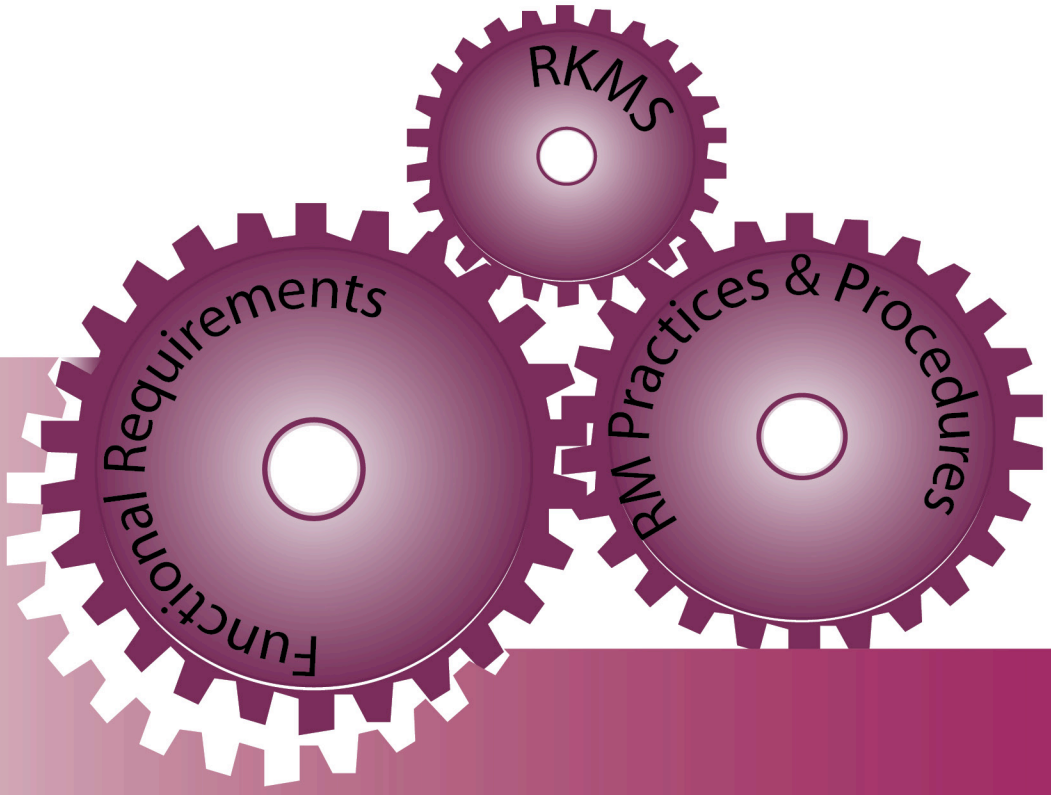
ELECTRONIC RECORDKEEPING SYSTEM IMPLEMENTATION GUIDELINES

Manual on Evaluation of an Electronic Recordkeeping System



Government Records Service

Manual on
Evaluation of an
Electronic Recordkeeping System

Government Records Service
Updated September 2016 *(with minor updates in November 2020)*

Revision History

Change number	Reason for change	Sections affected	Date issued
1			September 2015
2	To incorporate requirements for management of confidential records and updated requirements from the publications ***Functional Requirements of an Electronic Recordkeeping System*** (version 1.2) and the ***Recordkeeping Metadata Standard for the Government of the Hong Kong Special Administrative Region*** (version 1.1)	Various sections, Appendices 1, 2 and 3	September 2016
3	Minor update to terminology to align with government regulations	Appendix 1 Checkpoints 166 and 183, and Appendix 3 S/N 13	November 2020

Table of Contents

Chapter 1 Introduction 1

Purpose 2

Scope 2

Applicability 2

Government's RM policy and ERM requirements 3

Audience 4

Relationship with other RM publications 5

Updating of the manual 5

Structure of the manual 6

Assistance and support from GRS 6

Further information 6

Chapter 2 Compliance Assessment Programme 7

Introduction 8

Objectives of the compliance assessment 8

Mandatory components of the compliance assessment 8

Benefits of the compliance assessment 9

When should the compliance assessment be conducted 9

Assessment criteria and compliance ratings 11

Evaluation results of the compliance assessment 24

Skills required to conduct the compliance assessment 24

Roles and responsibilities for conducting the compliance assessment 25

Approving authority of the compliance assessment 26

Chapter 3 Evaluation Planning and Control 27

Introduction 28

Evaluation plans 28

Draw up a test plan and test specifications of an ERKS 30
Conduct testing of an ERKS..... 32
Consolidate evaluation results of an ERKS 33
Evaluate departmental RM policies, practices and procedures 33
Consolidate evaluation results of departmental RM policies, practices and procedures..... 35
Draw up a compliance assessment report 35
Seek endorsement of compliance assessment report 36
Implement improvements..... 36
Chapter 4 Dispensing with the Print-and-File Practice 37
Introduction 38
Mandatory print-and-file practice..... 38
Seeking approval from GRS 38
GRS' responsibility 39
Chapter 5 On-going Monitoring and Review.....41
Introduction 42
Regular reviews and continuous monitoring 42
Assistance and support from GRS 43

Appendices

Appendix 1	Evaluation of an electronic recordkeeping system for compliance with the ***Functional Requirements of an Electronic Recordkeeping System***
Appendix 2	Evaluation of an electronic recordkeeping system for compliance with the ***Recordkeeping Metadata Standard for the Government of the Hong Kong Special Administrative Region***

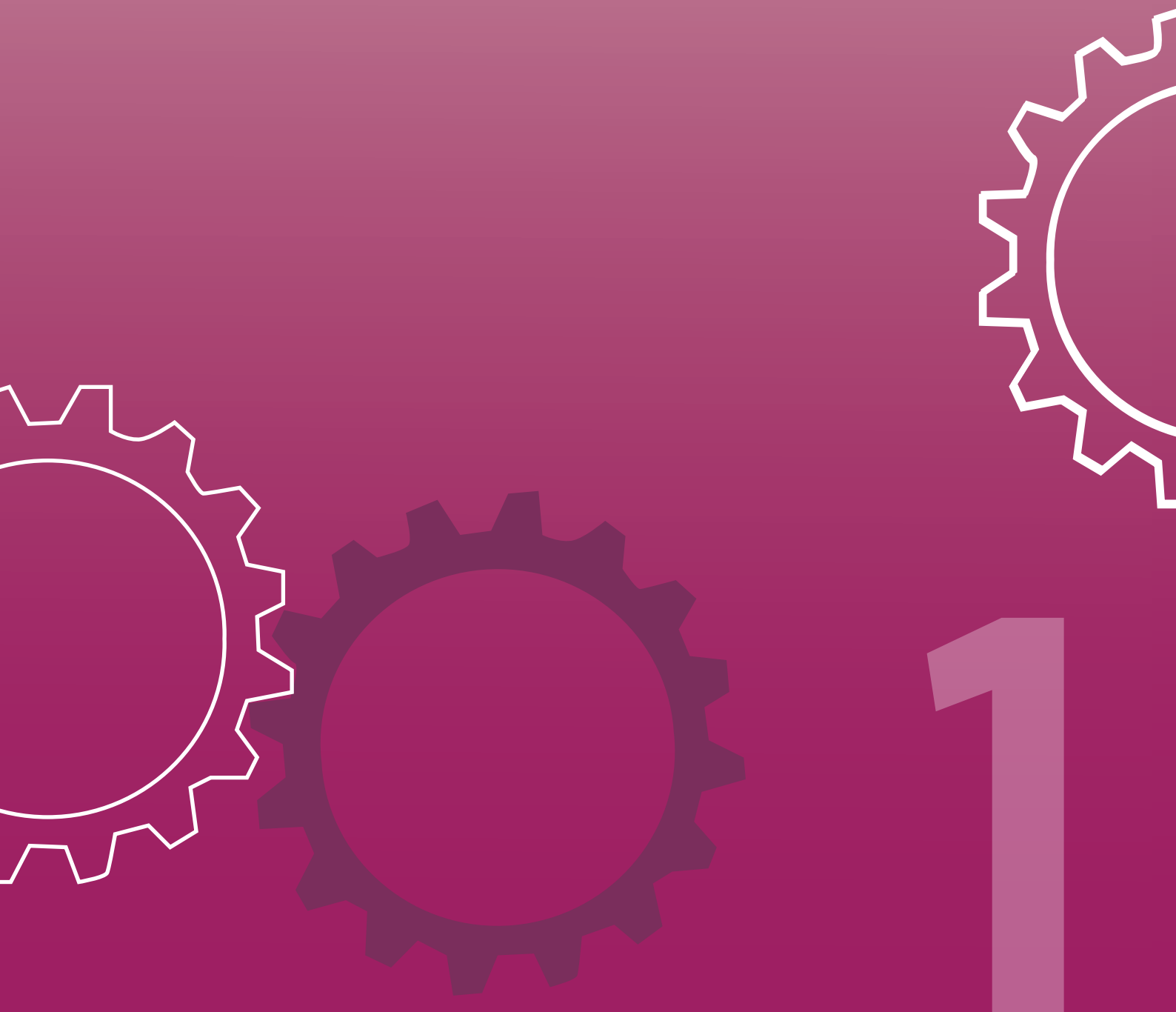
Appendix 3	Evaluation of the implementation and enforcement of proper departmental RM policies, practices and procedures for effective management of records in an electronic recordkeeping system
Appendix 4	A sample test plan of an ERKS
Appendix 5	A sample evaluation plan of departmental RM policies, practices and procedures
Appendix 6 (a) to (c)	Sample test case 1, sample test case 2 and test case template
Appendix 7	A sample compliance assessment report
Appendix 8	Request form for dispensing with the print-and-file practice

Abbreviations

AP	Application Profile
B/D	Bureau and/or department
CCGO	Central Cyber Government Office
CM	Circular Memorandum
DRM	Departmental Records Manager
DROID	Digital Record Object Identification
EIM	Electronic information management
ERKS	Electronic recordkeeping system
ERM	Electronic records management
FR of an ERKS	Functional Requirements of an Electronic Recordkeeping System
GC	General Circular
Government	Government of the Hong Kong Special Administrative Region
GRS	Government Records Service
IF	HKSARG Interoperability Framework [S18]
ITMU	Information Technology Management Unit
LDAP	Lightweight Directory Access Protocol
OCR	Optical Character Recognition
OGCIO	Office of the Government Chief Information Officer
PDF/A	Portable Document Format/Archive
PRO	Public Records Office of the Government Records Service
PSC	Project Steering Committee
RKMS	Recordkeeping Metadata Standard for the Government of the Hong Kong Special Administrative Region
RM	Records management
SRAA	Security risk assessment and audit
TIFF	Tagged Image File Format

Chapter 1

INTRODUCTION



1

Chapter 1 Introduction

Purpose

1.1 This manual provides guidelines for bureaux and departments (B/Ds) to evaluate and validate the compliance of -

(a) an electronic recordkeeping system (ERKS)[1]; and

(b) the associated departmental records management (RM) policies, practices and procedures governing the use, management and maintenance of an ERKS

with the Government's RM policy and electronic records management (ERM) requirements for proper management of government records[2].

Scope

1.2 This manual was issued by the Government Records Service (GRS) to guide B/Ds to evaluate and validate, by way of a **structured compliance assessment**, as to whether an ERKS complies with the Government's RM policy and ERM requirements as prescribed in paragraphs 1.6 to 1.8.

1.3 The compliance assessment also evaluates whether B/Ds have established proper departmental RM policies, practices and procedures; and defined clear RM roles and responsibilities to ensure effective and efficient management of records in an ERKS.

Applicability

1.4 It is incumbent upon B/Ds to ensure that an ERKS adopted/to be adopted for management of records should be a proper RM system in compliance with the Government's RM policy and ERM requirements. In this regard, B/Ds should apply the compliance assessment as set out in **Chapter 2** to -

---

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

[2] Records mean electronic records (such as spreadsheets and e-mails) and non-electronic records (such as paper records and microfilms) unless specified otherwise.

(a) an ERKS to be acquired, developed[3] or adopted[4] for management of records;

(b) an ERKS being acquired, developed or adopted for management of records at the time of promulgation of this manual; and

(c) an ERKS currently used for management of records.

1.5 **In case a B/D is implementing or is going to implement more than one ERKS in its organisation, each ERKS should be evaluated separately**. B/Ds may also evaluate, by way of the compliance assessment, as to whether a commercial off-the-shelf ERKS solution available in the market complies with the Government's RM policy and ERM requirements in the context of procuring an ERKS solution for management of records.

Government's RM policy and ERM requirements

1.6 Government's RM policy, mandatory RM requirements and RM good practices as promulgated in General Circulars (GCs) (e.g. GC Nos. 5/2006 and 2/2009), Administration Wing Circular Memoranda (CMs) relating to RM (e.g. Administration Wing CM on Establishment of Departmental Records Management Policies issued on 11 July 2012), the ***Records Management Manual*** and other RM publications and guidelines issued by GRS are available on the Central Cyber Government Office (CCGO)[5]. In gist, it is Government policy that each B/D should establish a comprehensive RM programme for proper management of government records. In addition, the Government is committed to identifying and preserving government records having archival value so as to enhance public awareness of Hong Kong's documentary heritage. Heads of B/Ds should accord appropriate priority and resources to implement a proper RM programme throughout their organisations.

1.7 Records are valuable resources of the Government to support evidence-based decision making, and meet operational and regulatory

---

[3] An ERKS developed by a B/D from scratch or a commercial off-the-shelf ERKS solution acquired by a B/D with certain degree of system configuration/customisation built in to meet the Government's RM policy and ERM requirements falls under this category.

[4] B/Ds may adopt an ERKS developed by the centre or by another B/D, or use an open source ERKS solution for management of records in their organisations. In this case, B/Ds may not need to go through system procurement and/or system development processes.

[5] GCs and CMs promulgated by the Director of Administration, and RM publications and guidelines promulgated by GRS are accessible at http://grs.host.ccgo.hksarg/cgp_intro.html.

requirements. They are essential for an open and accountable government. A record is any recorded information 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. An ERKS is able to capture records in different formats (e.g. e-mails, word-processed documents, spreadsheets, images and audio clips) and different media (e.g. paper, CDs and DVDs) which were created, received or sent through a wide range of sources, e.g. an e-mail system, fax, workflow (where applicable). It aims to maintain the content, context and structure of records so as to protect the authenticity, integrity, reliability and usability of records over time to serve as reliable evidence of decisions and activities.

1.8 As far as ERM and ERKS are concerned, B/Ds should make reference to ERM standards and guidelines developed by GRS for conducting the compliance assessment as specified in paragraphs 1.2 and 1.3. Specifically, B/Ds should ensure that requirements prescribed in the following standards and guidelines are adhered to -

(a) ***Functional Requirements of an Electronic Recordkeeping System***[6] (FR of an ERKS) (version 1.2);

(b) ***Recordkeeping Metadata Standard for the Government of the Hong Kong Special Administrative Region***[7] (RKMS) (version 1.1) and its implementation guidelines; and

(c) ***Disposal of Original Records*** (for records that have been digitised and stored in a digital form)[8].

Audience

1.9 This manual is intended for those officers, in particular the Departmental Records Managers (DRMs), Assistant Departmental Records Managers and IT staff of the Information Technology Management Units (ITMUs) in B/Ds, who are responsible for -

---

[6] ***Functional Requirements of an Electronic Recordkeeping System*** has been uploaded onto CCGO (accessible at http://grs.host.ccgo.hksarg/erm/s04/435.html).

[7] ***Recordkeeping Metadata Standard for the Government of the Hong Kong Special Administrative Region*** and its implementation guidelines have been uploaded onto CCGO (accessible at http://grs.host.ccgo.hksarg/erm/s04/457.html).

[8] ***Disposal of Original Records*** (for records that have been digitised and stored in a digital form) has been uploaded onto CCGO (accessible at http://grs.host.ccgo.hksarg/erm/s04/415.html).

(a) specifying requirements of, selecting and procuring an ERKS solution;

(b) developing and/or implementing an ERKS solution compliant with the Government's RM policy and ERM requirements;

(c) evaluating and validating the compliance of an ERKS with the Government's RM policy and ERM requirements; and

(d) managing and maintaining an ERKS compliant with the Government's RM policy and ERM requirements.

Relationship with other RM publications

1.10 This manual is part of the series of ERKS Implementation Guidelines[9] to help B/Ds initiate, plan and implement an ERKS in their organisations. It should be used in conjunction with FR of an ERKS and RKMS. These two publications prescribe the essential functionality and recordkeeping metadata that enable an ERKS to carry out and support RM functions and activities common to B/Ds. Please refer to FR of an ERKS and RKMS for a glossary of RM terms related to an ERKS and recordkeeping metadata respectively.

1.11 In case there are inconsistencies among this manual, FR of an ERKS, RKMS and other RM publications developed by GRS, B/Ds should seek advice from GRS.

Updating of the manual

1.12 This manual is a living document. It will be updated and further improved as necessary in future having regard to the latest international RM standards and best practices, changes in the Government's RM policy and ERM requirements and technological advances. This manual was first promulgated in September 2015. The current version was issued in September 2016 and has included additional checkpoints in the Appendices to evaluate the capability of an ERKS to manage confidential records.

---

[9] Other ERKS implementation guidelines include ***Guidelines on Mapping out Implementation of an Electronic Recordkeeping System in the Context of Developing Organisational Electronic Information Management Strategies***, ***Guidelines on Implementation of an Electronic Recordkeeping System: Key Considerations and Preparation Work Required***, and ***A Handbook on Records Management Practices and Guidelines for an Electronic Recordkeeping System***. They are available on CCGO (accessible at http://grs.host.ccgo.hksarg/erm/s04/424.html).

Structure of the manual

1.13 Other than this chapter, this manual is organised into four chapters as follows -

Chapter 2: Compliance assessment programme

Chapter 3: Evaluation planning and control

Chapter 4: Dispensing with the print-and-file practice

Chapter 5: On-going monitoring and review

Assistance and support from GRS

1.14 As far as this manual is concerned, GRS is responsible for -

(a) reviewing and updating this manual as and when necessary;

(b) developing further RM guidelines as appropriate; and

(c) providing RM advisory support and assistance to B/Ds to evaluate the compliance of an ERKS with the Government's RM policy and ERM requirements.

