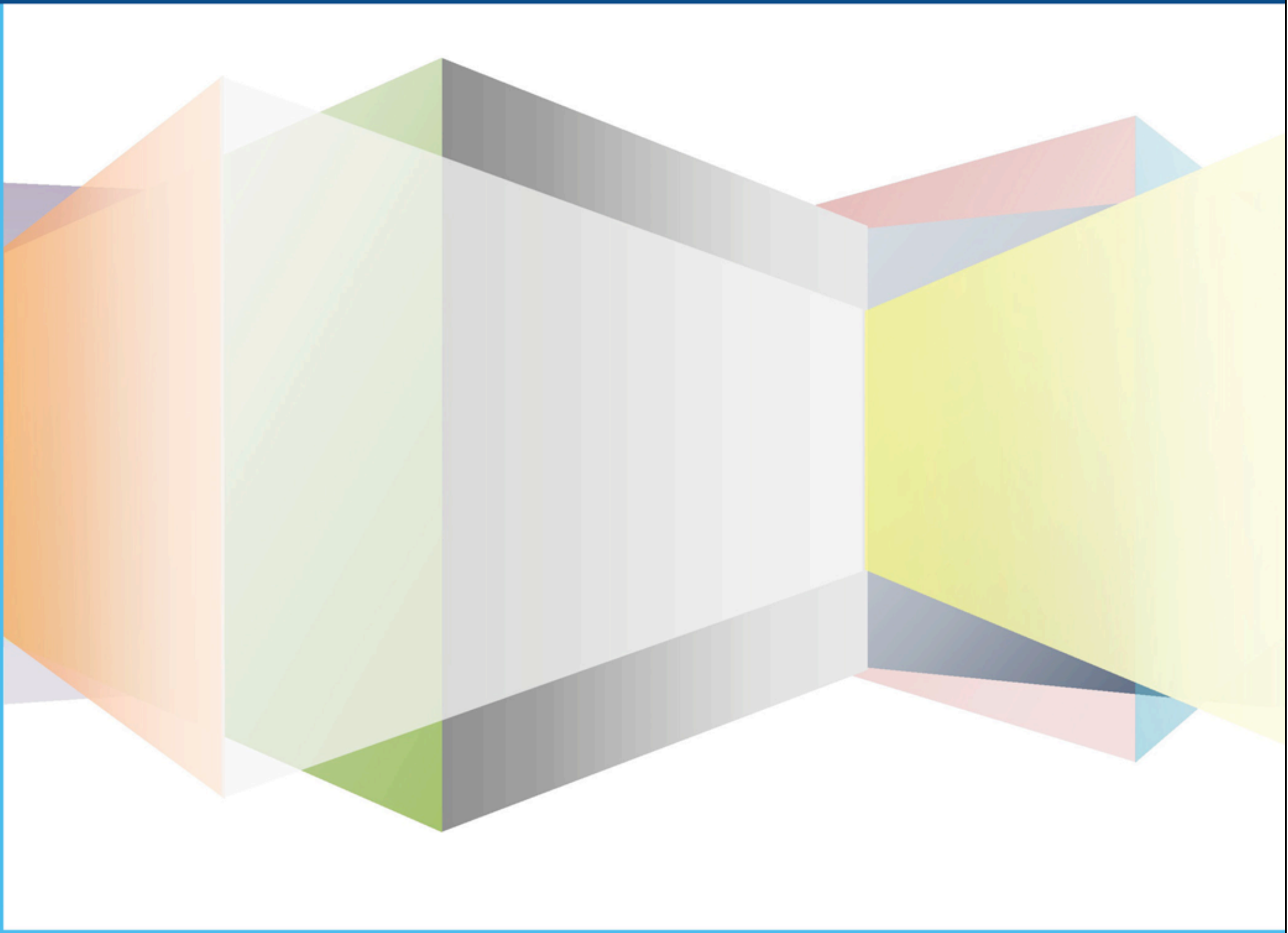
ELECTRONIC RECORDKEEPING SYSTEM IMPLEMENTATION GUIDELINES

A Handbook on Records Management Practices and Guidelines for an Electronic Recordkeeping System



Government Records Service

A Handbook on Records Management Practices and Guidelines for an Electronic Recordkeeping System

Government Records Service

Updated October 2020

Blank page

Table of Contents

Abbreviations

ADRM	Assistant Departmental Records Manager
B/D	Bureau and department
CCGO	Central Cyber Government Office
CM	Content management
DRM	Departmental Records Manager
EDMS	Electronic Document Management System
EIM	Electronic information management
ERKS	Electronic recordkeeping system
ERM	Electronic records management
FR of an ERKS	*Functional Requirements of an Electronic Recordkeeping System*
GARDS	*General Administrative Records Disposal Schedules*
GRS	Government Records Service
GRSD	Government Records Service Director
IT	Information technology
KM	Knowledge management
OGCIO	Office of the Government Chief Information Officer
RKMS	*Recordkeeping Metadata Standard for the Government of the Hong Kong Special Administrative Region*
RM	Records management
RMgr	Records Manager
RMO1	Records Inventory Form
RMO2	Records Retention and Disposal Authority
RO	Records Officer
RU	Records User
SA	System Administrator

DEVELOPMENT OF HANDBOOK

Part I

PART I DEVELOPMENT OF HANDBOOK

This part introduces the background, objectives and scope of this handbook. It has one chapter -

Chapter 1	Introduction

Chapter 1

Introduction

1

Chapter 1: Introduction

1.1 Background

1.1.1 Records are valuable resources of the Government to support evidence-based decision making, meet operational and regulatory requirements and are essential for an open and accountable government. Good records management (RM) not only helps protect records but also enhances an organisation's operational efficiency while minimising costs. RM is therefore an important common function of bureaux and departments (B/Ds).

1.1.2 Use of electronic means to conduct business and deliver public services has become increasingly commonplace in B/Ds. The proportion of government records being created digitally is increasing exponentially. Electronic records come in a wide variety of formats: e-mails, images, spreadsheets, texts, audio recordings, etc. and have a vulnerable nature. They are easily overwritten, lost or become inaccessible over time in light of rapid technological changes and obsolescence, unless specific policies, strategies and tools are developed and adopted to properly manage and preserve them for as long as they are required to serve legal, regulatory, business, operational, evidence and archival purposes.

1.1.3 In line with the Government's electronic information management[1] (EIM) strategy promulgated by the Office of the Government Chief Information Officer (OGCIO) vide OGCIO Circular No. 1/2011[2] on 3 May 2011, **B/Ds are required to take forward electronic records management (ERM) as an integral part of EIM and adopt an electronic recordkeeping system (ERKS) as a mandatory component to drive ERM in the Government**. Against this background, B/Ds should develop or adopt an ERKS to manage both their electronic and non-electronic records in an integrated, consistent and secure manner.

1.1.4 To enhance efficiency in preserving and managing government records, the Government announced in the Chief Executive's Policy Address Supplement published in October 2019 the **roll out of ERKS to all government B/Ds by end-2025**.

[1] EIM covers three domains, namely content management (CM), RM and knowledge management (KM).

[2] OGCIO Circular No. 1/2011 entitled "***Electronic Information Management Strategy and Framework***" is available on the Central Cyber Government Office (CCGO) (http://itginfo.ccgo.hksarg/content/cir/docs/OGCIO_Cir_201101.pdf).

1.2 Purpose

1.2.1 To underpin the efficient and effective management of records in an ERKS, this handbook ("Handbook") has been developed to -

(a) prescribe RM principles and best practices to manage aggregations (i.e. classes, sub-classes, folders, sub-folders and parts) and records; and their associated recordkeeping metadata and audit trails in an ERKS; and

(b) provide a framework and high-level guidance for B/Ds to follow and adopt as their own departmental handbook on ERKS RM practices and guidelines for compliance and reference by their staff in using, managing and maintaining their ERKSs so as to ensure the authenticity, integrity, reliability and usability of records managed by the ERKSs.

1.2.2 This Handbook has been drawn up with reference to internationally recognised policies, standards and practices and RM guidelines published by the Government Records Service (GRS). The RM principles and practices set out are generally applicable to the management of both electronic and non-electronic records in the ERKS environment irrespective of the ERKS solutions selected.

1.2.3 Given the inherent difference in the RM processes and procedures between the paper-based recordkeeping environment and the ERKS environment, B/Ds should supplement their own RM practices and guidelines for adoption in their own ERKS environment, in particular, the roles and responsibilities of ERKS users and the processes and procedures for performing RM tasks in the ERKS depending on their selected ERKS solutions and specific business and RM needs.

1.2.4 In practice, operational procedures for key RM functions and activities, such as scanning of paper records, should be tailor-made to cater for the system functionalities of the selected ERKS solution in addressing each B/D's specific business and RM needs. As these operational procedures are dependent on the ERKS solutions and business and operational needs of individual B/Ds, B/Ds should supplement the framework in this Handbook with information that is specific to the B/D (e.g. roles and responsibilities of ERKS users, and the practice and procedures to maintain and revise the records classification scheme) or specific to an ERKS solution (e.g. operating procedures for scanning paper records for management in the ERKS, or procedures to trigger the commencement of the retention period for carrying out records disposal in the ERKS). These supplementary information can be prescribed as appendices to B/Ds' departmental handbook on ERKS RM practices and guidelines so as to facilitate regular reviews and separate updating as and when necessary. The approach to be adopted and level of details to be covered in the departmental handbooks on ERKS RM practices and guidelines will depend on the skills, knowledge and needs of the ERKS users of B/Ds. B/Ds should therefore appropriately involve the relevant RM staff during the development of these guidelines.

1.3 Scope

1.3.1 This Handbook covers RM functions and activities supported by an ERKS under a hybrid RM environment, and in particular, electronic records in an unstructured computing environment[3] within a B/D. It does not cover the management of records in the web or structured computing environment[4] and preservation of electronic records having archival value which should be separately dealt with.

1.3.2 All government officers should continue to adhere to mandatory RM requirements and RM practices where applicable as set out in General Circulars and series of GRS' RM Publications[5] to manage their records such as arranging retention and disposal of administrative records in accordance with the requirements prescribed in GRS' RM Publication No. 4 - ***General Administrative Records Disposal Schedules*** **(GARDS)**[6].

[3] The 'unstructured' computing environment refers to where (i) business processes and workflows are not well defined; (ii) the user has relative autonomy over what information is created, sent, and stored (e.g. e-mail and attachments); and (iii) where accountability for recordkeeping has not been well defined.

[4] The 'structured' computing environment refers to where (i) business processes are typically highly structured; (ii) structured tools and techniques are employed to develop systems; and (iii) accountability for the design, development, and maintenance of systems (including integrity of the records generated in the system) has been assigned. The 'web' environment refers to where (i) the work processes are generally associated with the 'publication' of information (though this is changing rapidly with the advent of E-Government initiatives); (ii) the role of the webmaster is dominant; and (iii) recordkeeping issues are expressed as content management issues (e.g. authenticity, reliability, integrity, security, etc).

[5] GRS' RM Publications are available at CCGO (http://grs.host.ccgo.hksarg) and GRS' website (https://www.grs.gov.hk/en/hksar_government_administrative_guidelines_on_record_management.html)
.

[6] GARDS is available at CCGO (http://grs.host.ccgo.hksarg/file/2.4.4_P4(Oct_2013).pdf) and GRS' website (https://www.grs.gov.hk/pdf/P4(Oct_2013)(Eng_only).pdf).

1.4 Audience

1.4.1 This Handbook is intended primarily for RM staff, i.e. Departmental Records Managers (DRMs), Assistant Departmental Records Managers (ADRMs), Records Managers (RMgrs), Records Officers (ROs); and System Administrators (SAs) who are responsible for performing RM functions and activities and other related system management activities. Nevertheless, this Handbook is also useful to Records Users (RUs) who create, receive, capture and use records in their day-to-day operations. RUs are obliged to provide necessary support and facilitation to RM staff and SAs to manage records and an ERKS.

1.4.2 This Handbook is also relevant to RM staff who are responsible for developing their own departmental handbooks on ERKS RM practices and guidelines to underpin their B/D's ERKS.