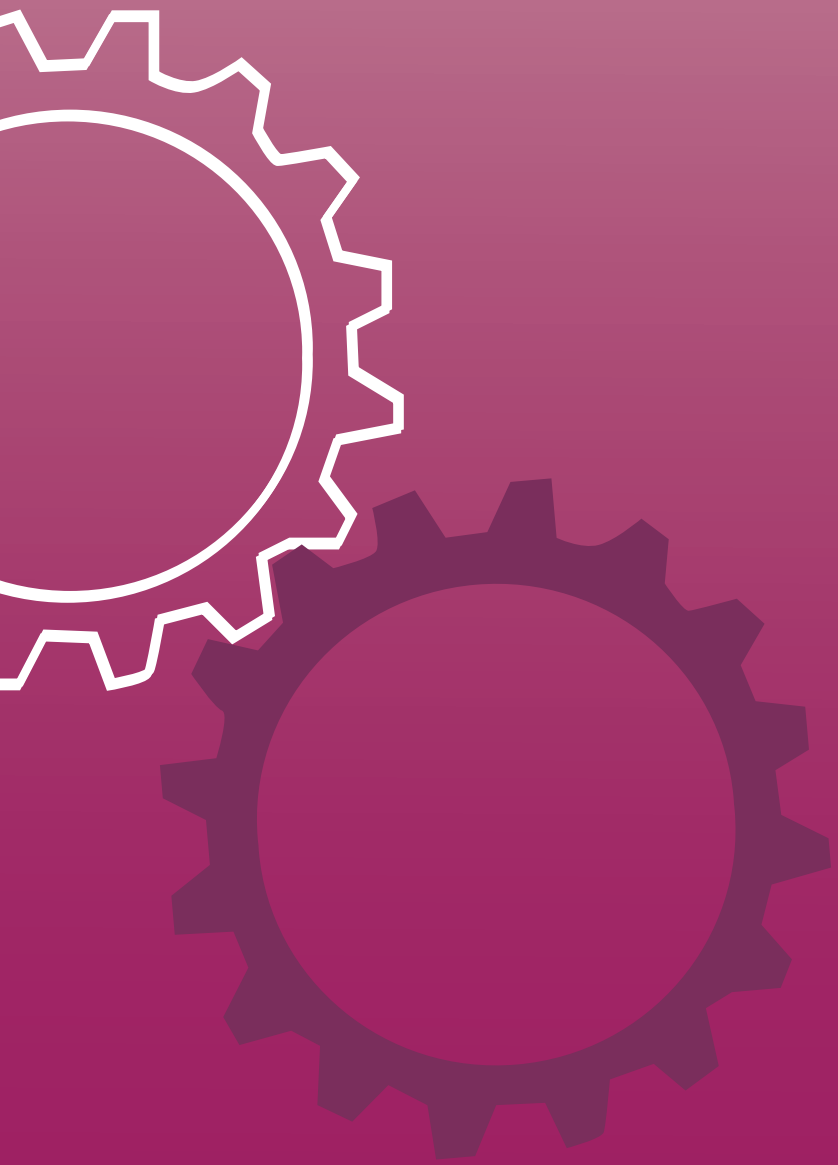
Further information

1.15 This manual is available on CCGO (accessible at http://grs.host.ccgo.hksarg/erm/s04/4232.html) for reference by B/Ds.

1.16 Enquiries arising from this manual should be addressed to Senior Executive Officer (Record Systems Development)1 on 2195 7750 or Executive Officer (Record Systems Development)1 on 2195 7783.

Chapter 2

COMPLIANCE ASSESSMENT PROGRAMME



2

Chapter 2 Compliance Assessment Programme

Introduction

2.1 This chapter explains the objectives, evaluation criteria and ratings; and roles and responsibilities for planning, conducting and approving the results of a compliance assessment. The processes and procedures of the compliance assessment are described in **Chapter 3**.

Objectives of the compliance assessment

2.2 A compliance assessment aims to assist B/Ds in evaluating and validating whether an ERKS and the associated departmental RM policies, practices and procedures governing the use, management and maintenance of an ERKS are able to -

(a) comply with the Government's RM policy and ERM requirements as specified in paragraphs 1.6 and 1.7;

(b) support the discharge of RM functions and activities common to B/Ds as specified in FR of an ERKS and RKMS;

(c) maintain the authenticity, integrity, reliability and usability[10] of records managed by an ERKS throughout their life cycle to serve as reliable evidence of decisions and activities of B/Ds[11];

(d) meet specific business, operational and RM needs of B/Ds; and

(e) ensure that records with archival value are properly managed by an ERKS before they are transferred to GRS for retention.

Mandatory components of the compliance assessment

2.3 A compliance assessment covers the following **mandatory** components -

---

[10] Please refer to FR of an ERKS for the definition of authenticity, integrity, reliability and usability of records.

[11] Electronic records are vulnerable in nature because they can be easily overwritten, lost or become inaccessible over time as technology changes, and can be lacking in self-evident and ready contextual information. Therefore proper controls over electronic records are of great importance to safeguard the smooth operation and legal and financial interests of the Government.

(a) an evaluation of an ERKS including its functionality, features, system configuration and customisation; and

(b) an evaluation of departmental RM policies, practices and procedures governing the use, management and maintenance of an ERKS.

2.4 Details of the compliance assessment are set out in ensuing paragraphs.

Benefits of the compliance assessment

2.5 By undertaking a compliance assessment, B/Ds should be able to -

(a) prove and demonstrate that an ERKS is capable of maintaining the authenticity, integrity, reliability and usability of records to meet continuous legal, business, evidence and accountability needs;

(b) identify gaps and weaknesses of an ERKS and their departmental RM policies, practices and procedures for improvements;

(c) satisfy themselves as to whether an ERKS complies with the Government's RM policy and ERM requirements; and

(d) satisfy themselves as to whether the "print-and-file" practice of e-mail records[12] can be dispensed with upon a proper ERKS being put to use.

2.6 If a B/D, after completing the compliance assessment, is satisfied that a proper ERKS is put in place in its organisation with implementation and enforcement of adequate and proper departmental RM policies, practices and procedures, it may seek GRS' prior agreement to dispense with the print-and-file practice of e-mail records in accordance with the procedures specified in **Chapter 4**.

When should the compliance assessment be conducted

2.7 In line with the established practice for IT project management, an ERKS, like other computer systems, should be tested prior to system

[12] General Circular No. 2/2009 entitled "**Mandatory Records Management Requirements**" stipulates that e-mail correspondence should be "printed-and-filed" for record purposes unless otherwise agreed by GRS.

acceptance to verify and confirm whether it fully meets pre-defined system and user requirements and is qualified as a reliable and quality computer system. Given that an ERKS to be used by B/Ds must comply with the Government's RM policy and ERM requirements, B/Ds should conduct the evaluation as specified in paragraph 2.3(a) for **a newly acquired, developed or adopted ERKS in the context of system acceptance** (which includes system acceptance tests[13], user acceptance tests[14] and security risk assessment and audit (SRAA)[15]). In case system acceptance is not required under certain circumstances, B/Ds should conduct the evaluation prior to rollout of an ERKS to users.

2.8 For the evaluation relating to departmental RM policies, practices and procedures specified in paragraph 2.3(b), B/Ds should conduct the evaluation **no later than three months after the rollout of an ERKS** to users on the assumption that those policies, practices and procedures should largely be finalised by that time.

2.9 Compliance assessment is not a one-time activity. Apart from the evaluation in the context of system acceptance, B/Ds should conduct a fresh compliance assessment once **every three to four years** after an ERKS is put to use or more often as required, e.g. after a serious non-conformity to departmental ERKS practices and procedures has been identified. Specifically, B/Ds should conduct a compliance assessment **immediately after** -

(a) the hardware, software and/or the functionality of an ERKS has been substantially upgraded, revised or supplemented; or

(b) the departmental RM policies, practices and procedures governing the use, management and maintenance of an ERKS have been substantially revised or updated.

In case of doubt, B/Ds should seek advice from GRS.

---

[13] System acceptance tests generally include functional test, system integration test, reliability test, load test and resilience test, etc.

[14] User acceptance tests mean tests conducted by end users to verify and confirm whether the functionality of a computer system meets the user requirements and accept the system for production rollout.

[15] Please refer to section 13 of ***IT Security Guidelines*** [G3] Version 7.0 (September 2012) issued by the Office of the Government Chief Information Officer (OGCIO) (accessible on ITG InfoStation at http://itginfo.ccgo.hksarg/content/sm/SMRO_ref_no.htm).

Assessment criteria and compliance ratings

2.10 To assist B/Ds in evaluating and validating the compliance of an ERKS with the Government's RM policy and ERM requirements notably FR of an ERKS and RKMS, **two self-assessment checklists** have been drawn up at **Appendix 1** and **Appendix 2** respectively to guide B/Ds to develop test specifications of an ERKS. These checklists set out key checkpoints on the functionality of an ERKS and creation, capture, use, management and maintenance of recordkeeping metadata.

2.11 With respect to the evaluation of implementation and enforcement of departmental RM policies, practices and procedures for proper management of records in an ERKS, a **self-assessment checklist** on key RM issues has been drawn up at **Appendix 3** for compliance and reference by B/Ds.

2.12 The checklists at **Appendices 1 to 3** are not intended to be exhaustive. B/Ds may include other checkpoints and issues for evaluation if deemed necessary, e.g. checkpoints to evaluate ERKS features that are tailor-made to meet specific RM needs of their organisations.

Checklists for evaluating an ERKS

2.13 **Appendix 1** and **Appendix 2** prescribe **a total of 341 and 24 checkpoints** respectively to assist B/Ds in evaluating how well an ERKS complies with FR of an ERKS and RKMS. The checkpoints cover the following categories with their objectives specified below -

Category	Objective of the checkpoints
Records classification and identification	To evaluate and validate whether an ERKS is capable of organising and classifying both electronic and non-electronic records in a structured and hierarchical records classification scheme(s) based on function and/or subject; and assigning a unique identifier to each aggregation of records and record.
Capture	To evaluate and validate whether an ERKS is capable of capturing the content, context and structure[16] of records in different formats and different media which were

[16] Please refer to FR of an ERKS for the definition of content, context and structure of a record.

Category	Objective of the checkpoints
	created, received or sent through a wide range of sources; and managing them in the ERKS.
Use of records	To evaluate and validate whether an ERKS is capable of supporting users to search, retrieve, print, download, charge-out/charge-in records, etc. in accordance with the security and access control of records.
Security and access control	To evaluate and validate whether an ERKS is capable of protecting records from inadvertent or unauthorised alteration, deletion, access and retrieval; and monitoring the integrity of records through audit trails.
Retention and disposal	To evaluate and validate whether an ERKS is capable of managing the retention periods and disposal actions of records in a managed, systematic and auditable way.
Language support	To evaluate and validate whether an ERKS is capable of supporting use of English and Chinese (including Traditional and Simplified Chinese) in the ERKS.
Administration	To evaluate and validate whether an ERKS is capable of monitoring the ERKS repository(ies), producing RM reports and managing vital records.
Metadata	To evaluate and validate whether an ERKS is capable of creating, capturing, using, managing and maintaining sufficient, accurate, complete and consistent metadata to support essential RM functions and activities throughout the life cycle of records; and persistently linking metadata to the associated entity, e.g. a folder or a record.
Workflow	To evaluate and validate whether an ERKS is capable of supporting automation of business processes and RM activities; and facilitating distribution and routing of records.

2.14 On the basis of checkpoints specified at **Appendix 1** and **Appendix 2**, B/Ds should then develop test specifications to test an ERKS, including test cases, test procedures and test data that specifically suit their

business, operational and RM context while ensuring that each checkpoint specified has been evaluated thoroughly.

Assessment of technical and non-functional requirements of an ERKS

2.15 Like other computer systems, an ERKS should be tested and evaluated in terms of the technical and non-functional aspects[17] having regard to the Government's and departmental IT policy and requirements, prior to system acceptance. They may include -

(a) system performance, scalability and reliability;

(b) ability of integration with other computer systems;

(c) ability of technical interoperability and compatibility;

(d) IT security;

(e) ease of use; and

(f) ease of system configuration/customisation.

2.16 ITMUs of B/Ds should develop specific evaluation criteria and test specifications to test the performance and effectiveness of an ERKS in technical and non-functional aspects. This evaluation forms part of the compliance assessment.

2.17 Upon completion of the evaluation, B/Ds should verify whether the ERKS satisfactorily meets the Government's and departmental IT policy and requirements, and the pre-defined technical and non-functional requirements.

Compliance ratings of an ERKS

2.18 Upon completion of a testing of an ERKS, B/Ds should evaluate and determine how well it complies with FR of an ERKS and RKMS. In this regard, B/Ds should select **one** of the following ratings which corresponds to the performance indicators that best describes the current performance of the ERKS -

[17] B/Ds should make reference to the ***Guidelines for Application Software Testing*** [G20] Version 1.8 (March 2015) issued by OGCIO to plan, arrange and conduct the testing (accessible on ITG InfoStation at http://itginfo.ccgo.hksarg/content/sm/SMRO_ref_no.htm).

Rating	Performance indicator
Full compliance	(a) An ERKS is proved to be complying with - (i) **all** mandatory requirements (including conditional mandatory requirements and non-conditional mandatory requirements) as set out in FR of an ERKS; (ii) **all** requirements pertaining to Application Profile (AP) 1 of RKMS to ensure that sufficient, accurate, complete and consistent recordkeeping metadata have been created, captured, used, managed and maintained in the ERKS; (iii) **all** requirements of other APs of RKMS if they have been implemented; and (iv) optional requirements as specified in FR of an ERKS if they have been implemented. (b) An ERKS satisfactorily passes a SRAA. (c) An ERKS satisfactorily meets the Government's and departmental IT policy and requirements; and the pre-defined technical and non-functional requirements as specified by the B/D concerned.
Moderate compliance requiring improvement	(a) An ERKS is proved to be complying with - (i) **70%**[18] **or more (but not all)** of the mandatory requirements (including conditional mandatory requirements and non-conditional mandatory requirements) as set out in FR of an ERKS; (ii) **70% or more (but not all)** of the requirements pertaining to AP1 of RKMS; (iii) **70% or more (but not all)** of the requirements of other APs of RKMS if they have been implemented; and (iv) optional requirements as specified in FR of an

[18] Generally speaking, a good quality ERKS solution should be able to meet at least 70% of the functional requirements before system customisation.

Rating	Performance indicator
	ERKS if they have been implemented. (b) Improvements, system re-configuration and/or bug fixing should be implemented. Re-testing of the ERKS is required to evaluate whether the ERKS is able to achieve full compliance upon the completion of system improvements.
Low to non-compliance	(a) An ERKS is proved to be - (i) **complying with less than 70%** of all mandatory requirements (including conditional mandatory requirements and non-conditional mandatory requirements) specified in FR of an ERKS; (ii) **complying with less than 70%** of the requirements of AP1 of RKMS or failing to create, capture, use, manage and maintain sufficient, accurate, complete and consistent recordkeeping metadata pertaining to AP1 of RKMS; (iii) **complying with less than 70%** of the requirements of other APs of RKMS if they have been implemented; or (iv) **partially** complying with or failing to meet optional requirements as specified in FR of an ERKS if they have been implemented. (b) Substantial system improvements/enhancements are required. Re-testing of the ERKS is required to evaluate whether the ERKS is able to achieve full compliance upon the completion of system improvements/enhancements.

2.19 **Until and unless an ERKS is proved to be achieving full compliance according to the criteria set out in paragraph 2.18 above, B/Ds should not take the position that the ERKS is a proper RM system with the capability of maintaining the authenticity, integrity, reliability and usability of records to meet continuous legal, business, evidence and accountability needs**.

Checklist for evaluating departmental RM policies, practices and procedures

2.20 The self-assessment checklist at **Appendix 3** guides B/Ds to evaluate how well they have implemented and enforced departmental RM policies, practices and procedures in managing records in an ERKS. It covers the following categories with their objectives specified below -

Category	Objective of the checkpoints
Departmental RM policies and responsibilities	To evaluate whether a B/D has established a clear direction and demonstrated support for, and commitment to, the proper management of records (including those managed by an ERKS) through the formulation, promulgation and maintenance of departmental RM policies, practices and procedures.
Records capture and registration	To evaluate whether a B/D has put suitable arrangements in place to ensure that sufficient but not excessive records are created and captured into an ERKS.
Records classification and organisation	To evaluate whether a B/D has established and implemented a logical, systematic, consistent and scalable records classification scheme(s) in an ERKS to cover all records irrespective of nature or formats, and adopted proper practices to manage the records classification scheme(s).
Records storage	To evaluate whether records managed by an ERKS are stored in a safe, secured and proper environment and are able to remain authentic, complete and accessible for as long as required.
Security and access control of records	To evaluate whether access control and security measures in place are able to demonstrate that records managed by an ERKS are adequately protected against unauthorised access, alteration and deletion.
Records tracking	To evaluate whether proper arrangements have been put in place to track the whereabouts of records, particularly non-electronic records,

Category	Objective of the checkpoints
	managed by an ERKS.
Records retention and disposal	To evaluate whether disposal of records in an ERKS, including destruction, is conducted in a systematic and auditable manner and such disposal is properly authorised.
Vital records protection	To evaluate whether suitable arrangements have been put in place to identify, select and protect vital records managed by an ERKS.
Monitoring and auditing	To evaluate whether departmental RM policies, practices and procedures have been properly implemented, monitored and regularly reviewed.
Training	To evaluate whether staff members responsible for managing records and/or managing an ERKS are competent and well-trained.
System management	To evaluate whether an ERKS is operated properly so as to ensure the authenticity, integrity, reliability and usability of records managed by the ERKS.
System back-up and recovery	To evaluate whether the authenticity and integrity of records managed by an ERKS are adequately protected from loss or corruption in case of system failure.
System maintenance	To evaluate whether an ERKS is maintained properly so as to ensure the authenticity, integrity, reliability and usability of records managed by the ERKS.
Optional (Note: B/Ds should assess their performance and effectiveness in the following two aspects if they have adopted scanning to convert non-electronic records into digitised records for management and storage in an ERKS and/or have used third party services relating to management, storage and maintenance of an ERKS.)	
Scanning procedures and processes	To evaluate whether the technology chosen, procedures and process of scanning are able to ensure and demonstrate that the digitised records stored in an ERKS are trustworthy and

Category	Objective of the checkpoints
	complete to ensure the legibility and usability of the digitised records.
Use of third party services (e.g. using cloud-based ERKS services provided by a service provider)	To evaluate whether a B/D is able to demonstrate compliance with the Government's and departmental IT and RM policies, requirements, practices and procedures by way of outsourcing RM services.

Compliance ratings of departmental RM policies, practices and procedures

2.21 Upon completion of the evaluation, B/Ds should determine how effective they have implemented and enforced departmental RM policies, practices and procedures to underpin the use, management and maintenance of an ERKS. In this regard, B/Ds should select **one** of the following ratings which corresponds to the performance indicators that best describe the current state of creations, use and management of records in an ERKS -

Rating	Performance indicator
Good	My B/D has - (a) **fully complied with** the Government's RM policy, mandatory RM requirements and RM practices and procedures as specified in GCs and CMs relating to RM notably GC Nos. 5/2006 and 2/2009 and Administration Wing CM on Establishment of Departmental Records Management Policies issued on 11 July 2012; (b) **developed and established departmental RM policies** to create, use and manage records (including those managed by an ERKS); (c) **established a logical, systematic, consistent and scalable records classification scheme(s)** in an ERKS to classify and organise records; (d) **developed guidelines and put in place sufficient measures and control** to ensure that staff members **create and capture adequate,**

Rating	Performance indicator
	complete and reliable records into an ERKS to meet continuous legal, business, evidence and accountability needs; (e) **properly tracked the whereabouts of records and stored records** managed by an ERKS in a secured and safe manner; (f) **properly kept and disposed of records** managed by an ERKS in accordance with the approved records retention and disposal schedules; (g) **identified, selected and suitably protected vital records** managed by an ERKS; (h) **developed comprehensive and proper RM practices, procedures and guidelines** governing the use, management and maintenance of an ERKS and supporting effective execution of RM functions and activities in the ERKS;[19] (i) **promulgated departmental RM policies, practices and procedures** for compliance by all staff members using, managing and maintaining an ERKS; (j) **implemented adequate and proper measures to monitor the enforcement of departmental RM policies, practices, procedures and guidelines** by staff members using, managing and maintaining an ERKS; (k) **implemented adequate and proper security and access control measures** to protect records and audit trail data of an ERKS;

[19] B/Ds should make reference to ***A Handbook on Records Management Practices and Guidelines for an Electronic Recordkeeping System*** (accessible at http://grs.host.ccgo.hksarg/erm/s04/4262.html). The Handbook provides 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 to underpin the operation of an ERKS.

Rating	Performance indicator
	(l) **properly undertaken system management and maintenance** of an ERKS; and **established adequate and proper procedures to guide execution of essential system management activities** such as back-up and restoration of records in case of system failures; (m) **defined clearly roles and responsibilities** of staff members to use, manage and maintain an ERKS and assigned appropriate officers to take up the relevant roles and responsibilities; (n) **properly documented, updated and reviewed departmental RM policies, practices and procedures** to create, use and manage records (including those managed by an ERKS); (o) **provided adequate and proper RM training** to staff members using, managing and maintaining an ERKS; (p) **put in place adequate measures to review the effectiveness of departmental RM policies, practices and procedures** to create, use and manage records (including those managed by an ERKS) having regard to changing business, operational and RM requirements and needs; (q) **developed proper practices and procedures for scanning** of non-electronic records *(Note: B/Ds should adopt this performance indicator if they have adopted scanning for converting non-electronic records into digitised records for management and storage in an ERKS.)*; and (r) **put in place sufficient measures and control to ensure that a service provider complies with the Government's and departmental IT and RM policy, requirements, practices and procedures** to provide services relating to management, storage and maintenance of an

Rating	Performance indicator
	ERKS *(Note: B/Ds should adopt this performance indicator if they have acquired third party's service relating to management, storage and maintenance of an ERKS.)*.
Fair	My B/D has - (a) **largely complied with** the Government's RM policy, mandatory RM requirements and RM practices and procedures as specified in GCs and CMs relating to RM notably GC Nos. 5/2006 and 2/2009 and Administration Wing CM on Establishment of Departmental Records Management Policies issued on 11 July 2012; (b) **developed and established departmental RM policies** to create, use and manage records (including those managed by an ERKS); (c) **developed departmental guidelines for creation and capture of adequate, complete and reliable records** into an ERKS to meet continuous legal, business, evidence and accountability needs; (d) **established a logical, systematic, consistent and scalable records classification scheme**(s) in an ERKS to classify and organise records; (e) **developed essential departmental RM practices, procedures and guidelines** governing the use, management and maintenance of an ERKS; (f) **promulgated departmental RM policies, practices, procedures and guidelines** to all staff members using, managing and maintaining an ERKS; (g) **put in place measures to track the whereabouts of records and store records** managed by an ERKS in a secured and safe

Rating	Performance indicator
	manner; (h) **kept and disposed of records** managed by an ERKS in accordance with the approved records retention and disposal schedules; (i) **identified and selected vital records** managed by an ERKS; (j) **implemented some security and access control measures** to protect records and audit trail data of an ERKS; (k) **undertaken system management** including system back-up and **established some basic procedures** for compliance by staff members **to execute essential system management activities of an ERKS**; (l) **provided some basic training** to users and RM staff to use, manage and maintain an ERKS; (m) **maintained documentation on departmental RM policies, practices, procedures and guidelines** to create, use and manage records (including those managed by an ERKS); (n) **defined roles and responsibilities** of staff members to use, manage and maintain an ERKS and assign the roles to staff members; (o) **developed some practices and procedures for scanning of non-electronic records** *(Note: B/Ds should adopt this performance indicator if they have adopted scanning for converting non-electronic records into digitised records for management and storage in an ERKS.)*; and (p) **included requirements in a contract or service specification to stipulate that a service provider complies with the Government's and departmental IT and RM policy, requirements, practices and procedures** to

Rating	Performance indicator
	provide services relating to management, storage and maintenance of an ERKS *(Note: B/Ds should adopt this performance indicator if they have acquired third party's service relating to management, storage and maintenance of an ERKS.)*.
Unsatisfactory	My B/D has - (a) **yet to develop and establish departmental RM policies** to create, use and manage records (including those managed by an ERKS); (b) **developed limited RM practices, procedures and guidelines** to support the use, management and maintenance of an ERKS; (c) **yet to enforce those RM practices, procedures and guidelines** consistently to all users of an ERKS; (d) **yet to develop guidelines** to help staff members create and capture adequate, complete and reliable records into an ERKS; (e) **established a records classification scheme(s)** in an ERKS but it **fails to classify and organise records in a consistent, logical and systematic way**; (f) **not properly undertaken system management and maintenance**; and **not drawn up written documentation** to guide execution of essential system management activities of an ERKS; (g) **yet to clearly define the roles and responsibilities** of staff members to use, manage and maintain an ERKS; (h) **yet to provide RM training** to staff members using, managing and maintaining an ERKS; (i) **yet to develop practices and procedures for**

Rating	Performance indicator
	scanning of records *(Note: B/Ds should adopt this performance indicator if they have adopted scanning for converting non-electronic records into digitised records for management and storage in the ERKS.)*; and (j) **yet to put in place measures to control and monitor the service quality of a service provider** providing services relating to management, storage and maintenance of the ERKS *(Note: B/Ds should adopt this performance indicator if they have acquired third party's service relating to management, storage and maintenance of an ERKS.)*.

Evaluation results of the compliance assessment

2.22 After completing the compliance assessment, a B/D should be able to satisfy itself whether it achieves a "**full compliance**" rating (as prescribed in paragraph 2.18) for its ERKS, and a "**good**" rating (as defined in paragraph 2.21) in respect of its performance and effectiveness in implementing and enforcing departmental RM policies, practices and procedures for compliance with the Government's RM policies and ERM requirements set out in paragraphs 1.6 and 1.7. In case a B/D has not achieved the said "full compliance" and "good" ratings, the B/D concerned should make timely improvements to its ERKS and/or departmental RM policies, practices and procedures as appropriate. For details, please refer to paragraphs 3.6, 3.7 and 3.11.

2.23 For the purpose of seeking GRS' approval to dispense with the print-and-file practice, a B/D should demonstrate that it has achieved the ratings of "**full compliance**" and "**good**" as specified in paragraphs 2.18 and 2.21 respectively. Please refer to **Chapter 4** for procedures to seek GRS' prior approval to dispense with the print-and-file practice.

Skills required to conduct the compliance assessment

2.24 Officers in B/Ds responsible for conducting a compliance assessment should have a good understanding and knowledge of the following -

(a) Government's RM policy and ERM requirements;

(b) Government's IT policy, requirements and guidelines;

(c) departmental RM and IT policies, requirements, practices and procedures; and

(d) system configuration/customisation and the functionality of the ERKS to be evaluated.

Roles and responsibilities for conducting the compliance assessment

2.25 B/Ds are responsible for conducting a compliance assessment and carrying out the following tasks and activities pertaining to the assessment -

(a) drawing up a test plan and test specifications as specified in **Chapter 3**;

(b) ensuring that the checklists at **Appendix 1**, **Appendix 2** and **Appendix 3** are thoroughly examined and evaluated in the compliance assessment;

(c) ensuring that documentation of the compliance assessment is properly created and kept for review and audit purposes;

(d) ensuring that the assessment and the associated tests such as system acceptance tests are conducted in a suitable test environment and in an impartial manner; and

(e) compiling an assessment report and following up the recommendations of the assessment report timely.

2.26 A suitable mix of officers with RM and IT knowledge and expertise is required to conduct the assessment. As an ERKS serves records users, B/Ds should suitably involve records users in the evaluation so that their views and feedback are adequately solicited.

2.27 **To avoid conflict of interests, B/Ds should, as far as possible, arrange the compliance assessment of an ERKS[20] to be conducted by a Test Group which does not include the contractor(s) responsible for developing**

[20] Please see the general testing principles set out in section 6.4 of ***Guidelines for Application Software Testing*** [G20] Version 1.8 (March 2015) issued by OGCIO (accessible on ITG InfoStation at http://itginfo.ccgo.hksarg/content/sm/SMRO_ref_no.htm).

the ERKS or providing system implementation and/or customisation services of the ERKS.

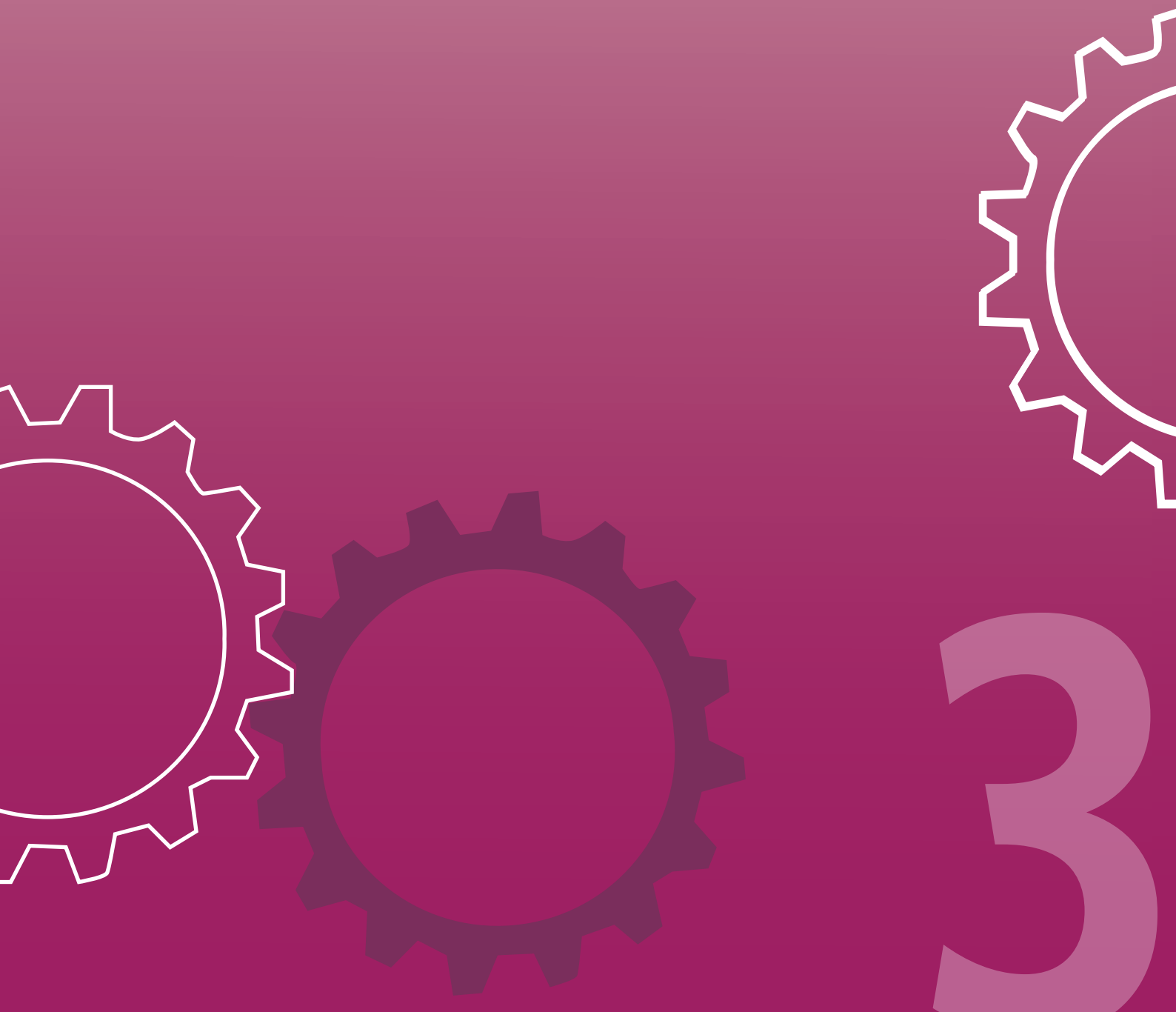
Approving authority of the compliance assessment

2.28 B/Ds should designate a **directorate officer** to approve the findings and recommendations of a compliance assessment and the compliance assessment report. For details, please see paragraph 3.14.

2.29 For the purpose of processing a request to dispense with the print-and-file practice (please see Chapter 4 for details), GRS may require a B/D to conduct a demonstration(s) of the functionality of its ERKS to GRS representatives on site and submit relevant documentation including approved test plan(s), test specifications (including test cases, test procedures and test data), test results, test incident logs and the assessment report of the ERKS and the associated departmental RM policies, practices and procedures to GRS for review.

Chapter 3

EVALUATION PLANNING AND CONTROL



Chapter 3 Evaluation Planning and Control

Introduction

3.1 This chapter provides guidelines for B/Ds to prepare and conduct a compliance assessment to evaluate an ERKS and the associated departmental RM policies, practices and procedures.

Evaluation plans

3.2 A compliance assessment of an ERKS should be conducted in a controllable, systematic and auditable manner. To this end, B/Ds should draw up the following evaluation plans -

(a) a test plan(s) and test specifications to test the functionality and the capability of an ERKS to meet the pre-defined technical and non-functional requirements. This is in line with the established IT practice to test a computer system prior to system acceptance[21]; and

(b) a plan to evaluate the effectiveness of departmental RM policies, practices and procedures governing the use, management and maintenance of an ERKS for management of records.

3.3 A high-level checklist, showing the major stages and tasks of a compliance assessment, is provided below to assist B/Ds in planning and conducting the testing and evaluation set out in paragraph 3.2(a) and (b), and in following up the findings and recommendations of the compliance assessment. Following that, detailed guidelines are provided in paragraphs 3.4 to 3.10.

[21] Please refer to Chapter 8 of the ***Guidelines for Application Software Testing*** [G20] Version 1.8 (March 2015) issued by OGCIO (accessible on ITG InfoStation at http://itginfo.ccgo.hksarg/content/sm/SMRO_ref_no.htm).

High-level steps to conduct a compliance assessment

Stage 1

Prepare

- Determine and establish a governance structure as appropriate to plan and conduct a compliance assessment
- Draw up a test plan(s) and test specifications to evaluate an ERKS
- Review and approve the test plan(s) and test specifications
- Set up a suitable test environment to test the ERKS
- Draw up an evaluation plan and determine the methodology to evaluate the effectiveness of departmental RM policies, practices and procedures

Stage 2

Conduct testing and evaluation

- Conduct system testing, e.g. system acceptance tests and user acceptance tests of the ERKS
- Re-test if required and resolve faults/problems
- Conduct activities such as interviews, surveys, documentation review and on-site inspections to assess the implementation and enforcement of departmental RM policies, practices and procedures

Stage 3

Analyse and consolidate findings and results

- Consolidate findings and results of the test of the ERKS and evaluation of departmental RM policies, practices and procedures
- Draw up an assessment report
- Seek internal approval to the assessment report

Stage 4

Improve and review

- Follow up the results and recommendations of the compliance assessment and make improvements where appropriate
- Set targets for improvements and assign priorities for action
- Implement improvements
- Schedule re-testing of the ERKS and/or re-evaluation of departmental RM policies, practices and procedures if required

Draw up a test plan and test specifications of an ERKS

3.4 In drawing up a test plan and test specifications of an ERKS, B/Ds should follow the ***Guidelines for Application Software Testing*** [G20] promulgated by OGCIO. Specifically, B/Ds should take the following actions -

Activity	Points to note
1. Establish a proper governance structure to plan and oversee the test	B/D should determine as to whether a Test Group[22] should be set up under the Project Steering Committee (PSC) to plan and execute the testing of an ERKS.[23]
2. Determine the schedule and scope of the test	(a) Same as other computer systems, a testing of an ERKS may comprise the following - (i) functional test; (ii) system integration test; (iii) reliability test; (iv) user acceptance test; (v) load test; (vi) resilience test; and (vii) disaster recovery drill test. (b) B/Ds should ensure that test cases cover - (i) all non-conditional mandatory functional requirements, conditional mandatory and optional functional requirements specified in FR of an ERKS that have been implemented in the ERKS to be tested; (ii) requirements pertaining to AP1 and other APs that have been implemented in the ERKS to be tested; and (iii) any additional functionality built in to

[22] Please see section 5.1.2 of ***Guidelines for Application Software Testing*** [G20] Version 1.8 (March 2015).

[23] Please see section 9.1 of ***Guidelines for Application Software Testing*** [G20] Version 1.8 (March 2015).

Activity	Points to note
	address specific business and/or RM requirements of the B/D concerned. (c) B/Ds should ensure that checkpoints for evaluating the functionality of an ERKS specified at **Appendix 1** and **Appendix 2** are duly and thoroughly incorporated into the test cases. (d) B/Ds should allow sufficient time to test the functionality of an ERKS in a thorough manner.
3. Draw up a test plan and test specifications	(a) Please see a sample test plan of an ERKS at **Appendix 4**. The test plan should include test procedures, test cases and test data. (b) Design test cases with test data in accordance with the guidelines specified in ***Guidelines for Application Software Testing*** [G20]. Specifically, the user acceptance test should specify the following for each test case - (i) the test objective and a mapping of the test case to FR of an ERKS and RKMS developed by GRS; (ii) test data; (iii) pre-test conditions; (iv) specific procedures if appropriate; and (v) expected results. (c) Two samples of test cases and a template for drawing up a test case to test the functionality of an ERKS are attached at **Appendix 6 (a) to (c)** for reference by B/Ds. B/Ds may tailor the test cases to suit their business, operational and RM scenarios.
4. Review and approve the test plan and test	(a) The PSC may be the approving authority of the test plan(s) and the test specifications. (b) DRM and Head of ITMU should be consulted

Activity	Points to note
specifications	about the test plan(s) and test specifications to ensure that sufficient test cases are developed to test RM and system functionality of an ERKS.
5. Set up test environment and system configuration	(a) Tests should normally take place on site. (b) The contractor should make ready the test environment and ensure that it is fully and properly configured prior to testing. (c) All of the test data for the test cases should normally be loaded into the test system prior to commencement of the tests.
6. Assign roles and responsibilities for conducting the testing of an ERKS	(a) B/Ds should assign appropriate officers to perform the following tasks - (i) conducting the tests in a suitable test environment and recording test results; (ii) re-testing a test case that was not completed previously; (iii) compiling and completing the test incident report, test progress report and test summary report; and (iv) endorsing the test results and the test summary report. (b) B/Ds should ensure that representatives of records users, records managers and other RM staff would participate in the test so that their views and comments can be solicited.