1.4.3 All ERKS users should comply with the guidelines and practices prescribed in this Handbook to create/collect, organise, classify, retrieve, use, store, maintain and dispose of records. All ERKS users should also comply with the departmental guidelines, practices and procedures set out in their departmental handbooks on ERKS RM practices and guidelines.

1.5 Related publications

1.5.1 General Circulars, Administration Wing Circular Memoranda and RM publications promulgated by GRS related to the management of records in an ERKS are listed below -

(a) General Circular No. 5/2006 entitled "***Management of Government Records***"[7] - This circular reminds heads of B/Ds of the importance of proper management of government records and draws their attention to good RM practices.

(b) General Circular No. 2/2009 entitled "***Mandatory Records Management Requirements***"[8] - This circular sets out mandatory

[7] General Circular No. 5/2006 is available on CCGO (http://ref.ccgo.hksarg/csogc/en/c200605e.pdf) and GRS' website (https://www.grs.gov.hk/pdf/GC_No._5-2006e.pdf).

[8] General Circular No. 2/2009 is available on CCGO (http://ref.ccgo.hksarg/csogc/en/c200902e.pdf) and

requirements on the management of government records.

(c) General Circular No. 5/2012 entitled "***Records Management Reviews***"[9] - This circular sets out the framework for reviewing the RM practices in B/Ds and the details of departmental RM reviews to be conducted by GRS.

(d) Administration Wing Circular Memorandum No. 4/2012 entitled "***Guidelines on Creation and Collection of Records***"[10] - This circular memorandum provides supplementary guidelines on creation and collection of records to assist B/Ds to enhance their records management practices.

(e) Administration Wing Circular Memorandum No. 5/2012 entitled "***Establishment of Departmental Records Management Policies***"[11] - This circular memorandum provides guidelines for B/Ds to formulate their departmental RM policies.

(f) ***Records Management Manual*** - This publication provides guidance and instructions for proper and coordinated management of government records.

(g) GRS' RM Publication No. 1 "***A Practical Guide to Records Scheduling and Disposal***" - This publication provides a detailed procedural guide on drawing up records retention and disposal schedules and explains the operation and services of the records centres operated by GRS.

(h) GRS' RM Publication No. 3 "***Subject Filing***" - This publication establishes a comprehensive standard classification scheme for administrative records, which are grouped into six schedules, viz. Administration, Accommodation and Facilities, Equipment and Supplies, Finance, Personnel as well as Information Systems and Services. It also provides guidelines on the development of a records

GRS' website (https://www.grs.gov.hk/pdf/GC_No._2_2009e.pdf).

[9] General Circular No. 5/2012 is available on CCGO (http://ref.ccgo.hksarg/csogc/en/c201205e.pdf) and GRS' website (https://www.grs.gov.hk/pdf/GC_No._5_2012e.pdf).

[10] Administration Wing Circular Memorandum No. 4/2012 is available on CCGO (http://ref.ccgo.hksarg/csocm/en/m201204e.pdf) and GRS' website (https://www.grs.gov.hk/pdf/CM_No._4_2012e.pdf).

[11] Administration Wing Circular Memorandum No. 5/2012 is available on CCGO (http://ref.ccgo.hksarg/csocm/en/m201205e.pdf) and GRS' website (https://www.grs.gov.hk/pdf/CM_No._5_2012e.pdf).

classification scheme for programme records.

(i) GRS' RM Publication No. 4 "***General Administrative Records Disposal Schedules***" (GARDS) - As a sequel to Publication No. 3 and using the same classification scheme of administrative records, this publication sets out retention and disposal schedules of administrative records for adoption by B/Ds.

(j) GRS' RM Publication No. 6 "***Manual on Vital Records Protection***" - This publication identifies common hazards to records, explains the importance of vital records protection, provides guidelines on selection of appropriate protection methods, and enumerates the steps in establishing a vital records protection programme.

(k) GRS' RM Publication No. 7 "***Topical Guide cum Checklists for Proper Records Management Practices***" – This publication is to assist B/Ds in assessing the effectiveness of their RM programme, identifying major problems and setting priorities for improvement. It also provides an overview of the basic components of a comprehensive RM programme. Staff of RM responsibilities may use it as a tool for planning, conducting and evaluating RM activities in their B/Ds.

(l) ***Functional Requirements of an Electronic Recordkeeping System*** (FR of an ERKS) - This publication sets out the functional requirements of an ERKS for B/Ds' compliance in developing or adopting an ERKS.

(m) ***Recordkeeping Metadata Standard for the Government of the Hong Kong Special Administrative Region*** (RKMS) and the associated implementation guidelines - This publication and the implementation guidelines set out, among others, essential recordkeeping metadata that should be created, captured, used, managed and maintained in an ERKS.

(n) ***Disposal of Original Records (for records that have been digitised and stored in a digital form)*** - This publication provides guidance for B/Ds to assess potential risks of early destruction of original non-electronic records after their digitisation.

(o) ***A Handbook on Preservation of Electronic Records*** - This publication provides guidelines for B/Ds to establish and implement a departmental preservation programme; and to adopt proper measures and practices to preserve their electronic records to meet legal and regulatory requirements, business and operational needs and evidence purpose.

1.6 Organisation

1.6.1 This Handbook comprises three parts including this introductory part. **Part II** introduces ERM principles, gives an overview of the major functions of an ERKS and explains different roles and responsibilities of ERKS users. **Part III** prescribes good practices for managing records and aggregations under the ERKS environment.

1.7 Updating

1.7.1 As good RM practices are continually evolving, this Handbook will be updated as and when necessary to keep pace with the international best RM standards and practices; and to ensure compliance with the Government's prevailing RM policy and directives.

1.8 Further information

1.8.1 This Handbook is available on CCGO (http://grs.host.ccgo.hksarg/erm/s04/4262.html) and GRS' website (https://www.grs.gov.hk/pdf/A_Handbook_on_Records_Management_Practices_and_Guidelines_for_an_ERKS(Eng_only).pdf) for reference by B/Ds.

1.8.2 Enquiries arising from this Handbook should be addressed to Senior Executive Officer (Record Systems Development)1 at 3468 6385, Senior Executive Officer (Record Systems Development)2 on 3468 6335 or Executive Officer (Record Systems Development)1 on 3468 6314.

Electronic Records Management

Part II

PART II ELECTRONIC RECORDS MANAGEMENT

This part introduces the principles of ERM and gives an overview of the major functions of an ERKS. It has three chapters -

Chapter 2	Electronic Records Management - Key Concepts
Chapter 3	Functionalities of an ERKS
Chapter 4	Roles and Responsibilities of ERKS Users

Chapter 2

Electronic Records Management - Key Concepts

2

Chapter 2: Electronic Records Management - Key Concepts

2.1 Definition of government records

2.1.1 A government record is any recorded information or data in any physical format or media created or received by a B/D during its course of official business and kept as evidence of policies, decisions, procedures, functions, activities and transactions.

2.1.2 In order to serve as evidence, a record must possess the following set of attributes and be part of the recordkeeping system that provides the necessary information to document accurately the policies, decisions, procedures, functions, activities and transactions for which the record was created or collected -

(a) **Content** - the content of a record refers to the information or idea the record contains;

(b) **Context** - the context of a record comprises the information about the circumstances in which the record is created, transmitted, maintained and used (e.g. who created it, when, to whom was it sent, why); and

(c) **Structure** - the structure of a record means the physical and/or logical format of the record, and the way parts of the record related to each other (e.g. the structure of an e-mail record covers its header, body, attachments and corresponding reply).

2.1.3 Records are an integral part of business processes and must be managed and retained for as long as they are needed to support the functions of a B/D and to provide evidence of decisions and activities.

2.1.4 It is the Government's policy to require the establishment of a comprehensive RM programme in each B/D to ensure that records as evidence of policies, decisions, procedures, functions, activities and transactions are properly kept and managed.

2.2 Qualities of a record

2.2.1 In order to serve as reliable evidence of decisions and activities, records must have qualities[12] of -

(a) **Authenticity** - an authentic record is one that can be proven (i) to be what it purports to be; (ii) to have been created or sent by the person purported to have created or sent it; and (iii) to have been created or sent at the time purported;

(b) **Reliability** - a reliable record is one whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities;

(c) **Integrity** - the integrity of a record refers to its being complete and unaltered; and

(d) **Usability** - a usable record is one that can be located, retrieved, presented and interpreted. It should be capable of subsequent presentation as directly connected to the business activity or transaction that produced it.

2.3 Electronic records

2.3.1 An electronic record means a record generated in digital form by an information system, which can be (a) transmitted within an information system or from one information system to another; and (b) stored in an information system or other medium[13].

2.4 Challenges of managing electronic records

2.4.1 Electronic records present unique challenges in RM because of -

(a) the fragility of the media (e.g. magnetic tapes and CD-ROMs) upon which they are recorded. These media are inherently unstable, requiring specific storage conditions and are highly susceptible to damage during handling and use;

(b) the dependency on technology to allow access and use. Unlike paper

[12] ISO15489-1:2001 Information and documentation – Records management – Part 1: General, paragraph 7.2.

[13] Electronic Transactions Ordinance (Cap.553), Hong Kong Special Administrative Region.

records which require no further technology to interpret the information therein, electronic records cannot be read directly without the aid of computer software and hardware to interpret the binary codes used to represent letters, numbers and figures and so on. Electronic records can be lost because they cannot be read or understood due to hardware and software obsolescence;

(c) the ease of manipulation (i.e. updated, deleted, altered intentionally or inadvertently) without being discovered; and

(d) the absence of self-evident and ready contextual information (e.g. who created it, when, to whom was it sent, why) to enable that the records are understandable and usable over time.

2.5 Need for electronic records management

2.5.1 In the era of e-government, due to the widespread use of desktop computers and communication/decision making through e-mails, a significant portion of electronic records is created and received in an unstructured computing environment where -

(a) business processes and workflows are not well defined;

(b) the user has relative autonomy over what information is created, sent, and stored (e.g. an e-mail and its attachments); and

(c) accountability for recordkeeping has not been well defined.

2.5.2 The characteristics of electronic records coupled with the unstructured computing environment may give rise to the following risks in RM -

(a) uncontrolled accumulation of records, documents and data;

(b) inadequate or incomplete keeping of records;

(c) inadvertent destruction of records;

(d) unauthorised tampering with records; and

(e) inadequate or lack of contextual information of records.

2.5.3 To deal with the challenges for managing electronic records, there is a need to develop policy, strategies and tools to ensure that government electronic records are managed properly and effectively. ERM, applying

RM principles and adopting electronic means, primarily an ERKS to keep and manage records, is a proven solution.

2.6 Hybrid records management environment

2.6.1 Although many records are created or received in digital format, non-electronic records will co-exist with electronic records for some time for various reasons, such as -

(a) paper is still the preferred medium by many people;

(b) records such as contracts, deeds, tenders, supplies or accounting records may need to be retained in their original paper format to ensure their authenticity and/or to meet regulatory or legal requirements; and

(c) non-electronic records which are inconvenient or difficult to be digitised, e.g. bulky books, oversized maps, audio/video tapes, exhibits may have to be kept in their original formats.

2.6.2 The co-existence of electronic records and non-electronic records creates a hybrid RM environment. Under this environment, it is important to maintain the links between related electronic and non-electronic records to ensure that the records are complete and the necessary contextual information is captured to facilitate understanding of the records.

2.7 Electronic recordkeeping system

2.7.1 An ERKS is an information/computer system with the necessary RM capabilities designed to electronically collect, organise, classify and control the creation, storage, retrieval, distribution, maintenance and use, disposal and preservation of records.

2.8 Anticipated benefits of ERKS

2.8.1 A properly designed and comprehensive RM programme supported by an ERKS provides ready access to relevant information about business activities, facilitates collaboration across workgroups, supports decision making and provides evidence of official transactions. These will bring about the following key benefits -

(a) better governance and greater accountability;

(b) enhanced operational efficiency and reduced cost for storing records;

(c) improved organisational compliance with legal and regulatory requirements;

(d) higher efficiency and effectiveness in managing electronic records;

(e) strengthened security and access control to records;

(f) better sharing of information; and

(g) better preservation of corporate and community memory.

2.8.2 An ERKS brings substantial tangible and intangible benefits to RMgrs and RM staff, including the following –

(a) assisting RMgrs and RM staff in complying with mandatory RM requirements as prescribed in General Circular No. 2/2009 entitled "***Mandatory Records Management Requirements***";

(b) saving manual efforts to organise, manage and maintain records;

(c) enabling automation of RM activities to enhance the overall efficiency and effectiveness in managing records;

(d) ensuring security and access control of records;

(e) supporting vital records protection;

(f) managing records retention and disposal actions in a managed, systematic and auditable manner; and

(g) facilitating the monitoring and reviewing of RM tasks and activities on an on-going basis.

2.8.3 By using an ERKS, an RU is able to –

(a) access records through desktop computers as authorised by his/her B/D;

(b) share information in a more efficient and effective way, e.g. supporting concurrent access to records;

(c) search and retrieve records speedily and easily;

(d) use authentic and complete records to conduct business and make informed decisions;

(e) obviate the need to print and file e-mail records; and

(f) use less paper.

2.9 Changing paradigm in records management responsibilities

2.9.1 In the paper-based recordkeeping environment, recordkeeping is primarily the duty of registry staff who are responsible for receiving and classifying records into the relevant files, keeping them on shelves, and retrieving and delivering the records/files to the RUs. In the ERKS environment, with the wide range of recordkeeping functions provided by the system, an RU can conveniently capture a document/e-mail which he/she created/received into the ERKS as a record by pressing some function keys and entering a few metadata about the record. Searching and retrieving records can be conveniently done by entering the keywords or browsing the file directory (i.e. the records classification scheme). Assistance from registry staff to locate and retrieve electronic records will be greatly reduced. In brief, RM will not only become a responsibility for all staff but also provide enhanced access for all users.

2.9.2 In the electronic environment, the focus of RM is less on the physical management of records but more on the planning and establishment of a sound and comprehensive framework to enable RUs to use records to carry out their duties effectively while records are properly kept to meet the short-term and long-term needs of a B/D.

2.9.3 In the circumstances, RM responsibilities have to be re-defined and re-assigned, and promulgated throughout a B/D so that all staff members are aware of their responsibilities in RM and how to take action. The roles and responsibilities of ERKS users are set out in **Chapter 4**.

Chapter 3

Functionalities of an ERKS

3

Chapter 3: Functionalities of an ERKS

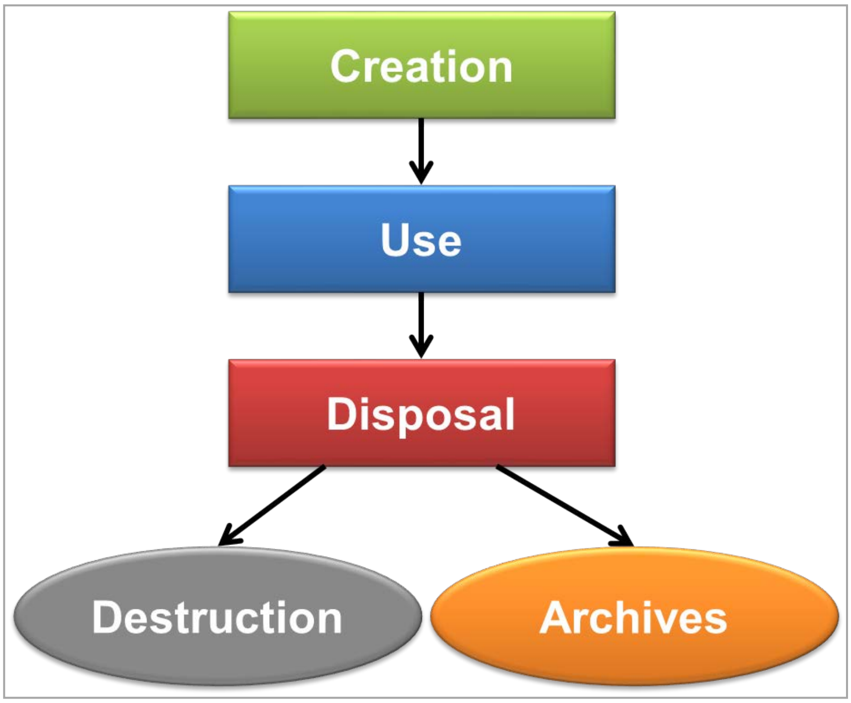
3.1 Introduction

3.1.1 An ERKS provides comprehensive RM functionalities to support efficient and effective management of electronic and non-electronic records throughout their life cycle. It could also have pre-defined workflows to support day-to-day business operations of an organisation. This chapter gives an overview of the functionalities and capabilities of an ERKS.

3.2 Records management throughout records life cycle

3.2.1 Similar to living things, a record has a life cycle that begins from record creation or receipt, through its useful life to final disposal (e.g. destruction or permanent retention as archival record). All records, electronic or non-electronic, need to be actively managed according to established rules and procedures to retain their authenticity, reliability, integrity and usability.

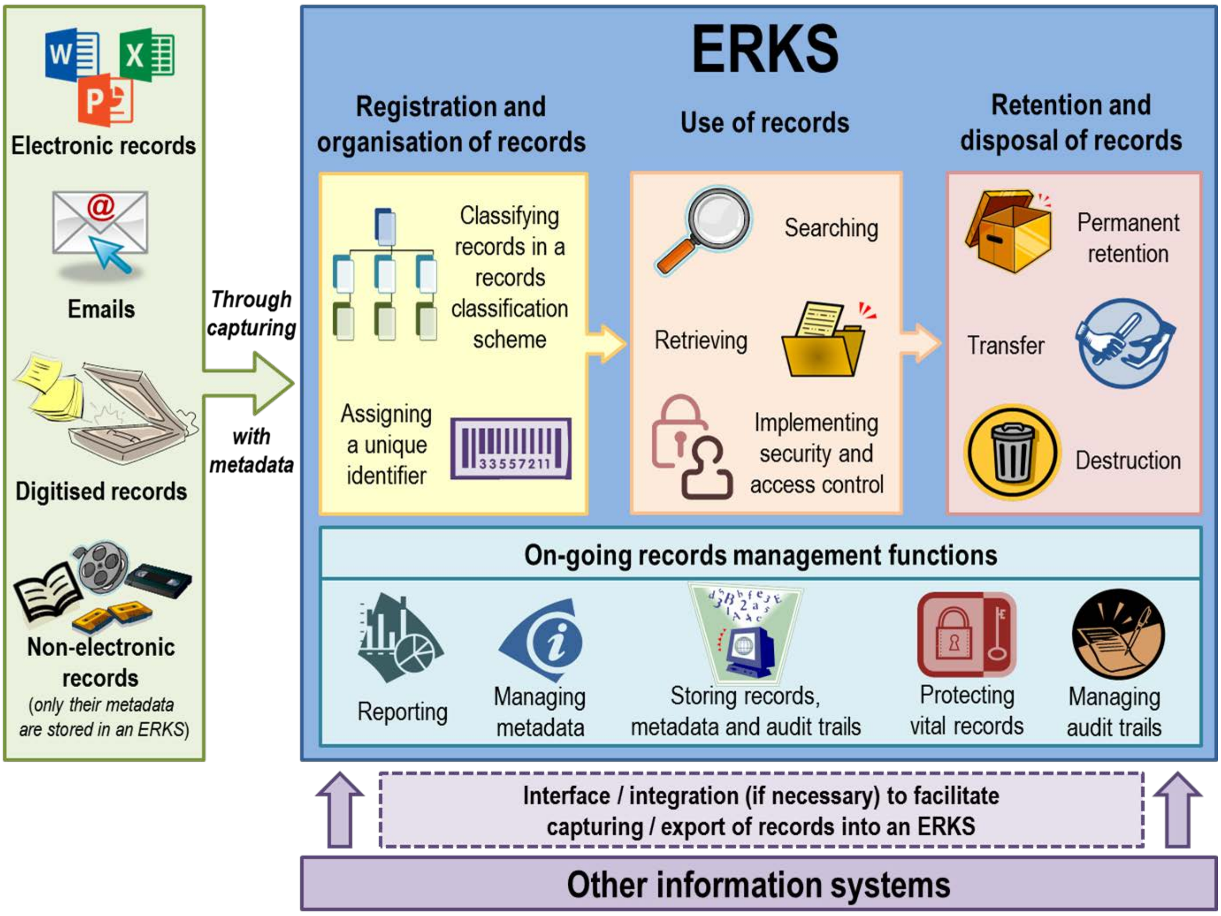
Diagram 1: Life cycle of records



3.2.2 An ERKS is capable of managing both electronic records and non-electronic records throughout the records life cycle. Electronic records can be stored in and fully managed by the system. Paper records (e.g. letters and memos) after converting to the digital form by scanning can be managed by the system as digitised records. Non-electronic records not suitable for conversion can be registered into the system under the same classification scheme and then managed by the ERKS.

3.2.3 An ERKS provides a set of functionalities for managing records stored in paper folders. These include classification, searching, tracking storage location, security and access control, handling request for retrieval of paper folders and their charge-in/charge-out, processing retention and disposal, etc. An ERKS manages electronic and non-electronic records in a coherent and consistent way.

Diagram 2: Functionalities of an ERKS


Electronic records
Emails
Digitised records
Non-electronic records
(only their metadata are stored in an ERKS)
Through capturing
with metadata
ERKS
Registration and organisation of records
Use of records
Retention and disposal of records
Classifying records in a records classification scheme
Assigning a unique identifier
33557211
Searching
Retrieving
Implementing security and access control
Permanent retention
Transfer
Destruction
On-going records management functions
Reporting
Managing metadata
Storing records, metadata and audit trails
Protecting vital records
Managing audit trails
Interface / integration (if necessary) to facilitate capturing / export of records into an ERKS
Other information systems

3.3 Capturing records

3.3.1 An ERKS is able to capture the content, context and structure of an electronic record to ensure that the record remains reliable and authentic evidence of the business transaction that it represents. It provides functionalities to capture and register electronic records in different formats (e.g. word-processed documents, spreadsheets, presentations, e-mails, images and graphics, video and audio clips) and store them in the system. **When a document has been captured into an ERKS as a record, it is no longer alterable so as to ensure its authenticity, reliability and integrity**.

3.4 Organising records through a records classification scheme

3.4.1 Records need to be classified into cognate groups, and for each group a set of records relating to the same business activity, case or subject is maintained so that the context of an individual record and the narrative of a sequence of records are preserved. An ERKS provides functionalities for organising records according to an organisation's records classification scheme to facilitate searching, retrieval, security and access control, and retention and disposal.

3.5 Recordkeeping metadata

3.5.1 An ERKS provides recordkeeping metadata (see **Chapter 7**) for each level of the records classification scheme to facilitate RM activities such as searching, retrieval, security and access control, retention and disposal, and vital records protection. Through system integration with the e-mail system of a B/D, an ERKS is capable of extracting automatically metadata elements (e.g. title and sender) from e-mails when they are captured as records.

3.6 Using records

3.6.1 An ERKS provides a set of functionalities for using records, including searching, retrieving, browsing, copying, downloading and printing subject to the appropriate security and access rights of users.

3.7 Security and access control

3.7.1 An ERKS provides robust security and access control to the system and records to protect against intentional or accidental alteration of the content, structure and context of electronic records captured and maintained by the ERKS. Users should authenticate themselves for access to the system. After successful authentication, users can only access the system functions and folders/records if they are assigned the respective rights.

3.8 Storing records

3.8.1 An ERKS provides reliable and secured storage of electronic records through security and access control and proper system management. Records and the associated metadata and audit trails should be backed up regularly.

3.9 Audit trail

3.9.1 An ERKS keeps audit trails on system events (e.g. creation of user accounts), user activities (e.g. creation of records) and actions taken on objects stored in the system (e.g. re-classification of a record) to ensure the authenticity, reliability and integrity of the records stored in the system.