Conduct testing of an ERKS

3.5 During the tests of an ERKS, the responsible officers or the Test Group, if established, should conform to the following procedures -

(a) exercising due diligence to test the ERKS according to the test specifications and test cases;

(b) completing each test case as appropriate;

(c) recording the outcome of each test case and any screenshots or other information required;

(d) recording any error or exception reported by the ERKS during testing;

(e) attempting to determine the reason for failure to pass the expected result of a test case; and

(f) deciding, based on the causes of failure of a test case, whether to simply re-test a failed test case, or whether the issue/problem is to be fixed by the contractor.

Consolidate evaluation results of an ERKS

3.6 On the basis of the testing results of an ERKS, a B/D should assess whether the ERKS achieves full compliance as prescribed in paragraph 2.18. If not, the B/D concerned should identify which parts of the ERKS functionality should be improved and resolve the problems identified in the testing; and critically consider whether the ERKS should be accepted in the context of system acceptance. Appropriate measures, e.g. bugs fixing, system improvements and/or enhancements should be taken timely to rectify the problems identified. In the meanwhile, B/Ds should not dispense with the print-and-file practice.

3.7 Re-testing should be arranged after the improvements/ enhancements have been successfully implemented. B/Ds should note that more than one re-testing may be required until and unless the affected system functionality has been testified as acceptable. In some circumstances, B/Ds should consider undertaking a full-scale re-testing if significant deficiencies/gaps have been identified in the ERKS functionality. B/Ds should properly document the results of re-testing and consolidate the findings into the test summary report.

Evaluate departmental RM policies, practices and procedures

3.8 To evaluate how well departmental RM policies, practices and procedures governing the use, management and maintenance of an ERKS support proper management of records, B/Ds should plan for the evaluation by conducting the following activities -

Activity	Points to note
1. Determine the scope of the evaluation	B/Ds should go through the checklist at **Appendix 3** to determine whether any RM issues specific to their organisations should be added to the checklist for evaluation.
2. Determine the stakeholders to be involved in the evaluation	B/Ds should involve records managers, other RM staff and representatives of records users in the evaluation so that their views and feedback can be solicited.
3. Draw up a schedule and documentation for conducting the evaluation	As an evaluation plan of departmental RM policies, practices and procedures is quite different from a test plan of an ERKS, B/Ds should separately draw up the evaluation plan documenting the scope, methodology and parties involved in the evaluation. A sample of an evaluation plan is provided at **Appendix 5**.
4. Plan activities to help conduct the evaluation	B/Ds may consider conducting focus groups interviews, surveys, documentation review and on-site inspections to assess the implementation and extent of enforcement of departmental RM policies, practices and procedures governing the use, management and maintenance of an ERKS.
5. Assign roles and responsibilities for conducting the evaluation	DRMs of B/Ds should take the lead in conducting the evaluation and consolidate the findings of the evaluation.

3.9 In conducting the evaluation, the responsible parties should complete the self-assessment checklist at **Appendix 3** by -

(a) checking and verifying relevant documentation to assess whether they cover all key RM functions, processes and activities as specified in the checklist at **Appendix 3**, e.g. the availability of an internal circular promulgating the departmental RM policies;

(b) auditing the execution of RM functions, activities and processes by RM staff and records users (Note: B/Ds may consider making surprise checks on site.);

(c) verifying whether staff members have strictly followed RM practices and procedures by reviewing RM activities performed in an ERKS. For example, B/Ds may check whether recordkeeping metadata have been created and captured in accordance with pre-defined guidelines; and

(d) interviewing RM staff and records users to assess whether they are fully aware of their roles and responsibilities and their understanding of the departmental RM policies, practices and guidelines.

3.10 B/Ds should properly document the results of the evaluation in the checklist at **Appendix 3** and propose recommendations and improvement as appropriate.

Consolidate evaluation results of departmental RM policies, practices and procedures

3.11 Based on the findings of the evaluation specified in paragraphs 3.8 to 3.10, a B/D should properly document the evaluation results in Part II and recommendations in Part III respectively of the checklist at **Appendix 3** and determine the appropriate rating of the effectiveness of their departmental RM policies, practices and procedures as specified in paragraph 2.21. The B/D concerned should identify which RM functions, activities and processes should be improved and take prompt actions to address the identified gaps, inadequacies and problems.

Draw up a compliance assessment report

3.12 Upon completion of the evaluation of an ERKS and departmental RM policies, practices and procedures, a **compliance assessment report** should be drawn up. The report should summarise the results, findings and recommendations of the evaluations, including the recommended ratings of the ERKS being evaluated and the effectiveness of departmental RM policies, practices and guidelines. A sample of the compliance assessment report is provided for reference at **Appendix 7**.

3.13 B/Ds should designate an officer **not below the rank of Senior Executive Officer or equivalent** to prepare the report. The responsible officer should consult keys stakeholders including DRM and Head of ITMU

about the contents of the compliance assessment report and document their comments and views in the report.

Seek endorsement of compliance assessment report

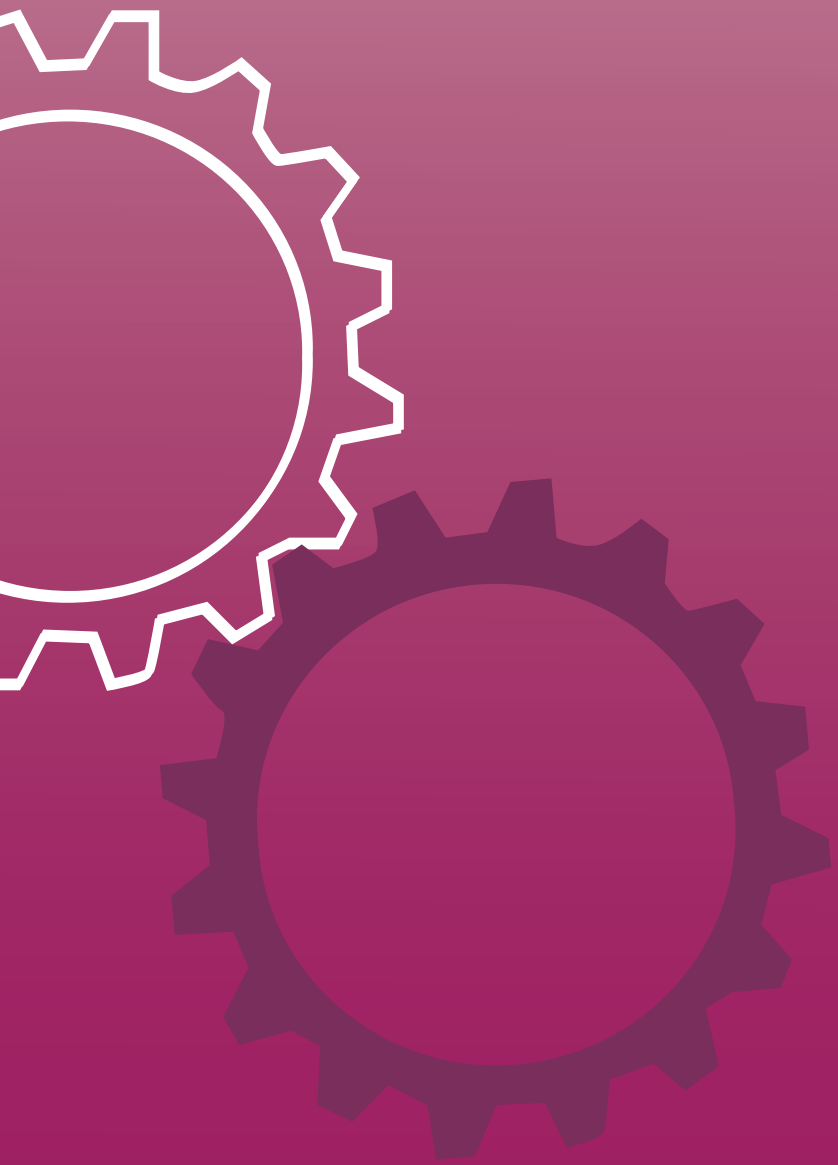
3.14 As stipulated in paragraph 2.28, B/Ds should designate a **directorate officer** to approve the findings and recommendations of a compliance assessment and the compliance assessment report. The approving officer should also oversee the implementation of system improvements/enhancements and other recommendations as set out in the compliance assessment report.

Implement improvements

3.15 Based on the findings and recommendations of a compliance assessment, B/Ds should rectify the problems identified and where appropriate make improvements to the ERKS being evaluated and/or departmental RM policies, practices and procedures. The actions taken should be properly documented and duly reported to the approving officer as specified in paragraph 3.14 for his/her endorsement.

Chapter 4

DISPENSING WITH THE PRINT-AND-FILE PRACTICE



4

Chapter 4 Dispensing with the Print-and-File Practice

Introduction

4.1 This chapter sets out the procedures for B/Ds which have fully implemented a proper ERKS to seek GRS' prior approval for dispensing with the print-and-file practice in managing e-mail records.

Mandatory print-and-file practice

4.2 GC No. 2/2009 entitled "**Mandatory Records Management Requirements**" stipulates, among others, that e-mail correspondence should be "printed-and-filed" for record purposes unless otherwise agreed by GRS. Subject officers should arrange to print an e-mail record directly from the e-mail software for filing in an appropriate paper file similar to other records. This is to ensure that e-mail records pertinent to the decision making process, formulation of policies and procedures and transaction of business should be managed and kept properly to serve as evidence of such business pending the full implementation of a proper ERKS in B/Ds.

Seeking approval from GRS

4.3 On the basis of the results of a compliance assessment, a B/D may make a request to seek GRS' agreement to dispense with the print-and-file practice in managing e-mail correspondence **only if the following conditions have been fully met** -

(a) an ERKS has achieved "**full compliance**" as prescribed in paragraph 2.18; and

(b) the B/D concerned has obtained the "**good**" rating as prescribed in paragraph 2.21 in terms of implementing and enforcing departmental RM policies, practices and procedures governing the use, management and maintenance of the ERKS.

4.4 A B/D should make a request for dispensing with the print-and-file practice in its entire organisation in one go unless otherwise agreed by GRS in advance. In the event that a B/D intends to seek approval to get rid of the print-and-file practice in a progressive manner to tie in with the phased implementation approach of an ERKS in its organisation, the B/D concerned

should submit its ERKS implementation plan to GRS for consideration. GRS will consider the merits of each case and agree with the B/D concerned the proper timing to submit a request(s) to GRS for processing.

4.5 The request should be signed by the DRM of the B/D concerned and be submitted in the form as specified at **Appendix 8** together with the following supporting documentation to GRS for consideration -

(a) a copy of system manual documenting the system functionality of an ERKS[24];

(b) a copy of application user manual which includes both user and administrator functions of an ERKS;

(c) a copy of finalised test plan(s), test specifications including test cases, test procedures and test data of an ERKS;

(d) a copy of a compliance assessment report in the form of **Appendix 7** documenting the results of a compliance assessment, of which a duly completed **Appendix 3** should be attached;

(e) a copy of departmental RM policies, practices and procedures governing the use, management and maintenance of an ERKS; and

(f) any other relevant considerations warranting the attention of GRS but have not been included in (a) to (e) above.

GRS' responsibility

4.6 Upon the receipt of a request from a B/D to dispense with the print-and-file practice, GRS will review the documentation and evaluation results of the compliance assessment submitted. If needed, GRS may require the B/D concerned to conduct a demonstration of the ERKS functionality on site to GRS representatives and provide additional information about the ERKS and its departmental RM policy, practices and procedures.

4.7 In the meantime, the B/D concerned should adopt a parallel run of the ERKS and the print-and-file practice until it has obtained the **prior agreement of GRS** to dispense with the practice. GRS will notify the B/D concerned in writing if agreement is given for it to dispense with the print-

[24] In case a B/D implements an integrated electronic information management (EIM) solution including an ERKS and other EIM modules, the B/D concerned should clearly indicate the system functionality of the ERKS in the system manual.

and-file practice with effect from a specified date. For a refusal case, GRS will provide advice and recommendations for the B/D concerned to make improvements. Upon the satisfactory completion of the improvement measures, the B/D concerned may make a fresh request to GRS to discard the print-and-file practice.

4.8 B/Ds should allow a lead time of about three months for GRS to process a case after they have submitted all required documentation specified in paragraph 4.5 to GRS, and the processing time may be lengthened for complex cases.

Chapter 5

ON-GOING MONITORING AND REVIEW

5

Chapter 5 On-going Monitoring and Review

Introduction

5.1 This chapter advises B/Ds to put in place suitable administrative arrangements to monitor and review on-going use, management and maintenance of an ERKS and continuous enforcement of departmental RM policies, practices and procedures across their organisations.

Regular reviews and continuous monitoring

5.2 On-going monitoring and review are essential for ensuring that an ERKS is operating properly and being managed in accordance with the Government's and departmental RM and IT policies, requirements, practices and procedures, so as to maintain the authenticity, integrity, reliability and usability of records managed by the ERKS.

5.3 B/Ds should monitor and review the ERKS functionality and the associated departmental RM policies, practices and procedures on a regular basis having regard to changes to the legal, business, accountability and evidence requirements. When effecting major enhancement to the functionality of the ERKS, B/Ds should critically review whether the proposed enhancement would result in failure of the ERKS in obtaining the ratings of "**full compliance**" and "**good**" as specified in paragraphs 2.18 and 2.21 respectively. In particular, B/Ds should review whether any changes in system functionality, operation and management of the ERKS would affect the authenticity, integrity, reliability and usability of records managed by the ERKS. B/Ds should adopt the compliance assessment approach specified in **Chapters 2** and **3** to conduct the review. **In any event, a review should be conducted at least once every three to four years or more often as required**, e.g. after a major system upgrade or serious security breach incidents.

5.4 In the course of conducting the review set out in paragraph 5.3, a B/D may identify the need for improvements and/or system enhancements. The B/D concerned should ensure that timely measures and actions are taken to implement improvements and/or system enhancements. Remedial measures and actions taken should be properly documented to demonstrate the B/D's commitment to and effectiveness of ensuring the compliance of its ERKS with the Government's RM policy and ERM requirements. This will in

turn demonstrate that records managed by the ERKS are authentic, complete, reliable and usable.

5.5 The results and findings of a review should be properly documented. If the findings of a review reveal that an ERKS and/or the departmental RM policies, practices and procedures fail to obtain the ratings of "**full compliance**" and "**good**" as specified in paragraphs 2.18 and 2.21 respectively, the B/D concerned should notify GRS immediately in writing and propose recommendations for improvement and rectification.

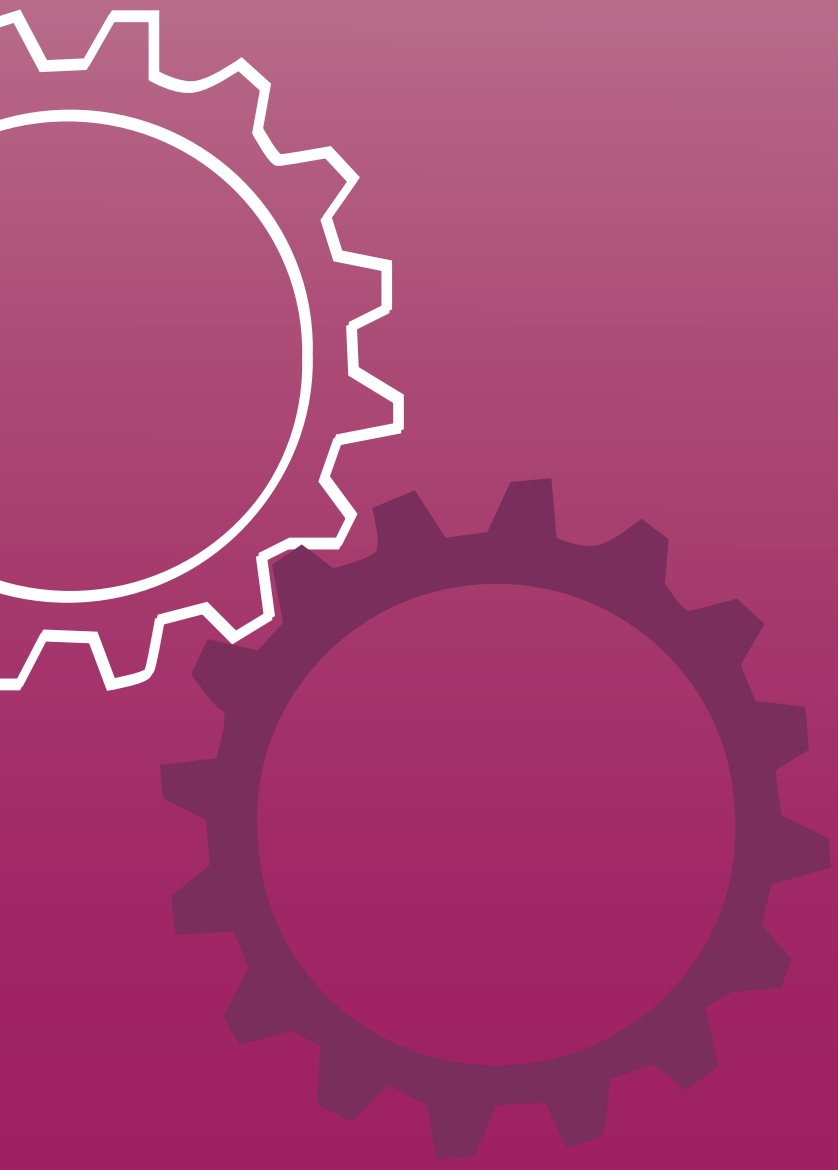
5.6 During day-to-day operations, B/Ds should put in place adequate and suitable measures and practices to monitor proper use, management and maintenance of an ERKS. For example, B/Ds may verify whether staff members have strictly followed departmental RM practices and procedures by conducting random checks on RM activities performed in their ERKSs.