3.10 Vital records protection

3.10.1 The ERKS identifies vital records[14] by labelling such records so that regular duplication, off-site protection or other suitable protection methods can be arranged and implemented.

3.11 Retention and disposal

3.11.1 An ERKS provides a set of functionalities (e.g. setting retention periods and disposal actions and disposal holds) to facilitate retention and disposal of records according to pre-defined retention and disposal schedules.

3.12 Language support

3.12.1 An ERKS supports processing (e.g. full text search) in English, Traditional Chinese and Simplified Chinese.

3.13 Management reports

3.13.1 An ERKS is able to generate different types of reports to facilitate management of records kept by ERKS, e.g. reports on inventory of folders, parts and records, users' activities, audit trails, records retention and disposal, etc.

[14] Vital records are records which are essential to the survival and continued operation of an organisation in the event of an emergency or a disaster.

3.14 Import, export and transfer of records

3.14.1 An ERKS supports import, export and transfer of records and the associated recordkeeping metadata stored in it, either in bulk or for a single record.

3.15 Workflows

3.15.1 As an optional functional requirement, an ERKS may provide pre-defined workflows[15] to automate business processes to improve efficiency in performing business and RM tasks.

[15] The Workflow Management Coalition (WfMC), an international association for developing workflow standards and interworking of different workflow systems defines workflow as “The automation of a business process, in whole or part, during which documents, information or tasks are passed from one participant to another for action, according to a set of procedural rules.” In this definition, a “participant” can be a user, a work group (i.e. a team), or a software application.

Chapter 4

Roles and Responsibilities of ERKS Users

4

Chapter 4: Roles and Responsibilities of ERKS Users

4.1 Overview

4.1.1 There are different roles under the ERKS environment. The following are typical RM roles in a B/D -

(a) DRM;

(b) ADRM;

(c) RMgr;

(d) RO;

(e) RU; and

(f) SA.

4.1.2 B/Ds may assign additional roles under the ERKS environment to meet their specific RM and business needs.

4.1.3 In assigning the roles to officers, the following considerations are relevant -

(a) officers are assigned the roles according to business needs and RM requirements. An officer may be assigned more than one of the above roles depending on the manpower deployment. It is not recommended to assign an ERKS user to perform more than two RM roles for the reason specified in (c) below;

(b) officers who are assigned the roles with access rights to classified records should meet the requirements including the "need-to-know" principle specified in the Security Regulations and the relevant guidelines; and

(c) appropriate segregation of duties and responsibilities amongst officers provides checks to minimise errors and irregularities and facilitate their early detection.

4.1.4 B/Ds should set out the responsibilities of each role clearly in their departmental handbook on ERKS RM practices and guidelines for compliance by their staff. In delineating the responsibilities of each role, B/Ds should take into account the major duties of DRM set out in the General Circular No. 2/2009 entitled "***Mandatory Records Management Requirements***" and the responsibilities of different roles set out in the B/Ds' departmental RM policy[16].

[16] According to Administration Wing Circular Memorandum No. 5/2012 entitled "***Establishment of Departmental Records Management Policy***" issued on 11 July 2012, all B/Ds should develop and establish their departmental RM policies by April 2013. B/Ds should note that the roles and responsibilities set out in their departmental RM policies may need to be realigned upon implementation of an ERKS.

Blank page

Electronic Recordkeeping Practices

Part III

PART III ELECTRONIC RECORDKEEPING PRACTICES

This part sets out good RM practices for managing records during their life cycle under the ERKS environment. The good practices cover -

Chapter 5	Creating, Capturing and Registering Records
Chapter 6	Organising Records
Chapter 7	Recordkeeping Metadata
Chapter 8	Use and Tracking
Chapter 9	Security and Access Control
Chapter 10	Storing Electronic Records
Chapter 11	Scheduling and Disposal of Records
Chapter 12	Protecting Vital Records
Chapter 13	Reporting Records Management Activities
Chapter 14	System Management
Chapter 15	Monitoring and Review
Chapter 16	Training and Support

The good practices should be adopted and adhered to in conjunction with the departmental RM procedures and guidelines developed by individual B/Ds.

Chapter 5

Creating, Capturing and Registering Records

5

Chapter 5: Creating, Capturing and Registering Records

5.1 Creating records

5.1.1 Records should be created to serve business (e.g. operational, legal and regulatory requirements), evidence and accountability purposes. They should accurately and adequately document government policies, decisions, procedures, functions, activities and transactions.

5.1.2 The creation of records should be adequate but not excessive in order to contain the growth of records because records require resources for storage and management.

5.1.3 In accordance with Administration Wing Circular Memorandum No. 4/2012 entitled "***Guidelines on Creation and Collection of Records***", B/Ds should develop business rules to document decisions as to what records are to be created and kept by B/Ds. RUs should create records in accordance with the B/D's established business rules. If in doubt, they should consult their supervisors or RM staff, e.g. RMgrs of their sections. RUs and ROs should capture records created/received in the course of business operations into the ERKS for proper management.

5.1.4 Naming conventions provide a set of rules to assist RM staff and RUs to allocate a title to a record at the time of creation and to provide a framework for naming records in a consistent manner. B/Ds should consider supplementing this Handbook with departmental guidelines on naming conventions for entitling their records to facilitate classification, searching, retrieval and consistent interpretation of business activities in the ERKS environment.

5.2 Capturing records

5.2.1 RUs and ROs should capture complete records. All elements that make up a record should be captured and linked together in a meaningful and useful manner to ensure its usability over time. For example, attachments of an e-mail should be captured with the e-mail in one go for ensuring the integrity of the e-mail record.

5.2.2 A record contains not only the content but also the structure and contextual information necessary to document an official transaction or activity. Recordkeeping metadata e.g. title and security classification associated with a record should be captured to provide contextual information on the record.

5.2.3 The capturing process involves the following steps, which are normally completed consecutively by an RU or RO. Depending on the ERKS solution adopted, the following steps may take place in a different order -

(a) capturing a record; (sections 5.2.4 to 5.4.4 below)

(b) registering a record; (section 5.5 below)

(c) classifying a record (**Chapter 6**); and

(d) inputting/capturing relevant metadata of the record (**Chapter 7**).

5.2.4 All records regardless of format should be captured into the ERKS upon creation or receipt, or as soon as practicable. Under normal circumstances, records should be captured into the ERKS within 30 days upon creation/receipt and under exceptional circumstances, records could be captured within three months. Records that are not suitable for scanning or records required to be kept in the paper format to meet regulatory/legal requirements (e.g. contracts and tender documents) should be kept and maintained in an appropriate part of a physical folder or a hybrid folder managed by the ERKS.

5.2.5 A B/D should set out departmental rules and practices and designate officers responsible for capturing records, in particular for records involving multiple recipients in the same office/unit. These departmental RM practices and guidelines for capturing records should be read in conjunction with the B/D's business rules of creation and collection of records, which sets out **what** and **when** records are created or collected, **who** to create/receive records, and **where** to keep records.

5.2.6 Capturing a document as a record in an ERKS is an irrevocable step. Once a document is captured into an ERKS as a record, it cannot be altered or deleted without proper authority.

5.2.7 If workflow is implemented in a B/D's ERKS, the workflow functions of an ERKS should be utilised as far as practicable so that records can be automatically captured. Workflow information (e.g. seeking approval/comments on a document) should be captured into the ERKS if they are qualified as records.

5.2.8 An electronic document management system (EDMS) is a computer-based application dealing with the management of documents throughout the document life cycle. The major functions of a typical EDMS include indexing, version control, storage and retrieval of electronic documents. It is an automated system used to support the creation, use and maintenance of electronically created documents for easy search and retrieval, integrate with office software packages and messaging systems, enable collaborative work, and provide access and version control over documents. An EDMS allows documents to be modified, to exist in several versions and to be deleted by their owners. Documents stored in the EDMS may not be accepted as evidence of the business of Government. Therefore, the EDMS functions are to manage documents rather than records that have evidential value. **An EDMS does not incorporate a recordkeeping function and is not designed for recordkeeping purposes. B/Ds must <u>NOT</u> use an EDMS to capture and keep records in lieu of an ERKS. Similarly, electronic systems/storage devices (e.g. shared network drives, shared directories and local hard disks) not designed for recordkeeping purposes must <u>NOT</u> be used to capture and keep records in lieu of an ERKS**.

5.2.9 Documents in an EDMS should be declared and captured as records in the B/D’s ERKS as soon as there are merits to retain them as evidence of business transactions. Documents stored in the EDMS should be declared as records by RUs in accordance with the business rules of creation of records established by B/Ds.

5.3 Capturing non-electronic records

5.3.1 Non-electronic records (e.g. paper records) should be captured into an ERKS as far as practicable by conversion into digital format through scanning taking into account operational needs and regulatory and legal requirements.

5.3.2 B/Ds should supplement this Handbook with departmental ERKS procedures and guidelines on scanning depending on the system functionalities of their own selected ERKS solution. RM staff should follow the departmental procedures and guidelines to ensure the authenticity, reliability, integrity and usability of the scanned records.

5.3.3 Although it might seem logical on efficiency grounds to destroy original paper records or other non-electronic records immediately after their digitisation and to use the digitised records in their stead, the full implications of early destruction of the original records should be thoroughly and carefully assessed to safeguard the Government's interests in accordance with the guidelines entitled ***Disposal of Original Records (for records that have been digitised and stored in a digital form)***.

5.3.4 In accordance with General Circular No. 2/2009 entitled "***Mandatory Records Management Requirements***", **B/Ds must obtain the prior agreement of the GRS Director (GRSD) before they destroy any government records, including those original paper records and digitised records.**

5.4 Handling of non-records

5.4.1 Information that does not meet the definition of government records[17] (including non-record materials, personal e-mails, etc.) should not be captured as records in an ERKS.

5.4.2 Non-record materials may include -

(a) library and museum material acquired solely for reference or exhibition purposes;

(b) stocks of publications and blank forms;

(c) drafting materials or working papers which need not be kept as records; and

(d) extra copies of records generated for convenience or personal reference, etc.

5.4.3 As set out in the ***Records Management Manual***, personal papers are documentary materials of a private nature that do not relate to or have an effect upon the conduct of official business. Such papers are excluded from the definition of government records. Example of personal papers includes, among others, personal e-mails that are not prepared or used for or circulated or communicated in the course of government business.

[17] Please see Section 2.1 of this Handbook and "***Records Management Manual***" (available on CCGO at http://grs.host.ccgo.hksarg/doc/RM_Manual.pdf) and GRS' website for definition of government records. B/Ds could also refer to "***Guidelines on Creation and Collection of Records***" issued by GRS (available on CCGO at http://grs.host.ccgo.hksarg/doc/gccr.pdf) and GRS' website (https://www.grs.gov.hk/pdf/CM_No._4_2012e.pdf) which provide further guidelines to facilitate B/Ds to adopt good practices on creation and collection of records.

5.4.4 Documents/materials, even though labelled as “personal”, “private” or with similar designation(s), if they have been used in the transaction of government business, are government records and should be kept in an ERKS properly.

5.5 Registering records

5.5.1 Registration is a way of formalising the capture of a record into an ERKS. Upon registration, the system will generate a unique identifier to each record to provide evidence that the record has been captured in the ERKS.

Chapter 6

Organising Records

6

Chapter 6: Organising Records

6.1 Organising records through records classification

6.1.1 A **logical and consistent records classification scheme** helps to place individual records in a proper context to facilitate understanding, retrieval and use; and provide an appropriate basis for security classification, access control, retention and disposal of records and protection of vital records. It is important to the successful implementation and use of an ERKS.

6.2 Records classification

6.2.1 Records classification is a systematic identification and arrangement of records into categories according to logically structured conventions, methods, and procedural rules represented in a classification system.

6.2.2 A records classification system comprises and is supported by the following -

(a) a records classification scheme[18] (also known as a file plan) drawn up by subject, organisation or function, etc.;

(b) finding aids and tools (e.g. file index and cross-referencing rules, scope notes, naming conventions/vocabulary control/thesaurus);

(c) record/file (also known as folder in the ERKS) titling and coding mechanism; and

(d) file manual[19].