Assistance and support from GRS

5.7 For review purpose, GRS may from time to time require B/Ds to produce the findings of reviews of their ERKSs for scrutiny and make on-site inspections of the operation and management of their ERKSs. In the event that GRS is not satisfied that an ERKS is being used and/or managed properly, GRS will provide advice to the B/D concerned to rectify the problems identified and make necessary improvements. If deemed necessary, GRS may require the B/D concerned to resume the print-and-file practice until satisfactory resolution of the identified problems and inadequacies.

****

APPENDICES



APPENDICES

Appendix 1	Evaluation of an electronic recordkeeping system for compliance with the ***Functional Requirements of an Electronic Recordkeeping System***
Appendix 2	Evaluation of an electronic recordkeeping system for compliance with the ***Recordkeeping Metadata Standard for the Government of the Hong Kong Special Administrative Region***
Appendix 3	Evaluation of the implementation and enforcement of proper departmental RM policies, practices and procedures for effective management of records in an electronic recordkeeping system
Appendix 4	A sample test plan of an ERKS
Appendix 5	A sample evaluation plan of departmental RM policies, practices and procedures
Appendix 6(a) to (c)	Sample test case 1, sample test case 2 and test case template
Appendix 7	A sample compliance assessment report
Appendix 8	Request form for dispensing with the print-and-file practice

Appendix 1

Evaluation of an electronic recordkeeping system for compliance with the Functional Requirements of an Electronic Recordkeeping System

Part I - Overview

This appendix provides guidelines for bureaux and departments (B/Ds) to evaluate the compliance of an electronic recordkeeping system (ERKS) with the requirements specified in the ***Functional Requirements of an Electronic Recordkeeping System*** (FR of an ERKS) (version 1.2) developed by the Government Records Service (GRS) to ensure the authenticity, integrity, reliability and usability of records managed by an ERKS[1].

2. In line with the established practice for IT project management, an ERKS, like other computer systems, should be tested according to the pre-defined **technical, non-functional and functional requirements** prior to system acceptance to assure the quality of the ERKS. As far as an ERKS is concerned, B/D should ensure that it fully meets the **mandatory** functional requirements of FR of an ERKS. In case there are inconsistencies between this appendix and FR of an ERKS, B/Ds should seek advice from GRS.

3. To assist B/Ds in evaluating how well an ERKS complies with the requirements specified in FR of an ERKS, a total of **341** key checkpoints have been specified in Part II. On the basis of these checkpoints, B/Ds should develop comprehensive test cases, test procedures and test data that specifically suit their business, operational and records management context to evaluate the ERKS functionality thoroughly in the context of system acceptance tests and user acceptance tests of an ERKS. B/Ds may add other checkpoints if deemed necessary. Two sample test cases with a template for developing test cases are attached at **Appendix 6 (a) to (c)** for reference by B/Ds. For existing ERKSs, B/Ds should conduct a compliance assessment according to the circumstances set out in paragraph 2.9 of **Chapter 2**.

4. Upon completion of a testing of an ERKS, B/Ds should determine the appropriate rating of the ERKS as prescribed in paragraph 2.18 of **Chapter 2**.

---

[1] Please read Appendix 2 for guidelines to evaluate the compliance of an ERKS with requirements as specified in the ***Recordkeeping Metadata Standard for the Government of the Hong Kong Special Administrative Region*** (RKMS).

5. Key records management terms used in this appendix are consistent with those of FR of an ERKS. Please refer to **Appendix 1** to FR of an ERKS for a glossary of key records management terms.

Part II - Key checkpoints

6. Key checkpoints specified below are largely presented according to the sequence of functional requirements specified in FR of an ERKS. These checkpoints do not cover **technical and non-functional requirements** of an ERKS. As with other IT systems, **Information Technology Management Units (ITMUs)** of B/Ds should develop separate checkpoints and test cases to evaluate technical and non-functional requirements such as system performance, scalability, integrity, reliability, ease of use, etc. of an ERKS.

7. A total of **341** specific checkpoints set out in Part II are grouped under the following **nine** broad categories of recordkeeping functions common to B/Ds -

Category	Checkpoint (C)
Mandatory requirements *of FR of an ERKS*	
(a) **Records classification and identification**	C(1) - C(81)
(b) **Capture**	C(82) - C(131)
(c) **Use of records**	C(132) - C(180)
(d) **Security and access control**	C(181) - C(235)
(e) **Retention and disposal**	C(236) - C(281)
(f) **Metadata** (Note: **Part II** only covers checkpoints relating to metadata as specified in FR of an ERKS. Other checkpoints relating to creation, capture, use, management and maintenance of recordkeeping metadata as specified in RKMS are included in **Appendix 2**.)	C(282) - C(292)
(g) **Language support**	C(293) - C(296)
(h) **Administration**	C(297) - C(329)
Optional requirements *of FR of an ERKS*	
(i) **Workflow**	C(330) - C(341)
	Total: 341

8. Checkpoints by different categories of recordkeeping functions are set out in the table below. Readers are requested to note that -

(a) "**the ERKS**" mentioned in individual checkpoints refers to the ERKS being tested and evaluated;

(b) the term "**attempt**" is used when the ERKS, a user or an authorised individual as appropriate shall attempt to execute an action though it is expected that the ERKS must deny such execution. There may exist different ways in which the ERKS denies actions;

(c) the term "**test**" is used when the ERKS, a user or an authorised individual as appropriate shall execute an action and it is expected that the action shall be successfully completed;

(d) B/Ds should assume that there is more than one authorised individual in their organisations. Authorised individuals may have access to different records classification schemes (if multiple records classification schemes have been implemented), different parts of a records classification scheme and/or different system functions according to their roles. For example, an authorised individual may include the Departmental Records Manager, records managers, registry staff and system administrator(s); and

(e) for those functional requirements such as **Requirement 6** that explicitly stipulate that an ERKS must support an authorised individual to perform specific RM functions, B/Ds should ensure that suitable test cases are developed to test whether the ERKS denies users (other than an authorised individual) performing such functions. Checkpoints specified below generally do not repeat the requirement of developing test cases for the stated purpose.

(a) Records Classification and Identification			
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**	
1	The ERKS must -		
	(a) support the classification and organisation of records[3] within a structured records classification hierarchy based on function and/or subject;	C(1)	Test whether the ERKS supports representation of a records classification scheme, by which classes, sub-classes, folders (including electronic folders, hybrid folders and physical folders), sub-folders (if implemented) and parts are placed in a hierarchical structure, consistent with the nature of the records classification scheme.
	(b) support a pre-defined records classification scheme in a hierarchical structure with at least **five** levels (down to folder level) below the root[4] of the records classification scheme; and	C(2)	Test whether the ERKS supports the creation and establishment of a records classification scheme with **at least five levels down to the folder level** in a hierarchical structure. The number of levels to be included in the test cases should reflect the actual design of the records classification scheme of the B/D concerned and cater for possible future expansion.
		C(3)	Test whether the ERKS supports **varying levels**, say three, four, five and six levels, in various parts of a records

[2] Mandatory functional requirements include non-conditional and conditional mandatory functional requirements of an ERKS. Conditional mandatory functional requirements are identified by the use of the prefatory phrase "***Where***...".

[3] Records include electronic records and non-electronic records as specified in FR of an ERKS unless specified otherwise.

[4] The root level here represents the starting point where the records classification scheme is constructed.

(a) Records Classification and Identification			
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**	
			classification scheme. For example, some parts of the records classification scheme may use three levels, other may use five levels.
	(c) support browsing and graphical navigation of the records classification scheme structure and records aggregations, and the selection, retrieval and display of aggregations and their contents through this mechanism.	C(4)	Test whether different users with specified access rights are able to browse and navigate the records classification scheme created in the ERKS. A graphical representation of the records classification scheme should be supported so that users can intuitively follow the flow of the hierarchical structure of the records classification scheme to locate aggregations and/or records as required, and access the contents of aggregations and/or records and their metadata as appropriate. Assuming that all these users do not have access rights to all parts of the records classification scheme, they should **only** be allowed to browse and navigate those parts that they have the access rights.
		C(5)	Test whether authorised individuals and users of different roles and responsibilities are able to select and retrieve different classes, sub-classes, folders, sub-folders (if implemented) and parts according to their access rights by way of the records classification scheme.
		C(6)	Regarding C(5), test whether the ERKS displays the

(a) Records Classification and Identification			
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**	
			contents of selected aggregations to authorised individuals and users. For example, if a user selects a folder in the records classification scheme, the ERKS should be able to show the contents (i.e. part(s) contained in the folder) to him/her.
		C(7)	Test whether the ERKS distinguishes and displays different levels of aggregations in a clear manner. For example, different icons are used to denote different levels of aggregations for easy identification by users.
	*[Note: Please read **Requirement 2** in conjunction with this requirement. An illustration showing the hierarchical structure and the relationships of aggregations within a fictitious records classification scheme is at **Appendix 2** to **FR of an ERKS**.]*		
2	***Where*** B/Ds choose to adopt more than one records classification scheme in the ERKS[5] to manage records, including administrative and programme records, the	C(8)	Test whether the ERKS supports creation of **three or more records classification schemes** with -

[5] If a B/D chooses to adopt a single departmental records classification scheme to manage records, including both administrative and programme records, it may consider selecting an ERKS to support only one records classification scheme. However, the B/D should note that it may be difficult to enhance such an ERKS to support multiple records classification schemes subsequently, e.g. division of the single departmental records classification scheme into two or more. The implications of adopting an ERKS that supports only one single records classification scheme should be critically assessed prior to taking such course of action and the Departmental Records Manager of the B/D should be consulted in this regard.

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
	ERKS must support the definition and simultaneous use of multiple records classification schemes in the ERKS. *[Note: Please read this requirement in conjunction with **Requirement 1**.]*	(a) different classification coding systems such as alphabetic, alpha-numeric and numeric systems; (b) different levels of aggregations; (c) different naming conventions of aggregations (e.g. some folders are titled by a name of a person plus a unique identifier of that person such as a staff ID number while some folders are named by a project title plus the commencement date of the project); and (d) different hierarchical structures within a single ERKS. C(9) Test whether the ERKS supports creation of **three or more records classification schemes** with - (a) same classification coding systems such as alphabetic, alpha-numeric and numeric systems; (b) same levels of aggregations; (c) same naming conventions of aggregations; and (d) same hierarchical structures within a single ERKS.

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
		C(10) Regarding C(8) and C(9), test whether an authorised individual is able to create, browse and navigate different aggregations (including electronic folders, hybrid folders, physical folders, sub-folders (if implemented) and parts) in all the records classification schemes. It is assumed that the authorised individual has access rights to and sufficient security clearance for the records classification schemes. C(11) Regarding C(8) and C(9), test whether different users are able to browse, navigate, search, select and retrieve different aggregations in the records classification schemes and capture records into the records classification schemes according to their access rights. It is assumed that the users have different access rights to the records classification schemes. Please include test cases under which a user captures records into three or more records classification schemes according to his/her access rights and the ERKS should support such execution of capturing of records. Please see also C(187).
3	The ERKS must - (a) support the initial and on-going construction, and	C(12) Test whether the ERKS supports the initial construction of a records classification scheme before folders and

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
	modification of a records classification scheme, including re-classification of aggregations[6], merging of records classification schemes[7] and modification[8] to classification codes and titles, etc.; and (b) notify an authorised individual if an action[9] under (a) will affect other levels in the hierarchy or other related records where appropriate.	records are added so as to demonstrate an initial overall design. C(13) Test whether the ERKS supports construction of parts of a records classification scheme such as creating one class with a number of child sub-classes and folders for capturing of records. Then continue to create the rest parts of the records classification scheme such as creating another three classes with a number of child sub-classes and folders. This is to test the scalability of a records classification scheme. C(14) Test whether the ERKS supports re-classification of a whole **sub-class**, including all child sub-classes, folders (including open and closed folders), sub-folders (if implemented, including open and closed sub-folders), parts (including open and closed parts) and records falling under that sub-class from a **class** of a records classification scheme to another **class** in the same

[6] Re-classification of aggregations may involve movement of aggregations from one position in a records classification scheme to another position of the same records classification scheme or from one records classification scheme to another records classification scheme established in the ERKS where multiple records classification schemes are adopted. The ERKS must ensure that all electronic records already allocated remain allocated to the aggregations (including parts) being relocated.

[7] The term "merge" used in this document is to be understood as when two records classification schemes are combined into one single records classification scheme.

[8] The ERKS must support making changes (including add, modify and delete) to the classification codes and titles of aggregations.

[9] For example, a change to the classification code of a sub-class will affect the classification code of all its child sub-classes.

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
		records classification scheme in a single operation. Test also re-classification of a whole **sub-class**, including all child aggregations and records falling under that sub-class from a **sub-class** of a records classification scheme to another **sub-class** in the same records classification scheme in a single operation. It is **not** acceptable for the ERKS to re-classify aggregations one by one for meeting **Requirement 3(a)**. Please see also C(49) to C(56). C(15) Test whether the ERKS supports re-classification of a **folder**, including all child sub-folders (if implemented, including open and closed sub-folders), parts (including opened and closed parts) and records falling under that folder from a **sub-class** of a records classification scheme to another **sub-class** in the records classification scheme in a single operation. It is **not** acceptable for the ERKS to re-classify sub-folders (if implemented), parts or records one by one for meeting **Requirement 3(a)**. Please see also C(49) to C(56). C(16) Test whether the ERKS provides an effective mechanism for an authorised individual to merge two records classification schemes (with classes, sub-classes, folders, sub-folders (if implemented), parts and records) into one

(a) Records Classification and Identification			
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**	
			records classification scheme. The effective mechanism should minimise manual efforts and errors. For the purpose of meeting the requirement to merge two records classification schemes, it is **not** acceptable to require an authorised individual to relocate aggregations singly so as to complete the whole process of merging.
		C(17)	Regarding C(12) to C(16), test whether the ERKS provides notifications to the authorised individual where appropriate that actions under **Requirement 3(a)** would affect other levels in the hierarchy or other related records in the processes of re-classification, merging and modification. The purpose of such notification is to ensure that the authorised individual would be able to make an informed decision whether to proceed with the selected actions.
4	The ERKS must -		
	(a) automatically assign a unique system identifier to each aggregation and record and ensure that the identifier is persistently linked to the aggregation and the record; and	C(18)	Ask the contractor to advise the **coding convention** of the system identifier assigned to an aggregation and a record and examine whether such coding convention will ensure **the uniqueness of the system identifier within the ERKS**. In case a B/D has implemented multiple

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
		repositories, the unique system identifier assigned to an aggregation or a record should remain unique across the different repositories. C(19) Test whether the ERKS **automatically** assigns a unique system identifier to each aggregation upon the creation of the aggregation. The ERKS should **not** require an authorised individual or a user to assign such system identifier or ask them to confirm whether such system identifier should be provided to an aggregation. C(20) Test whether the ERKS **automatically** assigns a unique system identifier to each record upon the creation/capture of the record. The ERKS should **not** require an authorised individual or a user to assign such system identifier or ask them to confirm whether such system identifier should be provided to a record.
	(b) allow an authorised individual to assign a classification code and allocate a textual title for each aggregation.	C(21) Test whether the ERKS supports an authorised individual to **assign a classification code to aggregations manually and/or automatically** according to the preference of the B/D concerned. C(22) Test whether the ERKS supports an authorised individual to provide a title in text and a unique classification code

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
		in string (supporting alphabetic, alpha-numeric and numeric codes) to each aggregation except for parts. This task should be done during the process of creating an aggregation. *[Note: The classification code of a part is the same as that of its parent folder or sub-folder (if implemented) as appropriate. To identify each part within a folder or a sub-folder, a value in string will be assigned to its metadata element "Part number".]* C(23) Test whether the ERKS automatically assigns a classification code to each newly-created aggregation if automatic numbering is adopted as the default method. C(24) Test whether the ERKS supports an authorised individual to **configure the structure of classification codes and naming convention of aggregations**. For example, an authorised individual configures the classification codes to 4 tiers such as "Adm-000-000-000" with the first three tiers are assigned according to classes and sub-classes of a records classification scheme while the last tier is a sequential running number for folders.

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
5	The ERKS must support an authorised individual to define and create aggregations of different levels[10] and folders of different types, including but not limited to the following -	
	(a) electronic folder for electronic records only;	C(25) Test whether the ERKS supports an authorised individual to define the type of folder as an "electronic folder", associated system functionality to manage electronic folders and the metadata profile of an electronic folder.
	(b) hybrid folder for both electronic and non-electronic records; and	C(26) Test whether the ERKS supports an authorised individual to define the type of folder as a "hybrid folder", associated system functionality to manage hybrid folders and the metadata profile of a hybrid folder. The ERKS should enable users to easily identify which records are electronic records or non-electronic records within a hybrid folder.
	(c) physical folder for non-electronic records only	C(27) Test whether the ERKS supports an authorised individual to define the type of folder as a "physical folder",

[10] Aggregations are created from the class (i.e. the highest level), sub-class, folder to the part (i.e. the lowest level). RKMS introduces one more type of aggregation, namely a sub-folder which is used primarily to classify records of a case nature into more refined groups of records based on the intellectual contents of the records for easy retrieval (see Chapter 3 of RKMS for details). The use of sub-folders is **optional**. ***Where*** B/Ds choose to implement sub-folders in an ERKS, all functionality applicable to a folder set out in FR of an ERKS applies to a sub-folder as well.

(a) Records Classification and Identification			
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**	
			associated system functionality to manage physical folders and the metadata profile of a physical folder. For example, the ERKS should ensure that defined metadata elements for physical folders are displayed to users.
	in the records classification scheme without a practical limit, and manage both electronic and non-electronic records in (b) above in an integrated manner.	C(28)	Examine whether the ERKS design or architecture (e.g. underlying database technology) imposes or has the effects of limiting the total number of classes, sub-classes, folders, sub-folders (if implemented) and parts within the ERKS. While it is acceptable to enhance hardware to cater for increasing quantity of aggregations and records, it is **not** acceptable for the ERKS to pre-determine the total quantity of aggregations and records that can be managed and stored within an ERKS.
		C(29)	Ask the contractor to advise whether there is a practical limit for creation or import of aggregations into the ERKS. The ERKS should **not** impose a limit on the number of aggregations to be created or imported into the ERKS.
		C(30)	Ask the contractor to advise whether there is a practical limit on creation of parts within a folder, parts within a sub-folder (if implemented), sub-folders (if implemented)

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
		within a folder, folders within a sub-class, sub-classes within a sub-class, sub-classes within a class and classes within the ERKS. The ERKS should **not** impose a limit on the number of child aggregations to be created in an aggregation. C(31) Ask the contractor to advise whether there is a practical limit for creation, capture or import of records in the ERKS. The ERKS should **not** impose a limit on the number of records to be created, captured or imported into the ERKS. C(32) Test whether the ERKS supports an authorised individual to create different aggregations, including a class, sub-class, folder, sub-folder (if implemented) or a part. C(33) If an authorised individual attempts to create - (a) a class under a class, a sub-class, a folder, a sub-folder (if implemented) or a part; (b) a sub-class under a sub-class containing a folder(s), a folder, a sub-folder (if implemented) or a part; (c) a folder under a class or a sub-class containing a sub-class(es) direct, a folder, a sub-folder (if implemented) or a part;

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
		(d) a sub-folder (if implemented) under a class or a sub-class direct, a folder containing a part(s), a sub-folder or a part; and (e) a part under a class, a sub-class, a folder containing a sub-folder(s) (if implemented) direct or a part, the ERKS must deny all these actions. C(34) Test whether the ERKS manages electronic and non-electronic records in an integrated and seamless manner, including assigning title and metadata, searching, retrieving, assigning security and access control, and establishing records retention and disposal schedules for electronic and non-electronic records. C(35) Test whether the ERKS supports users with access rights to and security clearance for a part that contains both electronic and non-electronic records to view metadata of both electronic and non-electronic records within this part. C(36) Test whether the ERKS supports users to search and retrieve the contents and metadata of electronic folders, hybrid folders and physical folders in a single retrieval process.

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
		C(37) Test whether the ERKS distinguishes and displays different types of folders (including electronic folders, hybrid folders and physical folders) and sub-folders (if implemented) clearly to users.
6	The ERKS must support an authorised individual to perform on-going records management functions, including but not limited to the following -	
	(a) opening and closing aggregations including folders and parts;	C(38) Test whether the ERKS supports an authorised individual to open (i.e. to allow a class, sub-class, folder and sub-folder (if implemented) to accept the additions of child aggregations or to allow a part to accept the additions of records) an aggregation. The ERKS should allow the opening date of a folder, a sub-folder (if implemented) or a part to be chronologically earlier than the creation of the folder, the sub-folder or the part in the ERKS. C(39) Test whether the ERKS supports an authorised individual to close (i.e. to prevent a class, sub-class, folder and sub-folder (if implemented) from accepting the addition of child aggregations or to prevent a part from accepting the addition of records) but still allows access to the

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
		aggregations. For example, the display and retrieval of the contents of a closed folder with all its child parts should be unaffected. C(40) If the ERKS supports automatic closure of an aggregation based on pre-defined criteria such as closing a part upon the closure of a financial year, test whether the ERKS is capable of closing an aggregation upon the fulfilment of the pre-defined criteria. C(41) Test whether the ERKS automatically closes all parts of a folder upon the closure of that folder by an authorised individual. C(42) If an authorised individual attempts to create an aggregation under a closed aggregation, e.g. a folder under a closed sub-class, the ERKS must deny such action. C(43) If a user attempts to capture a record under a folder, sub-folder (if implemented), sub-class or class direct, the ERKS must deny all these actions. C(44) Except for authorised persons, if a user attempts to capture a record into - (a) a closed part of an open folder; and

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
		(b) a closed part of an open sub-folder (if implemented), the ERKS must deny all these actions. C(45) Except for authorised persons, if a user attempts to capture a record into - (a) a part of a closed folder (i.e. under which all parts should be automatically closed upon the closure of the folder); and (b) a part of a closed sub-folder (if implemented) (i.e. under which all parts should be automatically closed upon the closure of the sub-folder), the ERKS must deny all these actions. C(46) Test whether the ERKS supports an authorised individual to capture a record into - (a) a closed part of an open folder; and (b) a closed part of an open sub-folder (if implemented). Depending on the implementation approach, the authorised individual may need to re-open the closed part before capturing the record and closing the re-opened part after capturing the record. In any case, the ERKS should ensure that the date of closure of the

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
		part remains unchanged. *[Note: Under very exceptional circumstances, there may be a need to capture records into a closed part of a folder or a sub-folder (if implemented) to ensure the completeness of records stored in the same part. For instance, financial records created/received in the same financial year may be kept in the same part for easy retrieval. Under the circumstances, there may be operational need to capture financial records received late, say on 5 April into the closed part which is automatically closed on 1 April of that year.]* C(47) Test whether the ERKS supports an authorised individual to capture a record into - (a) a part of a closed folder (i.e. under which all parts should be automatically closed upon the closure of the folder); and (b) a part of a closed sub-folder (if implemented) (i.e. under which all parts should be automatically closed upon the closure of the sub-folder). Depending on the implementation approach, the authorised individual may need to re-open the closed folder, sub-folder and/or part before capturing the

(a) Records Classification and Identification			
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**	
			record and closing the re-opened folder, sub-folder and/or part after capturing the record. In any case, the ERKS should ensure that the dates of closure of the folder, sub-folder (if implemented) and part remain unchanged.
	(b) monitoring and tracking the movement and locations of aggregations and records;	C(48)	Test whether the ERKS provides effective means and features for an authorised individual to record, monitor and track the movement and locations (including home and current locations, date moved from location, date received at location and user responsible for the move) of physical and hybrid aggregations and non-electronic records. Effective means and features here refer to methods that should minimise manual efforts and errors and are user-friendly. Information on the movement and locations of aggregations and records should be easily retrievable. It is **not** acceptable if such information is obtained only in the audit trail data.
	(c) re-classifying aggregations and records in bulk or singly and modifying their classification codes and titles; and	C(49)	Test whether the ERKS supports an authorised individual to re-classify a number of aggregations with records therein in one single operation. For example, an authorised individual re-classifies three folders with child parts and records therein from one sub-class to another

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
		sub-class in one single operation. It is assumed that the authorised individual has access rights to and sufficient security clearance for the aggregations. C(50) Regarding C(49), test whether the ERKS supports an authorised individual to modify titles of aggregations and change the classification codes of the re-classified aggregations manually and/or automatically according to pre-defined rules, e.g. the ERKS automatically assigns new classification codes in numeric format to the re-classified aggregations according to the coding convention of the destination sub-class. Test whether the original classification codes are not re-used in the originating aggregation after the re-classification. For example, if a folder with classification code 003-065-001 is re-classified to another sub-class, then when a new folder is created in the parent sub-class 003-065, the new folder cannot re-use the classification code 003-065-001. This is to avoid confusion as the original classification code may have been quoted in some correspondence. C(51) Test whether the ERKS supports an authorised individual to re-classify an aggregation singly and modify the classification code and title of that aggregation. Test

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
		whether the original classification code of the re-classified aggregation is not re-used in the originating aggregation. C(52) Test whether the ERKS supports an authorised individual to re-classify a number of records in a part in one single operation and then modify the titles of those records. It is assumed that the authorised individual has access rights to and sufficient security clearance for the records. If the ERKS assigns a record number to each record within a part and that record number is only unique within the part, test whether the ERKS supports assignment of a new record number for the re-classified record in the destination part and the original record number of the re-classified record is not re-used in the originating part. C(53) Regarding C(49) to C(52), test whether the data integrity is maintained after the re-classification, for example - (a) the number of aggregations and records should remain unchanged after the re-classification; (b) the relationship between a compound record and its constituent records should be retained after the

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
		re-classification; (c) all records are correctly and persistently linked to their parent parts, parts are linked to their parent folders or sub-folders as appropriate, sub-folders (if implemented) are linked to their parent folders, folders are linked to their parent sub-classes, sub-classes are linked to their parent sub-classes or classes as appropriate after the re-classification; (d) all aggregations that have been closed should remain closed after the re-classification; (e) all aggregations that have been opened should remain opened after the re-classification; (f) recordkeeping metadata are persistently linked to their associated entities, e.g. a folder, after the re-classification; (g) there is a proper and effective mechanism to change the security classifications, access rights and records retention and disposal schedules of the aggregations in bulk after the re-classification. Effective mechanism here means a way or a method that should minimise manual efforts and errors; and

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
		(h) relationships (e.g. cross-references) between aggregations, between records (e.g. between a compound record and its constituent records) and between an aggregation and a record should be retained after the re-classification. C(54) Regarding C(49) to C(52), test whether the ERKS provides a means to record the reason for the re-classification of aggregations and records. C(55) Regarding C(49) to C(52), test whether the re-classification event is documented in the audit trail. The ERKS should provide an effective means for a user to identify whether any records under a part or any aggregations under a position in the records classification scheme have been re-classified to another part or position in the records classification scheme and retrieve the new location of the re-classified aggregation and record. It is preferable that the new location of a re-classified record is traceable in the previous location of that re-classified record. For example, after a record is re-classified from Part 1 of Folder A to Part 2 of Folder B, a user should be able to identify in Part 1 of Folder A that a record has been re-classified and its new location is in Part 2 of Folder B. Similarly, the original location of

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
		the re-classified record should also be traceable in Part 2 of Folder B. C(56) ***Where*** B/Ds choose to adopt more than one records classification scheme in the ERKS, regarding C(49) to C(55), test whether the ERKS supports re-classification of aggregations and records from one records classification scheme to another one.
	(d) adding, updating, modifying and deleting metadata of aggregations and records except for metadata specifically identified as not editable.	C(57) Test whether the ERKS supports an authorised individual to perform the following - (a) adding a new metadata element with specified allowable values other than those specified in RKMS **for a record**. It is assumed that the value of the metadata element is editable; (b) adding a new metadata element with specified allowable values other than those specified in RKMS **for an aggregation**. It is assumed that the value of the metadata element is editable; (c) renaming the new metadata elements created under (a) and (b) above; (d) updating the metadata values such as "Location - current" of a physical part and a non-electronic

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
		record; (e) modifying the metadata values such as classification codes of aggregations and titles of records; (f) deleting the new metadata elements created under (a) and (b) above; and (g) ensuring that metadata values that are not changeable such as "System identifier" prescribed in RKMS remain unchangeable throughout the life cycle of records. Please see also C(284), C(285) and C(290).
7	***Where*** B/Ds choose to implement multiple repositories[11] across multiple locations, the ERKS must -	***Where*** multiple repositories are implemented across multiple locations -
	(a) support an authorised individual to efficiently manage multiple repositories with the required functionality including but not limited to the following -	C(58) Test whether the ERKS supports an authorised individual to efficiently manage **two or more repositories** (depending on the actual number of repositories that a B/D has implemented) across multiple locations. For example, an authorised individual assigns coding systems for a records classification scheme(s) across repositories,

[11] There are different architectural approaches to implement multiple repositories. For example, one instance of an ERKS controls multiple repositories or several instances of an ERKS, each has its own repository(ies), communicating with each other.

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
		access control and security and records retention and disposal schedules to aggregations and records stored in different repositories. C(59) Test whether the ERKS supports an authorised individual to specify which repository(ies) the users can access at each location.
	(i) supporting multiple records classification schemes ***where*** B/Ds adopt more than one records classification scheme across the repositories; or supporting a distributed records classification scheme across a network of repositories ***where*** B/Ds adopt a single records classification scheme[12];	C(60) Test whether the ERKS supports an authorised individual to create two or more different records classification schemes in different repositories (depending on the actual number of repositories that a B/D has implemented). C(61) Test whether the ERKS supports an authorised individual to create one single records classification scheme across the multiple repositories so that users accessing the records and aggregations of the records classification scheme are presented with a seamless, up-to-date view of the records classification scheme regardless of the user's location.
	(ii) adding a new repository and removing a	C(62) Test whether the ERKS supports an authorised individual

[12] Please see footnote 5.

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
	repository;	to add a new repository other than the existing repository(ies). C(63) Test whether the ERKS supports an authorised individual to remove a repository from the existing repositories.
	(iii) preventing or resolving any conflicts caused by changes made in different locations (such as different changes made to the metadata of the same class in different locations);	C(64) Test whether the ERKS prevents or resolves any conflicts caused by changes occurring in the following areas - (a) records classification scheme, e.g. making different changes to the structure of the classification code or the number of levels of the records classification scheme in different locations; or re-classifying a folder from one repository to another repository with different metadata profiles for the entity of folder in these two repositories; (b) capturing of records, e.g. capturing a record to two folders with different access control and security in two repositories. If the ERKS implements a pointer system to link a record to these two folders, test whether the ERKS will prevent or resolve conflicts of different access control and security imposed on the record due to inheritance of different access control and security of the two folders;

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
		(c) recordkeeping metadata, e.g. making different changes to the metadata elements of a folder in different locations and making different changes to the values of an encoding scheme in different locations; (d) audit trails, e.g. making different changes to the configuration of audit trails in different locations; and (e) records retention and disposal schedule, e.g. changing the default retention and disposal schedules of the same class and its child sub-classes in different locations.
	(iv) supporting monitoring [13] of the entire distributed ERKS both as a single entity and individual repositories;	C(65) Test whether the ERKS supports on-line reporting and/or production of pre-defined or ad hoc reports (such as quantitative reports on the number of aggregations or reports on failure etc.) that cover multiple repositories. C(66) Test whether the ERKS supports on-line reporting and/or production of pre-defined or ad hoc reports (such as quantitative reports on the number of aggregations or

[13] The monitoring may be conducted through a reporting tool.

(a) Records Classification and Identification			
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**	
			reports on failure etc.) that cover individual repository.
	(v) supporting propagating any administrative changes across all repositories within reasonable response times[14]; and	C(67)	Test whether the ERKS supports an authorised individual to perform administrative changes such as adding a new metadata element for a record, configuring a metadata element as a searchable field for searching records and carry out maintenance operations once to apply to the entire ERKS within multiple repositories within reasonable response times. ITMUs of the B/D concerned should determine the reasonable response times having regard to the design of the ERKS and IT infrastructure.
		C(68)	Test whether the ERKS supports an authorised individual to reconfigure an action as an auditable event in the audit trail across multiple repositories and examine whether the response times are reasonable.
	(vi) ***where*** the ERKS synchronises repositories, they must be synchronised of, including but not limited to, any change involving aggregations, records and their associated metadata; and	C(69)	***Where*** the ERKS synchronises repositories, test whether the ERKS synchronises actions such as changing the security classifications, classification codes and records retention and disposal schedules of aggregations.

[14] The response times are system dependent.

(a) Records Classification and Identification			
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**	
			Please see also C(67).
	(b) allow transfer of the records classification scheme and all associated data from a local repository to a central repository.[15]	C(70)	Test whether the ERKS supports an authorised individual to transfer a records classification scheme with all classes, sub-classes, folders, sub-folders (if implemented), parts and records from a local repository to a central repository.
8	The ERKS must -		
	(a) support the creation of cross-reference[16] among folders, among records; and among records and folders/parts; and	C(71)	Test whether the ERKS supports **automatic** (based on pre-defined rules as specified by the B/D concerned) **and manual creation** of cross-references such as a hyperlink between - (a) two folders; (b) two sub-folders (if implemented); (c) two records; (d) a record and a folder; (e) a record and a sub-folder (if implemented); and

[15] The number of repositories in an ERKS depends on the implementation approach of B/Ds.

[16] The "cross-reference" must at least be a hyperlink between related folders, between records, and between records and folders/parts.

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
		(f) a record and a part. C(72) Test whether the ERKS supports **automatic** (based on pre-defined rules as specified by the B/D concerned) and **manual creation** of cross-references such as a hyperlink among **three or more** - (a) folders; (b) sub-folders (if implemented); (c) records; (d) records and folders; (e) records and sub-folders (if implemented); and (f) records and parts. C(73) Regarding C(71) and C(72), test whether the ERKS supports users to easily identify and view the cross-references.
	(b) allow removal of the cross-references by an authorised individual.	C(74) Test whether the ERKS supports an authorised individual to remove cross-references between - (a) two folders; (b) two sub-folders (if implemented);

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
		(c) two records; (d) a record and a folder; (e) a record and a sub-folder (if implemented); and (f) a record and a part. C(75) Test whether the ERKS supports an authorised individual to remove all cross-references among three or more - (a) folders; (b) sub-folders (if implemented); (c) records; (d) records and folders; (e) records and sub-folders (if implemented); and (f) records and parts. C(76) Test whether the ERKS maintains the cross-reference between two entities even though the cross-references between three entities have been partially removed. For example, originally record A, record B and record C are cross-referenced with one another, but the cross-reference between record B and record C is removed subsequently. In such circumstances, the

(a) Records Classification and Identification		
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**
		cross-reference between record A and record B and cross-reference between record A and record C should still be maintained.
9	The ERKS must -	
	(a) support inheritance, system generation and automatic capturing of metadata for different levels of aggregations within a records classification scheme during their creation and at subsequent on-going records management activities[17] involving them; and	C(77) Test whether the ERKS supports system generation of specified metadata values e.g. "System identifier" for different levels of aggregations within a records classification scheme during their creation and at subsequent on-going records management activities involving them. Please see also C(80) and C(81). C(78) Test whether the ERKS supports inheritance of specified metadata values e.g. "Owner" for different levels of aggregations within a records classification scheme during their creation and at subsequent on-going records management activities involving them. Please see also C(80) and C(81). C(79) Test whether the ERKS automatically captures metadata for aggregations according to the modes of creation, capturing and inheritance of a core set of aggregation

[17] On-going records management activities include changes made to records retention and disposal schedules, security classification of aggregations, etc.

(a) Records Classification and Identification			
Mandatory functional requirement[2] as specified in FR of an ERKS		**Checkpoint**	
			level metadata as listed at **Appendix 3** to **FR of an ERKS**. Please see also C(80) and C(81).
	(b) support inheritance of metadata belonging to a higher level aggregation, e.g. a sub-class by all its lower level aggregations, e.g. folders and parts.	C(80)	Test whether the ERKS allows but not requires automatic inheritance of metadata belonging to a higher level aggregation by all its child aggregations. For example, during the creation of a folder under a sub-class, the ERKS automatically inherits the value of security classification of the sub-class to the folder but allows an authorised individual to override the value at the point of creating the folder.
		C(81)	Test whether the ERKS supports inheritance of metadata belonging to a higher level aggregation by all its child aggregations. The ERKS should ensure that any new aggregation created under this higher level aggregation inherit the metadata values by default.
	*[Note: The modes of creation, capturing and inheritance of a core set of aggregation level metadata as specified in RKMS are listed at **Appendix 3** to **FR of an ERKS**.]*		

(b) Capture			
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**	
10	The ERKS must enable integration with business applications, e.g. an e-mail system to facilitate records capturing.	C(82)	Test whether the ERKS supports users to capture records directly from the applications/systems that are integrated with the ERKS and classify the records into an appropriate folder(s). For example, users are able to capture records directly from the Lotus Notes E-mail System which provides a capture option for e-mails held within the user's mailboxes (including the inbox and outbox).
		C(83)	***Where*** the ERKS is integrated with a business system to capture structured contents from the latter system, test whether the ERKS supports import of metadata as specified in **Application Profile 2** of **RKMS** and records from the business system.
11	The ERKS must -		
	(a) support a user to capture electronic records [18] including electronic records with multiple components, compound records [19] and	C(84)	Test whether the ERKS supports users to capture an electronic record even though the generating application (i.e. the original software application) is not present.