6.2.3 A records classification scheme should link with records retention and disposal schedules and security and access control for consistent management of similar records on a group basis. Records retention and disposal can be automated in an ERKS. The retention and disposal schedules, if set at upper level of a records classification scheme such as the class or sub-class level, can be inherited to the lower level of the

[18] A records classification scheme is a plan or list in which records of an organisation are categorised according to its business functions and/or contents of the records and a coding system expressed in symbols (i.e. alphabetical, numerical, alpha-numerical, or decimal, etc.) that correspond to classes and sub-classes of records and are affixed to the records so categorised.

[19] It is a document which aids and controls the filing of records, explains a particular records classification system and contains details on its application, operation and maintenance.

records classification scheme such as the folder level and thus saves RMgrs' effort in managing records retention and disposal. B/Ds should therefore assign corresponding records retention and disposal schedules to the records classification scheme when developing or refining the records classification scheme.

6.2.4 Similarly, a records classification scheme should also link with security and access control for consistent management of similar records on an aggregate basis. In an ERKS, security and access control can be linked to any level of the records classification scheme. Security and access control set at the upper level of a records classification scheme could be inherited to the lower level of the records classification scheme in the ERKS environment. B/Ds should take into consideration the requirements of security and access control when developing or refining their records classification schemes for implementation in the ERKS environment. Please see **Chapter 9** for more details on security and access control in an ERKS.

6.2.5 A records classification system, in particular its key component (viz. the records classification scheme), is subject to changes to meet changing business and RM needs. As set out in General Circular No. 2/2009 entitled "***Mandatory Records Management Requirements***", **B/Ds should, among others, review their records classification schemes every two to three years.**

6.2.6 Records should be filed according to each B/D's records classification scheme. RUs should follow the relevant departmental procedures and guidelines and approach the responsible RM staff, e.g. RMgr or RO for creation of a folder or re-titling of a folder arising from business needs.

6.3 Managing records classification system

6.3.1 As the records classification system is unique for each B/D, B/Ds should supplement this Handbook with departmental RM procedures and guidelines to explain the design, structure and application of a records classification scheme to their administrative[20] and programme[21] records.

[20] As set out in General Circular No. 2/2009, administrative records are records created or received during the course of day-to-day administrative activities that deal with finance, accommodation, procurement and supplies, establishment, personnel and other general administrative activities. Records of this nature are common to all B/Ds.

[21] As set out in General Circular No. 2/2009, programme records are records created or received by a B/D whilst carrying out the primary functions, activities or missions for which the B/D was established.

B/Ds should also set out rules, practices and procedures to create, title, classify, organise and manage aggregations; and to maintain and revise the records classification scheme in an ERKS. All RM staff should adhere to the rules, practices and procedures set out in the departmental guidelines to manage the B/D's records classification system and aggregations.

Records of this nature are unique to each B/D.

Chapter 7

Recordkeeping Metadata

7

Chapter 7: Recordkeeping Metadata

7.1 What are recordkeeping metadata

7.1.1 Metadata are literally defined as "data about data". Recordkeeping metadata are data describing the context, content and structure of records and their management through time.

7.1.2 Recordkeeping metadata support RM activities by -

(a) ensuring the authenticity, reliability and integrity of records;

(b) facilitating retrieval and understanding of records;

(c) supporting the management of aggregations and records including managing the security classification of folders/records and access to them; and

(d) enabling the identification of the technological environment (e.g. the software used to create a record) in which the electronic records were created or captured and facilitating migration of records from one computer platform to another.

7.2 Different levels of recordkeeping metadata

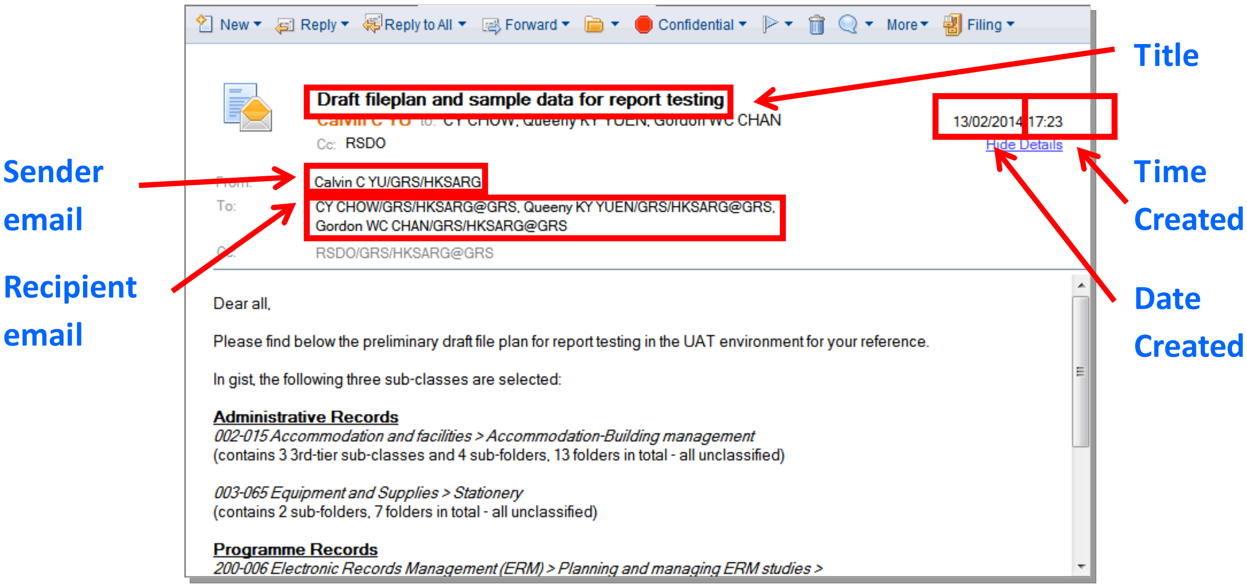
7.2.1 Recordkeeping metadata are captured at the following two levels -

(a) individual records; and

(b) aggregations (i.e. class, sub-class, folder, sub-folder or part).

7.2.2 Examples of record level metadata elements include **system identifier** (which is automatically generated by the ERKS when a record is captured), **title**, **date sent**, **creator name**, **security classification**, **date created** and **keyword**. They are useful in assisting RM staff and RUs to understand, search, retrieve and use records. For example, an RU can use the **title** or **keyword** to search for a record. Diagram 3 below illustrates some record level metadata of an e-mail record.

Diagram 3: Examples of record level metadata



Draft fileplan and sample data for report testing

Calvin C YU to: CY CHOW, Queeny KY YUEN, Gordon WC CHAN

Cc: RSDO

13/02/2014 17:23

From: Calvin C YU/GRS/HKSARG

To: CY CHOW/GRS/HKSARG@GRS, Queeny KY YUEN/GRS/HKSARG@GRS, Gordon WC CHAN/GRS/HKSARG@GRS

Cc: RSDO/GRS/HKSARG@GRS

Dear all,

Please find below the preliminary draft file plan for report testing in the UAT environment for your reference.

In gist, the following three sub-classes are selected:

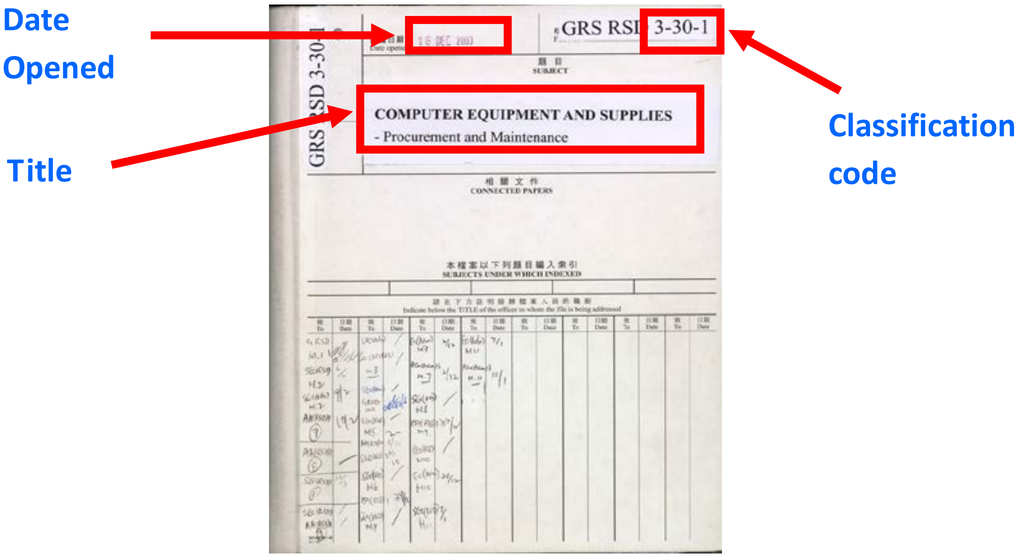
Administrative Records
002-015 Accommodation and facilities > Accommodation-Building management
(contains 3 3rd-tier sub-classes and 4 sub-folders, 13 folders in total - all unclassified)

003-065 Equipment and Supplies > Stationery
(contains 2 sub-folders, 7 folders in total - all unclassified)

Programme Records
200-006 Electronic Records Management (ERM) > Planning and managing ERM studies >

7.2.3 Examples of aggregation level metadata elements include **title, classification code**, **owner**, **security classification** and **date closed**. They are useful in the management of records on a group basis as some metadata elements of an aggregation will be inherited by its child aggregation(s) if appropriate (the inheritance principle). Diagram 4 below illustrates some aggregation level metadata of a folder.

Diagram 4: Examples of aggregation level metadata


Date Opened
Title
Classification code
GRS RSD 3-30-1
Date opened
16 DEC 2003
GRS RSD 3-30-1
題 目
SUBJECT
COMPUTER EQUIPMENT AND SUPPLIES
- Procurement and Maintenance
相 關 文 件
CONNECTED PAPERS
本檔案以下列題目編入索引
SUBJECTS UNDER WHICH INDEXED
Indicate below the TITLE of the officer to whom the file is being addressed
To
Date

7.3 Recordkeeping metadata captured for records

7.3.1 RUs or ROs input record level metadata elements during records capturing process. Some metadata elements are mandatory, e.g. **system identifier**, **creator name**, **title** and **security classification**; while some are conditional mandatory[22], e.g. **date received**, **recipient name** and **sender email**; or optional, e.g. **keyword** and **record content type**.

7.3.2 Through system integration of individual B/D's ERKS with Lotus Notes e-mail system, recordkeeping metadata of e-mail records could be captured into an ERKS automatically. Automatic capture of metadata of e-mail records not only saves RUs' or ROs' time and effort but also helps to ensure the accuracy and completeness of metadata. The capturing mode of recordkeeping metadata is set out at **Annex 3** of **RKMS**.

7.3.3 Throughout the life cycle of records, recordkeeping metadata of records may be added or updated. Normally, this responsibility is primarily undertaken by RM staff. Nevertheless, depending on the departmental ERKS RM practices and guidelines of individual B/Ds, RUs could be allowed to revise metadata if necessary, e.g. revising a mis-spelt title or add metadata such as the keyword after a record is captured into the ERKS.

7.4 Recordkeeping metadata captured for aggregations

7.4.1 RMgrs and ROs are responsible for inputting aggregation level metadata when creating an aggregation. Some metadata elements are mandatory, e.g. **title**, **classification code, owner**, **security classification** and **vital record status**; while some are conditional mandatory, e.g. **date closed**; or optional, e.g. **keyword** and **remark**.

7.4.2 RMgrs and ROs are also responsible for revising/updating aggregation level metadata if necessary after their creation.

7.4.3 A B/D is recommended to include a mapping of record and aggregation level metadata of the B/D's ERKS with RKMS in its departmental handbook on ERKS RM practices and guidelines for reference by its staff.