[18] Electronic records include e-mail records, digitised records (e.g. scanned paper and scanned microfilm records) and other records in digital form such as word-processed documents, spreadsheets, video, audio, etc. unless specified otherwise in FR of an ERKS.

[19] All components of a record and a compound record must be managed as a single unit to ensure the integrity of the record. The relationship between the constituent components of each record and the constituent records of a compound record must be retained.

(b) Capture		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
	non-electronic records[20] into aggregations[21] of the ERKS through user-activated specific action (User Decided Filing)[22]; and	That means the ERKS should support the capture of any electronic record without the need to access any additional software. C(85) Test whether the ERKS supports users to capture an electronic record with one component. Please test capturing of electronic records in different file formats, say the most frequently used ten file formats of the B/D concerned including electronic records in text and document, spreadsheet, image, audio, visual, presentation and multimedia file formats. C(86) Test whether the ERKS supports users to capture an electronic record with multiple components. Please test capturing of electronic records in different file formats, say the most frequently used five (or the number specified by the B/D concerned) file formats of the B/D concerned including electronic records in text and document, spreadsheet, image, audio, visual,

[20] Paper records may be converted into digital images through scanning and then captured into the ERKS as digitised records. For other non-electronic records that are not suitable for conversion into a digital form, the ERKS must support users to record their metadata in the ERKS.

[21] The ERKS must allow users to classify a record to multiple aggregations.

[22] To support automatic capturing of records, B/Ds may consider, among other means, adopting forced filing under which the capturing process can be automatically initiated, e.g. upon receipt of or sending out an e-mail message.

(b) Capture		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		presentation and multimedia file formats. C(87) Regarding C(86), the ERKS should ensure that - (a) the original structure of the record with multiple components is maintained and users must be able to retrieve and display the record contents in the same manner as observed in the original record; (b) the structural integrity and component relationships within the record are maintained; (c) all components must be re-classified as part of a single action on re-classification of the record with multiple components; and (d) all components must be destroyed as part of a single action on destruction of the record with multiple components. C(88) Test whether the ERKS supports users to capture compound records including an e-mail with multiple attachments. For example, test the capture of an e-mail with ten attachments. C(89) Regarding C(88), the ERKS should ensure that the constituent records of a compound record be managed as a single unit to ensure the integrity of records. For

(b) Capture		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		example, retrieval of a constituent record of a compound record will display all other constituent records of this compound record to users as well; and application of an appropriate records retention and disposal schedule consistently across the constituent records of the compound record. On re-classification of the compound record, all constituent records must be re-classified in a single action. On destruction of the compound record, all constituent records must be destroyed as part of a single action.
		C(90) Test whether the ERKS supports capturing of the file format of an electronic record in the metadata profile of the record together with other required metadata as specified in **Annex 3** of **RKMS**. To capture the file formats of electronic records, the ERKS may need to use tools such as Digital Record Object Identification (DROID) which is a file profiling tool developed by The National Archives of the United Kingdom. *[Note: Where DROID is adopted to capture the file formats of electronic records, the ERKS should support (a) the capturing of multiple PRONOM values as the file format if single PRONOM cannot be identified by DROID; (b) the update of signature files of DROID; and (c) the scanning and*

(b) Capture		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		updating of the assigned PRONOM values of captured electronic records if new signature files of DROID will identify PRONOM values different from those values that are already assigned to the records.] C(91) Test whether the ERKS supports users to capture a non-electronic record, record its metadata and classify the record into an appropriate folder or a sub-folder (if implemented) as appropriate. C(92) Test whether the ERKS supports users to capture a record to multiple folders in an effective way. An effective way here means a method which should minimise manual efforts and errors and is user-friendly. For example, the ERKS allows copying of the metadata elements of the record to multiple folders to save manual efforts in capturing metadata.
	(b) support a user to designate a record for capturing by a designated individual.	C(93) Test whether the ERKS supports a user to designate a record for capturing by a designated individual. Test whether the designated individual is notified of such instruction for capturing a record.
12	***Where*** multiple repositories are implemented, the ERKS must provide a user with the option to capture a record	C(94) ***Where*** multiple repositories are implemented, test whether the ERKS provides options for users to capture a

(b) Capture			
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**	
	in a selected repository and populate the specific metadata profile that matches the selected repository.		record into a repository according to users' selection.
		C(95)	Regarding C(94), test whether the ERKS automatically populates the specific metadata profile of the selected repository during the records capturing process for users to provide metadata values that match the selected repository.
13	***Where*** an electronic document management system is implemented together with an ERKS, the ERKS must support a user to capture a document with multiple versions as record during the records capturing process.[23]	C(96)	***Where*** an electronic document management system is implemented together with the ERKS, test whether the ERKS supports users to capture a document with at least three versions as records according to the way(s) that the B/D concerned chooses. For example, if a B/D requires the ERKS to capture a document with multiple versions as a single record, the ERKS must support users to capture the document with multiple versions as a compound record.
14	***Where*** a workflow facility is implemented together with an ERKS, the ERKS must support a user to capture the	C(97)	***Where*** a workflow facility is implemented together with the ERKS, test whether the ERKS supports users to

[23] B/Ds may prescribe to capture a document with multiple versions as a record(s) in the following ways: (i) all versions stored, held as a single record in the form of a compound record; (ii) all versions stored, held as separate but linked records; (iii) selected version or versions specified by the user, the latter either as a single record in the form of a compound record or as separate but linked records; and/or (iv) the most recent version. The principle is to ensure that records accurately and adequately document government policies, decisions, procedures, functions, activities and transactions but the creation/collection of records should not be excessive in order to contain the growth of records which require resources for storage and management.

(b) Capture			
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**	
	workflow process (including records such as comments, views and approvals generated in the workflow process) as a record.		capture a workflow process (including records such as comments, views and approvals generated in the workflow process) as a record in an appropriate folder(s) or a sub-folder(s) (if implemented) according to the users' selection and/or pre-defined criteria. The capturing of a workflow process as record may be done in one go or conducted step-by-step having regard to different business operations. As a records management principle, records should be captured into a proper recordkeeping system as soon as possible once they were created for proper management and storage.
		C(98)	***Where*** a workflow facility is implemented together with the ERKS, test whether the ERKS supports automatic capture of a workflow process (including records such as comments, views and approvals generated in the workflow process) as a record in an appropriate folder(s) or a sub-folder(s) (if implemented) according to the users' selection and/or pre-defined criteria. The capturing of a workflow process as record may be done in one go or conducted step-by-step having regard to different business operations.
		C(99)	Regarding C(97) and C(98), test whether the content, context and structure of records generated in the

(b) Capture		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		workflow process are maintained and kept in the record of the workflow process captured.
15	***Where*** B/Ds choose to convert paper records and/or microfilm records into digitised records and capture them as records into the ERKS, the ERKS must enable integration with scanning solutions to provide the interface with the scanning equipment and allow an authorised individual to perform scanning. The ERKS scanning facility must support certain essential features, including but not limited to the following -	C(100) Test whether the ERKS integrates with the selected scanning solution determined by the B/D concerned and the scanning facility provides a capture option for capturing the digitised record (i.e. a scanned record) into the ERKS after the scanning process and quality inspection.
	(a) monochrome and colour scanning;	C(101) Test whether the ERKS scanning facility performs monochrome scans and colour scans of paper and/or microfilm records.
	(b) simplex and duplex scanning;	C(102) Test whether the ERKS scanning facility performs simplex and duplex scanning. The ERKS scanning facility should ensure that the sequence of pages of the digitised record is correct.
	(c) capturing of scanned images as records immediately following the scanning process and quality inspection;	C(103) Test whether the ERKS scanning facility supports capturing of scanned images as records immediately following the scanning process and quality inspection.

(b) Capture		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		The ERKS scanning facility should ensure that no alteration or changes can be made to the scanned images after the completion of the scanning process and quality inspection.
	(d) automatic capturing of metadata for the scanned image with an added facility allowing an authorised individual to select/input metadata that are unable to be automatically captured to complete the capturing process;	C(104) Test whether the ERKS scanning facility supports automatic capturing of metadata for a scanned image and allows an authorised individual to select/input metadata that are unable to be automatically captured to complete the capturing process. Some metadata such as "System identifier" should be system-generated by the ERKS.
	(e) providing Optical Character Recognition (OCR) functionality to produce text from a scanned image to support full text searching for records based on the text. The OCR must at least support Traditional Chinese, Simplified Chinese and English simultaneously;	C(105) Test whether the ERKS scanning facility is able to produce text from a scanned image by OCR functionality and capture the scanned image as a digitised record into the ERKS. Test whether a user can successfully perform a full text search based on the OCR text to locate and retrieve the record. C(106) Regarding C(105), test the OCR functionality by using scanned images containing text in - (a) Traditional Chinese only;

(b) Capture		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		(b) Simplified Chinese only; (c) English only; (d) Traditional Chinese and Simplified Chinese interweaved in the scanned image; (e) Traditional Chinese and English interweaved in the scanned image; (f) Simplified Chinese and English interweaved in the scanned image; and (g) Traditional Chinese, Simplified Chinese and English interweaved in the scanned image.
	(f) using lossless compression technique; and	C(107) Test whether the ERKS scanning facility saves images in a lossless compression format such as Tagged Image File Format (TIFF).
	(g) saving images at different resolutions, in colour or greyscale and in a lossless compression format.	C(108) Test whether the ERKS scanning facility saves images in colour at different resolutions (e.g. 300 dpi and 600 dpi) that meet legal, operational and business needs of the B/D concerned. C(109) Test whether the ERKS scanning facility saves images in greyscale at different resolutions that meet legal,

(b) Capture		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		operational and business needs of the B/D concerned.
	*[Note: The modes of creation, capturing and inheritance of a core set of record level metadata (including that for digitised records) as specified in RKMS are listed at **Appendix 4** to **FR of an ERKS**.]*	
16	The ERKS must prevent the alteration and deletion of the contents of any electronic records during and after records capturing (subject to the exceptions listed in **Requirement 23**).	C(110) Attempt to amend, remove from or add any contents to an electronic record such as an e-mail record during the process of capturing the record into the ERKS. If a user can do so, the ERKS fails to comply with **Requirement 16**. C(111) Attempt to amend, remove from or add any contents to electronic records of different file formats (e.g. e-mails, word-processed documents, spreadsheets, images, video clips and audio clips) once captured into the ERKS. If a user or an authorised individual can do so, the ERKS fails to comply with **Requirement 16**.
17	The ERKS must -	
	(a) populate the specific metadata profile according to the record form[24] of the record to be captured as	C(112) Test whether the ERKS automatically populates the specific metadata profile according to the record form of

[24] Two record forms, namely "electronic" and "non-electronic" were defined to facilitate interoperability of records among B/Ds. Please see **Appendix 4** to **FR of an ERKS**.

(b) Capture		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
	an ERKS record and automatically capture, generate and inherit metadata, including but not limited to those listed at **Appendix 4** to **FR of an ERKS**; and	the record to be captured and automatically captures, generates and inherits metadata for the record at the time of capturing the record, including but not limited to those listed at **Appendix 4** to **FR of an ERKS** according to the pre-defined modes of creation, capturing and inheritance as specified in **Appendix 4** to **FR of an ERKS**. For example, if a user captures an e-mail record created by himself/herself into the ERKS, the ERKS should automatically populate the metadata profile "electronic" form and automatically capture, generate and inherit metadata such as "Title", "Date sent", "Time sent", "Creator name", "System identifier", "Date time captured", "Record form", etc. Please see also C(286). C(113) Test whether the ERKS automatically populates the specific metadata profile "non-electronic" for a non-electronic record and automatically captures, generates and inherits metadata for the non-electronic record at the time of capturing the record, including but not limited to those listed at **Appendix 4** to **FR of an ERKS** according to the pre-defined modes of creation,

B/Ds may create sub-forms of records under each record form to meet their specific business needs but should bear in mind the compatibility issues of different sub-forms of records and the associated metadata when there is an operational need to transfer records with their associated metadata to other B/Ds or GRS.

(b) Capture		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		capturing and inheritance as specified in **Appendix 4** to **FR of an ERKS** such as "Date time captured", "System identifier" and "Record form". Please see also C(286).
	(b) automatically assign an identifier, unique within the entire ERKS, to each record at the point of capture.	Please see C(20).
18	The ERKS must prompt the user to capture[25] metadata which cannot be captured automatically, system-generated or inherited from its parent aggregation at the time of capturing a record. *[Note: The modes of creation, capturing and inheritance of a core set of record level metadata (for electronic records and non-electronic records) as specified in RKMS are listed at **Appendix 4** to **FR of an ERKS**.]*	C(114) Test whether the ERKS prompts (such as presenting the metadata elements) and provides effective means for users to capture metadata that cannot be captured automatically, system-generated or inherited at the point of capturing a record. For example, the ERKS provides the drag-and-drop method for users to capture those metadata from the record content. C(115) If a user attempts to enter metadata values that are not allowed, e.g. entering an invalid date format or an invalid date (e.g. 2002-12-32), the ERKS must deny storing the invalid values and should prompt the user to provide a valid value.
19	The ERKS must support capture of e-mail messages and	C(116) Test whether the ERKS ensures -

[25] The user may capture values of metadata elements by different means such as using "drag-and-drop" method to copy the values from the record and selecting proper metadata values from drop down menus.

(b) Capture		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
	attachments (sent and received) and enable the attachments to always be relatable to the e-mail message to which they were attached in the form of a compound record.	(a) the integrity of a compound record containing the e-mail message and attachment(s) so that the entire e-mail (as captured) can be accessed and acted upon as a single unit throughout its life cycle; (b) when the record content is viewed, it must be displayed in a logical manner, showing the message and attachment(s) as appropriate; and (c) when settings such as access control and records retention and disposal schedule are applied, they must take effect across all constituent records of the compound record (i.e. an e-mail message and all its attachment(s)). Please see also C(88) and C(89).
20	The ERKS must allow, when capturing a record that has more than one manifestation, a user to choose to capture the record **at least** in one of the following ways - (a) all manifestations as one record in the form of a compound record; (b) one specified manifestation as a record; and/or (c) each manifestation as an individual record.	C(117) Depending on the implementation approach of this functional requirement by the B/D concerned, test whether the ERKS supports users to choose to capture a record that has more than one manifestation such as a report in Microsoft Word format, PDF format and HTML format at least in one of the following ways - (a) all manifestations in the form of a compound record. If this implementation approach has been adopted,

(b) Capture		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		C(88) and C(89) are also relevant; (b) one specified manifestation as a record; and/or (c) each manifestation as an individual record. B/Ds may consider creating automatic cross-references among these manifestations and test the cross-references.
21	The ERKS must capture electronic records in their native file formats[26] and retain them in commonly-used file formats[27] as specified in the HKSARG Interoperability Framework [S18] (IF) and those specified by B/Ds.	C(118) Test whether the ERKS captures electronic records in the file format in which it was originally created. C(119) If a facility is implemented with the ERKS to render electronic records into another specified file format(s) to fix the record contents, test and examine whether the

[26] As a good electronic records management practice, B/Ds must capture a record in its native file format to ensure that its content, context and structure remain intact to maintain the authenticity, integrity, reliability and usability of the record. However, there are cases under which B/Ds may need to render a record into another specified file format at the point of capture with a view to, among other reasons, fixing the record contents of dynamic nature, which challenges the on-going management of the authenticity, integrity, reliability and usability of the record. For instance, B/Ds may need to render records of HTML pages that include external links to graphics and other objects, or spreadsheets that include external links to a database into file formats such as PDF to preserve the static appearance and content of the records as at the point of capture, though it is likely to result in losing the links. B/Ds may document the rendering of the record in the metadata of the rendered record. Prior to implementing an ERKS, a B/D may conduct an exercise to review the file formats of its departmental records and assess the needs for rendering records into specified file formats at the point of capture and the implications, including whether the integrity of the records will be compromised and the degree of compromise if it is unavoidable.

[27] To ensure that records stored in an ERKS can be viewed, used and transferred to other B/Ds as and when required, it is necessary to ensure that records stored therein are retained in commonly-used file formats as specified in the HKSARG Interoperability Framework [S18] (IF) and those specified by B/Ds. For records whose native file formats are not commonly-used file formats as specified in IF and those specified by B/Ds, B/Ds should consider using the functionality as set out in **Requirement 32** to render them into specified file formats.

(b) Capture		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		rendition is completed and the content, context and structure of the electronic record is maintained after the rendering to the degree as pre-defined by the B/D concerned. C(120) Test whether the ERKS imposes rendering of the electronic records whose native file formats are not commonly-used file formats as specified in IF or those specified by the B/D concerned. It is **not** acceptable to require a user to determine whether such rendering should be performed at the point of capture of an electronic record. C(121) Regarding C(120), test whether the ERKS provides means or tools to automatically identify file formats of electronic records. It is **not** acceptable to require a user to provide such information.
22	The ERKS must -	
	(a) support an authorised individual to import aggregations and electronic records with associated metadata into the ERKS in bulk and maintain the content, context and structure of the imported electronic records including the correct contextual	C(122) Test whether the ERKS supports import of aggregations and electronic records with associated metadata into the ERKS in a bulk operation with validation checks and appropriate measures in place to prevent data loss and minimise the risk of manual error. That means it is **not**

(b) Capture		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
	relationships between individual electronic records and their metadata; and	acceptable to manually declare individual records in separate actions. C(123) Regarding C(122), a successful import of records should result in all imported records being captured into the appropriate locations of a records classification scheme(s). The content, context and structure of records should be kept and the metadata should be correctly and persistently linked to the associated records. C(124) There may be a need to create and update metadata values for imported records. Some should be done by system automatically such as the "System identifier" and "Date time captured". While some may require manual update such as the "Responsible officer", B/Ds should test whether all required metadata are created and updated. C(125) Regarding C(124), test whether the ERKS supports entering the missing metadata manually to complete the import.
	(b) support import of metadata in bulk for non-electronic records and maintain the	C(126) Test whether the ERKS supports import of metadata in bulk for non-electronic records with validation checks

(b) Capture		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
	relationship with the aggregations they are allocated to.	and appropriate measures in place to prevent data loss and minimise the risk of manual error. That means it is **not** acceptable to capture the metadata of individual non-electronic records in separate actions. C(127) Regarding C(126), a successful import of metadata should result in all imported metadata being allocated to appropriate aggregations of the records classification scheme. C(128) There may be a need to create and update metadata values. Test whether the ERKS supports entering the missing metadata manually to complete the import.
23	The ERKS must prevent deletion of records except -	
	(a) destruction in accordance with an approved records retention and disposal schedule; and	C(129) If a **user** attempts to destroy a record in accordance with its approved retention and disposal schedule or delete the record, the ERKS must deny such action. Different ERKSs may adopt different measures to prevent deletion of records. C(130) If an **authorised individual** such as a records manager attempts to destroy an aggregation with records therein prior to the expiry of the approved records retention and disposal schedule in force, the ERKS must deny such

(b) Capture		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		action.
	(b) deletion by an authorised individual under a very exceptional situation.	C(131) Test whether the ERKS allows the deletion of a record by an authorised individual under very exceptional situation and documents such deletion in the audit trail. The ERKS should ensure that the deletion of a record is beyond reconstruction.
	Such deletion must be logged in the audit trails.	