[22] For metadata elements which are conditional mandatory, a value must be given for these metadata elements under specific conditions. For instance, a value must be given for the metadata element "Date created" if the date for creation of a record is known.

7.5 Managing recordkeeping metadata

7.5.1 Recordkeeping metadata on records should be captured at the point of record registration and should be updated throughout the whole life cycle of records.

7.5.2 Recordkeeping metadata on records accrue on an ongoing basis. These metadata should include information on the management activities that have been or will be (e.g. scheduled disposal action and re-classification) conducted on each record.

7.5.3 Recordkeeping metadata should only be accessed and used (e.g. search and print) by authorised users. In an ERKS, this should be integrated with its security and access control arrangements. The security and access control, and storage of metadata should be aligned with those of the associated records and folders (or any aggregations of records).

7.5.4 Recordkeeping metadata should only be updated/changed by authorised users under well-defined rules (see sections 7.3 and 7.4). Any updating/changes should be documented (e.g. through audit trail).

7.5.5 Metadata should be consistently and persistently linked to the records over time.

7.5.6 Some metadata elements (e.g. **title**, **classification code**, **security classification**, **owner** and **date disposed**) are retained and managed beyond the life of the associated aggregations so as to keep a record of the disposed or transferred records.

7.5.7 Metadata should be reviewed regularly to meet RM and business needs, e.g. the change of business processes may induce addition/deletion of metadata element(s). The results of the reviews and any subsequent changes to the sets of metadata should be properly documented.

7.6 Mapping of recordkeeping metadata

7.6.1 A mapping of recordkeeping metadata of a B/D's ERKS with the recordkeeping metadata specified in RKMS helps RM staff to maintain recordkeeping metadata of the B/D's ERKS in accordance with the Government's requirements on recordkeeping metadata. The list of recordkeeping metadata specified in RKMS is available at **Annexes 1 and 3** of **RKMS**, which is also available at **Appendices 3 and 4** of **FR of an ERKS.**

7.6.2 B/Ds should prepare a mapping table to map the recordkeeping metadata implemented in their ERKS with the recordkeeping metadata specified in RKMS for reference by users to facilitate the retrieval of the recordkeeping metadata. Example of the mapping table is provided below as a guide for B/Ds.

Metadata configured in an ERKS		Metadata specified in RKMS		Obligation level as specified in RKMS
Name	Location in the ERKS	Name	Definition	
Aggregation level metadata in a B/D's ERKS				
[E.g. Classification code]	[E.g. Aggregation Metadata under **Categories** tab]	Classification code	The classification code applied to an aggregation or a stub	Mandatory
...	...	...	...	...
Record level metadata in a B/D's ERKS				
[E.g. Created]	[E.g. **General** tab]	Date time captured	The date and time at which the record was captured in an ERKS	Mandatory
...	...	...	...	...
Metadata specified in RKMS which has not been implemented in a B/D's ERKS *(Note: For the sake of completeness, B/Ds are recommended to set out the metadata elements which are* ***not mandatory*** *as specified in the RKMS and have* ***not*** *been implemented in a B/D's ERKS as the B/D does not have such operational need in a mapping table as shown below. For example, if the metadata "Description" is not implemented in an ERKS, it is recommended to set out this metadata in the following table.)*				
N/A	*N/A*	Description	A free-text description of the entity	Optional
...	...	...	...	...

Chapter 8

Use and Tracking

8

Chapter 8: Use and Tracking

8.1 Use of records

8.1.1 Depending on the security and access control of the ERKS, RUs can use the following functionalities subject to their access rights to the respective aggregations and records -

(a) capture a record;

(b) search an aggregation and/or a record and their recordkeeping metadata;

(c) browse a records classification scheme (i.e. the folder structure in the ERKS);

(d) retrieve and browse a record via a native application or a universal viewer (if implemented);

(e) download single/multiple records into local hard disk;

(f) copy a record to another folder;

(g) cross-reference a record and view records under cross-reference;

(h) browse metadata of an aggregation and/or record including cross-reference;

(i) print records and their associated recordkeeping metadata; and search results;

(j) request retrieval of a physical part of a physical folder or a physical part of a hybrid folder;

(k) *(if workflow is implemented)* trigger a workflow and attach record(s) in the workflow; and

(l) *(if workflow is implemented)* be a receiver of a workflow and take action assigned in the workflow.

8.2 Managing the use of records

8.2.1 Access to and use of the records and the relevant system functions should be permitted in accordance with an officer's pre-defined roles and responsibilities. In an ERKS, this should be tightly integrated with its security and access control.

8.2.2 An ERKS possesses functionality to support a user to reserve, charge-out and charge-in a physical part of a physical folder, a physical part of a hybrid folder or a non-electronic record managed by an ERKS (e.g. through automatic notification to ROs). Access to non-electronic records stored in a physical part of a physical folder or a physical part of a hybrid folder should be managed by an ERKS. RUs should request retrieval of a physical part of a physical folder or a physical part of a hybrid folder via an ERKS while ROs should register the charge-in and charge-out of the physical part in an ERKS.

8.2.3 If workflow is implemented, automated workflows should be adopted to facilitate the use of records in business processes as far as practicable.

8.3 Tracking use of records by audit trails

8.3.1 Audit trails are data which allows the reconstruction of a previous activity, or which enables attributes of a change (such as date/time, operator (i.e. responsible user)) to be stored so that a sequence of events can be reconstructed in their correct chronological sequence[23].

8.3.2 Audit trails provide a historical record on all significant events associated with the stored records and an ERKS. As part of the security and access control, system and folder/record activities should be tracked and documented through audit trails and metadata.

8.3.3 Audit trail data should, as far as practicable, be generated automatically by the system. An ERKS must automatically capture and keep unalterable audit trails about type of actions, including but not limited to those listed at **Appendix 5** of **FR of an ERKS** which is reproduced below -

[23] The National Archives of UK: Requirements for Electronic Records Management Systems - Reference Document.

Item	Actions
Creation, Use and Modification of Records Classification Scheme and Aggregations	
(1)	Creation of aggregations
(2)	Access and use of aggregations, including but not limited to close and re-open folders/parts
(3)	Changes made to the records classification scheme, e.g. merging of two records classification schemes and re-classification of aggregations
Capturing, Access and Use of Records	
(4)	Capturing of records
(5)	Access and use of records, including but not limited to read, charge-out, charge-in, render, print and download records
(6)	Re-classification of records
Security and Access Control	
(7)	Changes made to the access rights and security clearance of a user, user group or user role
(8)	Changes made to the security classification of aggregations and records
(9)	Export, transfer and purge of audit trail data
(10)	Where applicable, track any attempted violations of access control of the ERKS (i.e. a user's attempts to access a record or an aggregation to which he is denied access)
(11)	Creation, amendment or deletion of a user, user group or user role
Records Retention and Disposal	
(12)	Application of retention and disposal schedules to aggregations and records therein and changes of the application
(13)	Changes made to any retention and disposal schedules
(14)	Retention and disposal review actions carried out by an authorised individual
(15)	The placing or removal of a disposal hold on aggregations and records therein
(16)	Disposal action of aggregations and records [Note: Deletion is also included.]

Item	Actions
(17)	Export and transfer of aggregations, records and metadata
Recordkeeping Metadata	
(18)	Changes, including creation, addition, modification and deletion of any metadata and/or metadata values associated with aggregations, records and other entities [Note: Changes should include actions taken by a user and an authorised individual.]
Administration	
(19)	Changes made to administrative parameters, e.g. reconfigure the audit trails [Note: It should never be possible to turn off the auditing of changes to audit trail parameters so that the ERKS does not record in the audit trails who changed them and when.]
(20)	Indication that selected aggregations (or part of an aggregation) and records are considered to be vital records
(21)	Indication that selected aggregations (or part of an aggregation) and records previously designated as vital records are no longer considered to be vital records

8.4 Managing audit trails

8.4.1 Audit trails should be comprehensively and properly managed. If any part of an audit trail can be maliciously or inadvertently altered, then the whole audit trail may be discredited and the integrity of the records held within the system may also be challenged.

8.4.2 Audit trails have to be stored properly at an appropriate level of security to prevent any change to their data.

8.4.3 Audit trail data should be stored for at least as long as the record to which it refers.

8.4.4 Access to the audit trail information should be restricted to authorised persons only. Responsibility for managing audit trails should be properly set out and documented in the departmental handbook on ERKS RM practices and guidelines.

8.4.5 An ERKS supports SAs and other authorised persons to run audit trail reports to monitor system activities and identify irregularities.

Chapter 9

Security and Access Control

9

Chapter 9: Security and Access Control

9.1 Objectives

9.1.1 Security and access control should be established and implemented to protect the security and integrity of records stored in an ERKS. It should ensure that -

(a) aggregations and records and the associated metadata, and audit trails, etc. are protected from tampering, unauthorised intervention and data loss;

(b) aggregations and records and the associated metadata are protected according to the relevant security classifications as stipulated in the Security Regulations;

(c) aggregations and records and their associated metadata are only accessible by authorised users; and

(d) system functions are only accessible by authorised users.

9.2 Considerations in establishing security and access control

9.2.1 In implementing security and access control in an ERKS, the following considerations are relevant -

(a) Security Regulations and relevant guidelines on classified information, including the "need to know" principle in disseminating classified information, technical requirements in respect of storage, processing and transmission of classified information;

(b) Government IT security related regulations, policies and guidelines including departmental IT security policies and guidelines;

(c) users' needs on accessing folders/records (including any aggregations of records);

(d) users' needs on accessing various system functions according to their roles and responsibilities in RM; and

(e) the advantages of records sharing. Undue restriction on records access will limit the benefits generated from records sharing.

9.3 Security and access control of an ERKS

9.3.1 For effective access control management, a standard set of permitted system functions for different roles of an ERKS (viz. DRM, ADRMs, RMgrs, ROs, RUs and SAs) is recommended to be set up according to their roles and responsibilities.

9.3.2 An ERKS deals with the security and access arrangements in a structured way on the following -

(a) security classification for each aggregation and record;

(b) the rights of each user or user group to access aggregations and records having regard to their respective security clearance; and

(c) the rights of each user or user group to access different system functions for aggregations.

9.3.3 Security and access control of records in a B/D has a close linkage with its records classification scheme as an effective records classification scheme should facilitate and support implementation of security and access control at all levels of the records classification scheme depending on the business needs. For example, the access control of programme records for one section of a B/D could be established at class level while the access control of some administrative records which are for shared use by different sections could be set at folder level. B/Ds should take into account the requirements of security and access control when developing or refining their records classification scheme for implementation in the ERKS environment.

9.3.4 Under the hybrid RM environment, the ERKS security and access control is applicable to aggregations and electronic records stored in the ERKS and physical folders, sub-folders, parts and non-electronic records stored outside the ERKS but are under its management.

9.3.5 For efficient and effective management, it is recommended that users be grouped into different user groups for the purpose of managing their access rights. Users who have the same access rights to folders or sub-folders or users with the same RM role should be grouped into the same user group.

9.3.6 As a user’s access rights to aggregations are normally linked with his/her post, B/Ds may create a user group for each post for effective management. These single-user groups form larger user groups according to the principles mentioned in paragraph 9.3.5 above. Under this arrangement, change of access rights arising from the change of the incumbent of a post can be effected through replacing the outgoing officer with the incoming officer as the member of the single-user group once, irrespective of the number of user groups linked with the post. This will minimise maintenance effort.

9.4 Managing security and access control

9.4.1 Due to the importance of security and access control, B/Ds should establish a mechanism to co-ordinate to monitor and review such control. All the relevant activities should be properly documented in order to demonstrate that sufficient control is in place to ensure the overall security and integrity of the system.

9.4.2 B/Ds should supplement this Handbook with departmental procedures and guidelines to facilitate management of security and access control. The procedures and guidelines should set out clearly the roles and responsibilities of different roles in management of security and access control, and the procedures for at least the following activities -

(a) Change in security classification of records;

(b) Change in security classification of aggregations;

(c) Changes in access rights of users and user groups to an aggregation; and

(d) Changes in users and user groups.

9.4.3 The security and access control should be regularly monitored and reviewed to cope with changing situations (e.g. addition/deletion of users, changes of responsibilities of users, changes to the records classification scheme, changes of security classification of folders/records).

9.4.4 Regular security risk assessments and audits should be performed for an ERKS to ensure the overall system security and integrity in accordance with OGCIO’s guidelines. A security risk assessment should also be performed before production, and prior to major enhancements and changes associated with the system.

Chapter 10

Storing Electronic Records

10

Chapter 10: Storing Electronic Records

10.1 Storage requirements and arrangements

10.1.1 The selection of storage media, storage system, storage environment and handling procedures of an ERKS should be based on the business and RM considerations such as the quantity and growth rate of records, characteristics of storage systems/media, records security needs, use of records, retrieval requirements, preservation need, relative cost of records storage options and backup systems.

10.1.2 ***A Handbook on Preservation of Electronic Records***[24] sets out good practices for preserving electronic records, e.g. tips for addressing media durability and proper handling of storage media. The publication also provides guidelines for B/Ds to establish and implement a departmental preservation programme which should include practices and procedures to refresh storage media and migrate electronic records from the existing ageing IT systems to upgraded systems.

10.1.3 The hardware and software of the ERKS should be installed at a location meeting various government standards and guidelines, industry standards and other related requirements.

10.1.4 Physical/system security in respect of storage and handling of classified records (including the associated metadata and the relevant backups) stored in the ERKS and in other digital media should meet the requirements set out in Security Regulations and Baseline IT Security Policy (S17), IT Security Guidelines and any equivalent. Proper documentation should be maintained to demonstrate that sufficient physical/system security arrangements for records storage/handling are in place to ensure that the records have not been tampered with.

10.1.5 Advice from the departmental IT security officers is necessary in respect of the technical aspects of storing electronic records.

10.1.6 As the costs of hardware services increase as the quantity of records stored in an ERKS grows, B/Ds should monitor the storage of records and

[24] The handbook is available at GRS' ERM themepage on CCGO (http://grs.host.ccgo.hksarg/erm/s04/461.html) and GRS' website (https://www.grs.gov.hk/pdf/A_Handbook_on_Preservation_of_Electronic_Records_(July_2013)(Eng_only).pdf).

arrange timely disposal of time-expired records to control the growth of records.

10.2 Backup

10.2.1 B/Ds should set up a programme to backup aggregations, records, recordkeeping metadata and other system data of an ERKS regularly to prevent their loss or damage. This programme can be integrated with routine system maintenance and vital records protection programme / disaster recovery plan / business continuity plan. The programme and backup schedules should be properly documented.

10.3 Review and proper documentation

10.3.1 The storage requirements and arrangements should be regularly reviewed to meet RM and business needs (e.g. growth of records and advancement of technology).

10.3.2 Proper documentation should be maintained by B/Ds on the storage arrangements to facilitate routine monitoring, refreshment, migration and review.

Blank page

Chapter 11

Scheduling and Disposal of Records

11

Chapter 11: Scheduling and Disposal of Records

11.1 What is records scheduling and disposal

11.1.1 Records accumulate and grow in the course of business. If records are not properly and systematically disposed of, useful and unwanted records will mix together making records retrieval difficult and time-consuming and impeding operational efficiency. Furthermore, storage and handling of records take up considerable resources.

11.1.2 General Circular No. 2/2009 entitled "***Mandatory Records Management Requirements***" stipulates that B/Ds should arrange retention and disposal of records in accordance with requirements specified in the GARDS for administrative records and the retention and disposal schedules established for programme records.

11.1.3 Records scheduling is the action of developing records retention and disposal schedules which specify the duration that records should be retained (i.e. retention period) and the disposal arrangement (i.e. transfer to records centres, permanent preservation, destruction, etc.).

11.1.4 Under the hybrid RM environment, records scheduling and disposal should cover both electronic records and non-electronic records managed by an ERKS.

11.2 Authority of records scheduling and disposal

11.2.1 GRS has the overall responsibility for authorising the disposal of government records regardless of formats through approving records disposal requests and records disposal schedules, and issuing disposal authority or agreement.

11.2.2 No government records are to be destroyed without the prior agreement of the GRSD.

11.2.3 Records (including the associated metadata and other relevant information as required by GRS) appraised to have archival value should be transferred timely to the Public Records Office of GRS for permanent retention.

11.2.4 DRM of the B/D should establish and implement records retention and disposal schedules in consultation with the relevant business units.

11.3 Drawing up disposal schedules

11.3.1 Records disposal should be implemented on a group basis (e.g. folders are grouped into records series). Records retention and disposal schedule(s) for newly created aggregations (if they are not covered by existing approved records retention and disposal schedules) should be drawn up as early as possible[25].

11.3.2 The procedures and requirements for disposing of administrative records and programme records are different. In disposing of administrative records, B/Ds should follow the requirements set out in the GARDS.

11.3.3 B/Ds should draw up disposal schedules for programme records based on the following criteria -

(a) administrative, operational, financial and legal requirements; and

(b) archival value as advised by GRS.

11.3.4 B/Ds are recommended to make reference to the following steps in drawing up a records retention and disposal schedule -

(a) conduct a records survey to take inventory of the concerned records (e.g. type and nature, security classification/level, quantity, growth rate);

(b) group records into records series taking into account the characteristics of the records (e.g. created or received for what functions or activities, how records are classified, physical format);

(c) identify disposal classes within the series to group similar records (in terms of functions, content, and retention value) in a records series that merit the same disposal arrangement;

(d) identify the retention value of each disposal class and determine criteria for defining records as inactive (e.g. after actions completed, after file closed);

(e) propose retention periods of the disposal class(es) based on the administrative, operational, financial and legal requirements;

[25] General Circular No. 2/2009 stipulates that B/Ds should forward draft disposal schedules to GRS for approval within two years upon creation of new records series.

(f) propose suitable disposal action(s); and

(g) complete documentation including Records Inventory Form (RMO1) and Records Retention and Disposal Authority (RMO2) and forward the schedule to Records Management Administration Office of GRS for agreement.

11.3.5 For more information on the procedures, B/Ds may refer to GRS' RM Publication No.1 - ***A Practical Guide to Records Scheduling and Disposal***[26].

11.3.6 The process of records scheduling should be properly documented.

11.3.7 The disposal schedules approved by GRS should be properly kept in the ERKS.

11.4 Retention period and inactive records

11.4.1 Retention period means the time the records are to be kept after the records become inactive but before their final disposal. This concept applies to both electronic and non-electronic records.

11.4.2 According to the ***Records Management Manual*** published by GRS, inactive records are those records which are no longer or rarely required for action or reference. As a general yardstick, records are inactive if they have not been referred to for two years. This yardstick may be varied or re-defined according to individual office's operational consideration. B/Ds should supplement this Handbook with specific departmental ERKS RM guidelines and procedures having regard to the system functionalities of their ERKSs for their RM staff to trigger the commencement of the approved retention period in their ERKSs.

11.5 Disposal action

11.5.1 B/Ds should propose the disposal action for the concerned inactive records upon the lapse of the specified retention period for agreement by GRS when drawing up retention and disposal schedules. Such disposal actions include destruction, microfilming, permanent retention by B/D, transferring to GRS for permanent preservation, etc.

[26] GRS RM Publication No. 1 is available on CCGO (http://grs.host.ccgo.hksarg/file/2.4.1_P1.pdf) and GRS' website (https://www.grs.gov.hk/pdf/P1(2019-01)(Eng_only).pdf).

11.6 Disposal schedules and general procedures on records disposal

11.6.1 Disposal schedules should be integrated with the records classification scheme(s) as explained in **Chapter 6**. For example, an approved disposal schedule should be linked with the relevant folders (or any aggregations of records) of an ERKS for implementation on a group basis.

11.6.2 Records should be retained and disposed of according to the approved retention period and disposal action set out in the relevant disposal schedules. Arrangement should be in place to trigger regular disposal of records managed by the ERKS according to approved disposal schedules in a timely manner. As stipulated in General Circular No. 2/2009 entitled "***Mandatory Records Management Requirements***", **B/Ds should dispose of time-expired records at least once every two years for all their administrative records, which are covered by GARDS, and for all their programme records with approved disposal schedules**.

11.6.3 An ERKS should implement records disposal under proper control. Only authorised users, e.g. RMgrs and ROs should be allowed to access the records disposal related system functions of the ERKS. **No records should be disposed of automatically in the ERKS even though they have fulfilled the approved retention period.**

11.6.4 To facilitate records disposal, as a good practice, a part of a folder in an ERKS should be closed when the corresponding paper file for keeping the non-electronic records has become too bulky, the subject matter is completed and further action is not likely, or the folder has been opened for more than five years, whichever is earlier. In an ERKS, to ensure better system performance, B/Ds should close a part of a folder when the number of records reach a pre-defined number set by the B/Ds, e.g. 400 records in a part. B/Ds should review those parts of folders which are inactive but remain unclosed to see whether they should be closed and then disposed of. It should be noted that all Government records reaching 30 years old should be appraised by PRO to determine whether or not they possess archival value for permanent retention.

11.6.5 When applying the retention and disposal requirements of GARDs to administrative records or approved disposal schedules to programme records, B/Ds should examine whether records of different retention and disposal requirements have been mingled together or whether administrative records have been mixed with programme records in the same part of folder in the ERKS. If either situation occurs, B/Ds should adopt the principles set out in paragraphs 3.4.5 to 3.4.6 of GRS' Records Management Publication No. 1 "***A Practical Guide to Records Scheduling And Disposal***" to determine the retention periods and disposal actions of the records.

11.6.6 B/Ds should establish procedures and guidelines to handle records disposal. If appropriate, these procedures could be implemented through a pre-defined workflow. The procedures should include the following -

(a) a responsible officer (e.g. RMgr) of the respective office to identify time-expired records that are due for disposal;

(b) a responsible officer (e.g. the subject officer) to conduct a review on the concerned records to confirm whether the records are ready for disposal;

(c) a responsible officer in the respective office be appointed to endorse the actual disposal subject to GRSD's prior agreement;

(d) a responsible officer (e.g. RMgr) of the respective office to seek prior agreement from GRSD to the actual disposal;

(e) a responsible officer (e.g. RMgr) of the respective office to ensure that all relevant records, including non-electronic records stored in paper folders, associated metadata and the respective backups are disposed of accordingly;

(f) a responsible officer (e.g. RO) of the respective office to ensure that selected metadata (e.g. title, classification code and date disposed) are retained in the ERKS; and

(g) proper documentation of the disposal arrangement (e.g. the workflow record relating to the disposal authorisation process).

11.6.7 Classified records (including the associated metadata) and data should be destroyed according to the provisions set out in the **Security Regulations**.

11.6.8 B/Ds should temporarily suspend (i.e. through a disposal hold) the disposal action for the concerned records to meet ad-hoc retention requirement, e.g. a discovery of documentary evidence in a court case. Disposal action should be resumed after meeting the ad-hoc retention requirement. The whole process should be properly documented.

11.7 Disposal of electronic records

11.7.1 Destruction of time-expired electronic records should ensure that the concerned records, associated metadata and backups are irrecoverable.

11.8 Review of disposal schedules

11.8.1 To meet current business needs and other new requirements, all disposal schedules should be reviewed at least **once every 5 years** or more often to determine whether amendments are required.

11.8.2 B/Ds should document the review result for future reference. If any amendments are proposed, they should approach GRS for agreement.

Chapter 12

Protecting Vital Records

12

Chapter 12: Protecting Vital Records

12.1 Vital records

12.1.1 Vital records are records that contain information essential to the survival and continued operation of a B/D in the event of an emergency or a disaster.

12.1.2 Protecting vital records can reduce the risks of records disaster, ensure that the organisation has adequate information to resume operation during and after a disaster as well as to limit the extent of damage and loss.

12.1.3 B/Ds should refer to GRS' RM Publication No. 6 - ***Manual on Vital Records Protection***[27] for details on establishing a vital records protection programme. This chapter focuses on issues relating to protection of vital electronic records stored and managed in an ERKS.

12.2 Protection of vital electronic records

12.2.1 Electronic records and data stored on digital storage devices can be more susceptible to damage than other record formats. Relatively minor damage to digital storage devices or electricity power failure may render all information contained in a storage device inaccessible. Restoration of vital electronic records should be accorded a high priority in the business continuity plan as delays in recovery may result in delay in resumption of essential operations.

12.2.2 Vital records should be proactively identified. An ERKS provides labelling of vital electronic and non-electronic folders/records to mark vital records for protection.

12.2.3 One way of protecting vital electronic records is to duplicate the records and the associated metadata by backup and maintain the duplicated records in secure and suitable off-site storage. The relative ease with which electronic records can be duplicated and the low cost of digital storage makes this strategy effective and affordable. The off-site storage should always be at a sufficient distance from the ERKS servers so that the vital records can have better protection from the effects of the same

[27] GRS' RM Publication No. 6 is available on CCGO (http://grs.host.ccgo.hksarg/file/2.4.6_P6(2017-08).pdf) and GRS' website (https://www.grs.gov.hk/pdf/P6(2017-08)(Eng_only).pdf).

disaster.

12.2.4 If vital records protection is to be implemented through backup, B/Ds should carefully devise their backup strategy (e.g. coverage and frequency).

12.2.5 Systems and application software and documentation, access codes, passwords, serial numbers and other relevant information which are necessary for accessing vital records stored off-site in an emergency or a disaster should be properly maintained in a safe and secure location.

Blank page

Chapter 13

Reporting
Records Management Activities

13

Chapter 13: Reporting Records Management Activities

13.1 Records management reporting

13.1.1 An ERKS supports production of statistical and descriptive reports through pre-defined report templates and ad-hoc enquiry to facilitate planning, execution and monitoring of RM activities under the ERKS environment. These reports may be generated on a regular or need basis.

13.1.2 Pre-defined RM reports mainly cover the following RM activities -

(a) managing an organisation's records classification scheme and records inventory (e.g. list of folders, no. of folders, parts and records);

(b) managing recordkeeping metadata;

(c) planning and managing records scheduling and disposal (e.g. retention periods of folders, disposal action put on hold);

(d) managing security and access control (e.g. information on users or user groups having access rights to selected folders);

(e) monitoring users' activities and audit trail data;

(f) tracking the movement and location of non-electronic records; and

(g) monitoring export of records.

13.1.3 Management reports with sensitive information should be classified according to Security Regulations, as appropriate.

13.1.4 B/Ds should list out the pre-defined RM reports in their ERKSs with brief description in their departmental handbooks on ERKS RM practices and guidelines.

Chapter 14

System Management

14

Chapter 14: System Management

14.1 Proper system management

14.1.1 An ERKS should be properly operated and maintained to ensure the authenticity, integrity, reliability and usability of records kept in the system. Improper system functionality or malfunction may put the integrity or authenticity of a record into doubt.

14.1.2 System administration rights should be properly established, documented and maintained, and regularly reviewed to meet RM and business needs.

14.1.3 System security (including data transmission) should be properly controlled and maintained, and regularly reviewed according to Security Regulations, Baseline IT Security Policy, IT Security Guidelines, departmental IT security policies and guidelines and any equivalent.

14.1.4 All system management and maintenance activities should be properly documented to demonstrate and prove that the system is operating as intended at all times in accordance with the organisation's normal business practices, system's technical specification and performance specification.

14.2 Business continuity plan

14.2.1 The system availability and stability should be properly managed and monitored to meet business needs. B/Ds should develop business continuity plan for ERKS system failure having regard to the specific needs of individual B/Ds.

14.2.2 B/D should develop a disaster recovery plan to deal with system failure.

14.3 Arrangements in case of outsourcing

14.3.1 If the maintenance of an ERKS is outsourced to a service provider, proper security management processes have to be defined and included in the outsourcing service specification to protect the data as well as to mitigate the security risks associated with outsourced IT projects/services.

14.3.2 The security roles and responsibilities of the service provider should be clearly defined and documented by B/Ds. B/Ds should note that the overall responsibility of the system management and maintenance rests with the B/Ds concerned though the maintenance of the ERKS is outsourced to a service provider.

Blank page

Chapter 15

Monitoring and Review

15

Chapter 15: Monitoring and Review

15.1 Importance of monitoring and review

15.1.1 Regular monitoring and review help ensure that records managed by the ERKS will be accepted as evidence in a court of law. Through regular monitoring, B/Ds will be ready to provide evidence to demonstrate that records stored in the ERKS are authentic, reliable and complete.

15.2 Areas of monitoring

15.2.1 The monitoring should cover the following areas -

(a) compliance with the established Government's and departmental RM policy, practices and guidelines;

(b) compliance with the established Government's and departmental IT security policy, practices and guidelines;

(c) proper functioning of the ERKS and regular maintenance as scheduled; and;

(d) any irregularities and malpractices, e.g. loss of records and unauthorised destruction of records.

15.3 Implementing monitoring

15.3.1 B/Ds should adopt a systematic monitoring approach and develop a departmental monitoring mechanism for on-going review and monitoring of the ERKS. B/Ds should appoint an officer (e.g. DRM or a directorate officer) to oversee and co-ordinate the departmental monitoring programme with the assistance of other responsible officers.

15.3.2 To assist B/Ds in planning, executing and reviewing the departmental monitoring programme, a four-step approach: Plan, Act, Check and Review is recommended.

15.3.3 Step 1: Plan. B/Ds should carefully plan the departmental monitoring programme. The departmental monitoring programme may include generating RM reports, verifying documentation, calling regular returns and reports, checking audit logs and conducting surprise checks and surveys on usage of ERKS.

15.3.4 Step 2: Act. Once the departmental monitoring programme is largely formulated, B/Ds should perform tasks and activities according to the departmental monitoring programme. Procedures and results of the review and checking shall be properly documented. B/Ds should take immediate actions if any irregularities or improvement areas are identified. The remedial actions taken should be properly documented.

15.3.5 Step 3: Check. B/Ds should monitor the effectiveness of their departmental monitoring programme on an on-going basis.

15.3.6 Step 4: Review. B/Ds should review and revise the departmental monitoring programme on regular intervals, say once every two years or as and when necessary having regard to the prevailing RM and operational needs, RM and IT requirements and ERKS operations.

15.4 Records Management review

15.4.1 In accordance with General Circular No. 2/2009 entitled "***Mandatory Records Management Requirements***", B/Ds should review their RM practices regularly to ensure that their RM programme is functioning effectively. General Circular No. 5/2012 entitled "***Records Management Review***" sets out that GRS will continue to coordinate self-assessment RM review exercises of B/Ds on a regular basis (e.g. once every two to three years).

15.4.2 B/Ds should conduct regular RM reviews on the departmental RM programme to ensure that it meets current RM and business needs. The review should have regard to the RM policy, practices and guidelines, and the scope includes classification scheme(s), records retention and disposal, operation and maintenance of ERKS.

15.4.3 It is recommended to assign the DRM of individual B/D to oversee and co-ordinate the RM reviews.

Blank page

Chapter 16

Training and Support

16

Chapter 16: Training and Support

16.1 Importance of training

16.1.1 RM under the ERKS environment involves a paradigm shift. It is important to put in place suitable training programme to promote a proper RM culture in a B/D, to ensure compliance with the departmental policies, practices and procedures in RM and to facilitate understanding of the ERKS functions.

16.2 Personnel to be trained

16.2.1 All staff and any personnel who are required to perform RM duties need to receive appropriate training.

16.2.2 B/Ds are recommended to provide new staff with the necessary ERKS training as part of their induction training so that they are competent to perform their RM roles and responsibilities.

16.2.3 As on-going training, B/Ds are also recommended to conduct refresher training on a regular basis to familiarise staff with RM practices and operation of ERKS.

16.3 Coverage of training

16.3.1 The training should cover the following four areas -

(a) departmental RM policies;

(b) ERKS RM practices and guidelines;

(c) records classification system of the B/D (see Section 6.2.2); and

(d) use of ERKS application.

16.3.2 Continuous training should be provided to cope with changing RM and business needs (e.g. change of the classification scheme due to addition of new business unit/function, addition of new functions to the ERKS) and to promote awareness on the importance of RM among staff.

REFERENCES

REFERENCES

This Handbook has been developed with reference to the following General Circulars, Administration Wing Circular Memoranda, RM publications promulgated by GRS and international standards -

1. General Circular No. 5/2006 entitled "***Management of Government Records***" - This circular reminds heads of B/Ds of the importance of proper management of government records and draws their attention to good RM practices.

2. General Circular No. 2/2009 entitled "***Mandatory Records Management Requirements***" - This circular sets out mandatory requirements on the management of government records.

3. General Circular No. 5/2012 entitled "***Records Management Reviews***" - This circular sets out the framework for reviewing the RM practices in B/Ds and the details of departmental RM reviews to be conducted by GRS.

4. Administration Wing Circular Memorandum No. 4/2012 entitled "***Guidelines on Creation and Collection of Records***" - This circular memorandum provides supplementary guidelines on creation and collection of records to assist B/Ds to enhance their records management practices.

5. Administration Wing Circular Memorandum No. 5/2012 entitled "***Establishment of Departmental Records Management Policies"*** - This circular memorandum provides guidelines for B/Ds to formulate their departmental RM policies.

6. ***Records Management Manual*** - This publication provides guidance and instructions for proper and coordinated management of government records.

7. GRS' RM Publication No. 1 "***A Practical Guide to Records Scheduling and Disposal***" - This publication provides a detailed procedural guide on drawing up records retention and disposal schedules and explains the operation and services of the records centres operated by GRS.

8. GRS' RM Publication No. 3 "***Subject Filing***" - This publication establishes a comprehensive standard classification scheme for administrative records, which are grouped into six schedules, viz. Administration, Accommodation and Facilities, Equipment and Supplies, Finance, Personnel as well as

Information Systems and Services. It also provides guidelines on the development of a records classification scheme for programme records.

9. GRS' RM Publication No. 4 "***General Administrative Records Disposal Schedules***" - As a sequel to Publication No. 3 and using the same classification scheme of administrative records, this publication sets out retention and disposal schedules of administrative records for adoption by B/Ds.

10. GRS' RM Publication No. 6 "***Manual on Vital Records Protection***" - This publication identifies common hazards to records, explains the importance of vital records protection, provides guidelines on selection of appropriate protection methods, and enumerates the steps in establishing a vital records protection programme.

11. GRS' RM Publication No. 7 "***Topical Guide cum Checklists for Proper Records Management Practices***" – This publication is to assist B/Ds in assessing the effectiveness of their RM programme, identifying major problems and setting priorities for improvement. It also provides an overview of the basic components of a comprehensive RM programme.

12. ***Functional Requirements of an Electronic Recordkeeping System*** - This publication sets out the functional requirements of an ERKS for B/Ds' compliance in developing or adopting an ERKS.

13. ***Recordkeeping Metadata Standard for the Government of the Hong Kong Special Administrative Region*** and the associated implementation guidelines - This publication and the implementation guidelines set out, among others, essential recordkeeping metadata that should be created, captured, used, managed and maintained in an ERKS.

14. ***Disposal of Original Records (for records that have been digitised and stored in a digital form)*** - This publication provides guidance for B/Ds to assess potential risks of early destruction of original non-electronic records after their digitisation.

15. ***A Handbook on Preservation of Electronic Records*** – This publication provides guidelines for B/Ds to establish and implement a departmental preservation programme; and to adopt proper measures and practices to preserve their electronic records to meet legal and regulatory requirements, business and operational needs and evidence purpose.

16. ***ISO/TR 13028:2010 - Information and documentation - Implementation guidelines for digitization of records***

17. ***ISO 15489-1:2001 - Information and documentation - Records management - Part 1: General***

18. ***ISO/TR 15489-2:2001 - Information and documentation - Records management - Part 2: Guidelines***

19. ***ISO 23081-1:2006, Information and documentation - Records management processes - Metadata for records - Part 1: Principles***