(c) Use of Records		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
24	The ERKS must provide a flexible and powerful range of search functions to support a user to search, retrieve and access -	C(132) Test whether the ERKS provides an integrated interface for searching both metadata and record content. C(133) Test whether the search functionality of the ERKS supports users to search on record contents stored within the ERKS in a controlled manner according to their access rights and the security classification of records and return the appropriate records based on the search criteria and access controls. Please see also C(187). C(134) Test whether the ERKS ensures the search or retrieval function does not reveal any information of an entity (e.g. the name of a folder to which the user does not have access) to a user where the access controls prevent access by that user. C(135) Test whether the ERKS provides facilities for defining and storing search terms, for re-use by users. C(136) Regarding C(135), test whether the ERKS supports users to perform a search by using the stored search terms. C(137) Test whether the ERKS displays the search results after a search is performed and the number of items found. Aggregations, electronic records and non-electronic

(c) Use of Records		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		records meeting the search criteria should be included in the same search result. C(138) Test whether the ERKS displays search results in a clear, structured, user-friendly and organised manner. Where no search results are found, the ERKS should provide a suitable message to inform the user of this and indicate that the search process is complete. C(139) Test whether the ERKS supports users to specify a date range, e.g. calendar dates as search terms when performing a search. C(140) Test whether the ERKS enables users to refine a search without re-entering the search criteria. C(141) Test whether the search interface of the search function appears in a consistent manner independent of how a user searches for records or a specified level of aggregations within the ERKS. C(142) Test whether the user interface of the search function of the ERKS is intuitive to users. Users should be able to use simple methods such as selecting checkboxes to perform searching. It is **not** acceptable for users to input a command or a query to perform search function.

(c) Use of Records		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
	(a) individual records;	C(143) Test whether the ERKS supports search and retrieval of records with one component and multiple components and displays the records correctly. C(144) Test whether the ERKS supports search and retrieval of compound records, including the child record(s) and displays the compound records correctly. C(145) Test whether the ERKS supports the search for electronic and non-electronic records. Test whether users are able to retrieve any electronic records and the metadata of any non-electronic records in a set of search results and whether the ERKS supports display of the contents and metadata of the electronic records on retrieval.
	(b) aggregations; and/or	C(146) Test whether the ERKS supports users to perform a search for a class, sub-class, folder, sub-folder (if implemented) and part by using a combination of two or more metadata elements as search terms. Test whether users are able to retrieve any aggregations in a set of search results and whether the ERKS supports display of the contents of the aggregations on retrieval.
	(c) associated metadata	C(147) Test whether the ERKS supports users to search on any of the metadata elements used within the ERKS in a

(c) Use of Records			
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**	
			controlled manner. While the ERKS may provide a simple "free text" field, which will search on everything in a single action, it must also provide tools for users to specify the individual metadata field(s) to be used in the search.
	in an intuitive manner in the whole ERKS.		
25	***Where*** B/Ds implement a secondary storage[28] facility (e.g. near-line, off-line or off-site storage) for records in addition to the on-line storage of the ERKS, the ERKS must behave in an identical manner[29] (save that the mechanism and performance for presenting the aggregations and records may vary) when searching regardless of whether the aggregations and/or the records being searched for are stored on-line, near-line, off-line or off-site.	C(148)	***Where*** B/Ds implement a secondary storage facility (e.g. near-line, off-line or off-site storage) for records in addition to the on-line storage of the ERKS, test whether the ERKS supports users to search for, retrieve and access records and/or aggregations stored in secondary storage. The ERKS should behave in an identical manner such as the user interface for making a search for records stored on-line or in secondary storage should be the same. It is **not** acceptable to require users to specify the storage location such as secondary storage of records and/or aggregations to be searched for the purpose of conducting a search. The ERKS should always assume

[28] Due to system capacity, B/Ds may select to store records that are no longer in constant use but may be required infrequently in secondary storage.

[29] For example, it is not expected that a user has to first ascertain, before conducting a search, as to whether an aggregation or a record to be searched for, is stored near-line, off-line or off-site.

(c) Use of Records		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		that users are unaware of the storage locations of records and aggregations.
26	The ERKS must -	
	(a) support efficient searches, including but not limited to, full text, wild card and Boolean searches on one or a combination of any of the metadata elements and on the contents (where they exist) of records in an integrated and consistent manner;	C(149) Test whether the ERKS supports users to search for records by using - (a) a metadata element; (b) combination of metadata elements using Boolean operators (AND, OR, NOT); (c) records contents in text; (d) combined records contents using Boolean operators (AND, OR, NOT); and (e) wild card search and/or partial match search on metadata element and on records content. For example, the search results present records where the "Title" field contains the text "manage", whether it appears as a part of a word or as a whole word. Please see also C(132) to C(145).
	(b) support efficient searches of records containing multiple languages including at least Traditional	C(150) Test whether the ERKS supports users to search for

(c) Use of Records		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
	Chinese, Simplified Chinese and English; and	records containing - (a) Traditional Chinese in contents and/or metadata; (b) Simplified Chinese in contents and/or metadata; (c) English in contents and/or metadata; (d) Traditional Chinese and Simplified Chinese in contents and/or metadata; (e) Traditional Chinese and English in contents and/or metadata; (f) Simplified Chinese and English in contents and/or metadata; and (g) Traditional Chinese, Simplified Chinese and English in contents and/or metadata.
	(c) allow an authorised individual to configure and change the default search fields.[30]	C(151) Test whether the ERKS allows an authorised individual to configure a metadata element (which should be searchable) as a non-searchable field. C(152) Regarding C(151), attempt to search for a record by using the non-searchable metadata element as a search term.

[30] For example, an authorised individual may specify any element of aggregation and record metadata, and optionally full record contents, as search fields.

(c) Use of Records		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		C(153) Test whether the ERKS allows an authorised individual to configure a metadata element (which should be non-searchable) as a searchable field. C(154) Regarding C(153), test whether the ERKS supports users to search for a record by using the searchable metadata element as a search term.
27	The ERKS must allow a user to specify whether a search is to find records or a specific level and/or type of aggregation and to limit the scope of any search to any repository (if more than one repository is implemented) at the time of search.	C(155) Test whether the ERKS allows a user to specify a search to find a part, sub-folder (if implemented), folder, sub-class and class according to his/her access rights. Please see also C(187). C(156) Test whether the ERKS allows a user to limit a search to a record. C(157) Test whether the ERKS allows a user to limit a search to find all electronic folders, hybrid folders or physical folders under a specific sub-class according to his/her access rights. Please see also C(187). C(158) If more than one repository is implemented, test whether the ERKS allows a user to specify a search to find a record, part, sub-folder (if implemented), folder, sub-class and class in a designated repository according to his/her access rights. Please see also C(187).

(c) Use of Records		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
28	The ERKS must -	
	(a) launch the authoring applications (if the applications are available in the user's workstation)[31] from within the retrieval function of the ERKS for the purpose of viewing or presenting[32] ("playing" on-screen) a record;	C(159) If a universal viewer is implemented with the ERKS, ask the contractor to confirm the number and types of file formats that the viewer is able to support. C(160) Regarding C(159), test whether users are able to use the universal viewer to view at least the most common ten file formats that are used in the B/D concerned. For multimedia, audio and visual records, the ERKS universal viewer should be able to present/output the record as appropriate. The scope of the test should cover text and document, spreadsheet, image, e-mail, audio, visual, presentation (e.g. Microsoft PowerPoint) and multimedia file formats. C(161) If no universal viewer is available in the ERKS, test whether users are able to launch the authoring application such as Microsoft Word 2010 to view records from within the retrieval function of the ERKS. C(162) Regarding C(161), test at least the most common ten file

[31] For the sake of user-friendliness, B/Ds may consider including a universal viewer in their ERKSs to facilitate viewing of records as some users may not have the authoring applications.

[32] "Presenting" here is applicable to audio and video records. They have to be presented through an appropriate output device.

(c) Use of Records		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		formats that are used in the B/D concerned. The scope of the test should cover text and document, spreadsheet, image, e-mail, audio, visual, presentation (e.g. Microsoft PowerPoint) and multimedia file formats.
	(b) allow a user to select and retrieve one or more components from a record and one or more records from a compound record; and	C(163) Test whether the ERKS allows a user to select and retrieve one or more records from a compound record. For example, test whether the ERKS supports a user to retrieve one or more attachments from an e-mail record. C(164) Test whether the ERKS allows a user to select and retrieve one or more components from a record. For example, test whether the ERKS supports a user to retrieve one or more components such as JPEG images from a web page record.
	(c) ensure that the associated metadata of the record can be retrieved and displayed in an efficient manner.	C(165) Test whether the ERKS allows retrieval and display of the metadata of a record easily, say by one or two single clicks or keystrokes. C(166) Test whether the ERKS displays to the user the metadata “security classification” and “security classification type” of the classified information they are accessing or going to access in an efficient manner.

(c) Use of Records		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
29	***Where*** an electronic document management system is implemented together with an ERKS, the ERKS must support a user to retrieve easily any version or multiple versions as specified by the user when multiple versions or all versions of the electronic record are stored. *[Note: Please see also **Requirement 13**.]*	C(167) ***Where*** an electronic document management system is implemented together with the ERKS, test whether the ERKS supports a user to search for and retrieve - (a) multiple versions of an electronic record as specified by the user and the version number of each is clearly visible; (b) all versions of an electronic record and the version number of each is clearly visible; and (c) any version of the electronic record as specified by the user and the version number is clearly visible when multiple versions or all versions of the electronic record are stored.
30	The ERKS must provide a user with flexible options for printing records (where text contents exist) and/or associated metadata and results list from all searches.	C(168) Test whether the ERKS supports users to print record contents and/or metadata. It is **not** acceptable for users to use "screen-dumping" or "snapshots". Preferably, the ERKS should support users to select printing of record contents and/or metadata of multiple records in one go. C(169) Test whether the ERKS supports users to print the search results list. Where the search results are presented

(c) Use of Records		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		over multiple pages, the ERKS should provide appropriate options for printing the entire result set as required.
31	The ERKS must allow a user to -	
	(a) download electronic records; and	C(170) Test whether the ERKS supports users to download electronic records subject to any prevailing security restrictions set by an authorised individual. The ERKS should support users to select downloading of multiple records in one go.
	(b) transmit links of ERKS-stored electronic records and metadata[33] to other users	C(171) Test whether the ERKS supports users to transmit links of ERKS-stored electronic records and links of metadata of non-electronic records to other users. Subject to the access rights of the user receiving the links, the ERKS should ensure that he/she is able to retrieve and access the electronic records and/or metadata by clicking the links. Please see also C(187).

[33] For a non-electronic record, a user may transmit a link of its associated metadata to other users.

(c) Use of Records		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
	subject to any prevailing security restrictions set by an authorised individual.[34]	
32	The ERKS must support rendering of electronic records[35] into the following specified file formats[36] for retrieval over time in addition to their native file formats and retrieval of the renditions -	
	(a) text and spreadsheet records in Portable Document Format/Archive (PDF/A)[37]; and	C(172) Test whether the ERKS supports rendering text and spreadsheet records in Portable Document Format/Archive (PDF/A) in addition to their native file formats. B/Ds should ensure that test cases cover the frequently-used text and spreadsheet file formats used by their organisations. The ERKS should ensure that the content, context and structure of the rendered records are kept as far as practicable. C(173) Regarding C(172), test whether the ERKS supports

[34] B/Ds may impose restrictions to constrain users from downloading records stored in a specific aggregation, e.g. a folder containing sensitive personal data.

[35] For audio and video records, B/Ds may use the Broadcast Wave Format (BWF) and Material eXchange Format (MXF) respectively.

[36] The currently specified file formats are subject to changes from time to time having regard to the international records management standards and best practices and technological changes. They will be further reviewed in the context of studying strategies and solutions for long-term preservation of electronic records.

[37] PDF/A provides a mechanism for representing electronic records in a manner that preserves their visual appearance over time, independent of the tools and systems used for creating, storing or rendering the files. There may be a loss of data, e.g. the formula of a spreadsheet will be lost after the spreadsheet is rendered into PDF/A format.

(c) Use of Records		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		retrieval of the rendered records.
	(b) images in TIFF.	C(174) Test whether the ERKS supports rendering images in TIFF in addition to their native file formats. B/Ds should ensure that test cases cover the frequently-used image file formats used by their organisations. The ERKS should ensure that the content, context and structure of the rendered images are kept as far as practicable. C(175) Regarding C(174), test whether the ERKS supports retrieval of the rendered images.
33	The ERKS must -	
	(a) support a user to reserve, charge-out and charge-in physical and hybrid aggregations and non-electronic records (including those aggregations and records in off-site storage) managed by the ERKS (e.g. through automatic notification to registry staff) and provide appropriate information to the user such as the status of reservation of the physical and hybrid aggregations and non-electronic records; and	C(176) Test whether the ERKS supports a user to reserve for use one or more physical and/or hybrid aggregation(s) and non-electronic record(s) and allows the user to specify a future date for receiving the aggregation(s) and record(s). The ERKS should provide appropriate information to the user such as the status of reservation of the physical and/or hybrid aggregation(s) and non-electronic record(s). C(177) Test whether the ERKS supports a user to charge-out one or more physical and/or hybrid aggregation(s) and

(c) Use of Records		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		non-electronic record(s). C(178) Regarding C(177), test whether the ERKS supports a user to charge-in one or more physical and/or hybrid aggregation(s) and non-electronic record(s) for returning the borrowed aggregation(s) and record(s). C(179) Regarding C(176) to C(178), the ERKS should track actions including recording the movement of physical and hybrid aggregations and non-electronic records from one location to another location(s), date of charge-out and charge-in and the user(s) responsible for the charge-out and charge-in actions. Please see also C(48).
	(b) support a user to retrieve and access electronic and hybrid aggregations and electronic records that are stored off-line and managed by the ERKS (e.g. through automatic notification to registry staff) and provide appropriate information to the user such as time by which the user can expect to retrieve and access the electronic and hybrid aggregations and electronic records.[38]	C(180) Test whether the ERKS supports a user to retrieve and access one or more electronic and/or hybrid aggregation(s) and electronic record(s) that are stored off-line ***where*** B/Ds implement an off-line storage facility. The ERKS should provide appropriate information to the user such as time by which the user can expect to retrieve and access the electronic and/or hybrid aggregation(s) and electronic record(s).

[38] Upon receipt of a user's request for retrieving and accessing electronic aggregations and records that are stored off-line, an authorised individual may use different

(d) Security and Access Control		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
34	The ERKS must provide a self-contained security system designed to protect the integrity of aggregations and records within the ERKS environment and enable the system to work effectively together with the security products specified by B/Ds.	C(181) Test whether the ERKS has its own security system including user authentication and security measures/rules to protect the integrity of aggregations and records within the ERKS environment having regard to the confidentiality and sensitivity of the aggregations and records. *[Note: B/Ds should test the effects and outcomes of the security measures and rules in accordance with C(183) to C(224). Where B/Ds implement an ERKS with other Lightweight Directory Access Protocol (LDAP) software specified by the B/D concerned to access and maintain directory information services, the ERKS should work effectively and seamlessly with the LDAP software.]* C(182) Test whether the ERKS works effectively with security products such as an information rights management product specified by the B/D concerned.
35	The ERKS must provide proper management of user ID and password information, and deny a user's access to	C(183) Test whether the ERKS properly manages user ID and password information to ensure that only users

means to provide access to the requested electronic aggregations and records such as by uploading them into the ERKS or forwarding them to the user direct having regard to a number of considerations such as the quantity and size of requested aggregations and records. Therefore, there may not be a need for a user to charge-out and charge-in the electronic aggregations and records.

(d) Security and Access Control		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
	aggregations and records that have a higher security classification than the user's security clearance.	authorised to use the ERKS are allowed to access to system functions, aggregations and records according to their access rights and security clearance. *[Note: Where B/Ds implement two-factor authentication with the ERKS for access to CONFIDENTIAL information, it should work effectively and seamlessly with the ERKS.]* C(184) Test whether the ERKS denies any attempt to access to system functions, aggregations or records by any unauthorised person. C(185) Test whether the ERKS allows an authorised individual to configure log-on to govern the access to the system. C(186) Test whether the ERKS allows users to get access to the system after a successful identification and authentication. C(187) Test whether the ERKS denies a user to get access to aggregations and records that have a higher security classification than the user's security clearance. The test should include browsing, navigating, searching, selecting and retrieving aggregations and records in the records classification schemes, as well as accessing records by using the links transmitted by the ERKS.

(d) Security and Access Control		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		C(188) Test whether the ERKS denies access by a user to aggregations and records or their metadata by means of any search, retrieval, printing or downloading functions, where the access controls and security allocated to those aggregations or records prevent access by that user. For example, the ERKS does not include in the search list aggregations, records or their metadata for which the user does not have the access rights or sufficient security clearance to access.
36	The ERKS must support an authorised individual to -	
	(a) create, add, manage and delete users, user groups and user roles[39];	C(189) Test whether the ERKS supports an authorised individual to create user profiles and user accounts to enable users to use system functions and get access to aggregations and records according to their access rights and security clearance. C(190) Test whether the ERKS provides effective tools/measures which should minimise manual efforts and errors and are user-friendly, e.g. a query function, for an authorised individual to manage users, user groups and user roles.

[39] User roles, for example, include Departmental Records Manager, Records Manager, Records Officer, Records User and System Administrator.

(d) Security and Access Control		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		C(191) Test whether the ERKS supports an authorised individual to create user roles with specific access rights to system functions as specified by the B/D concerned. The ERKS should **not** limit the number of user roles. C(192) Test whether the ERKS supports an authorised individual to create user groups. The ERKS should **not** limit the number of user groups. C(193) Test whether the ERKS supports an authorised individual to delete a user, a user group or a user role from the ERKS. Such deletions should **not** erase traces of actions performed by the user, the user group or the user role.
	(b) allocate users to and remove them from user groups and user roles[40];	C(194) Test whether the ERKS supports an authorised individual to add users into a user group or a user role without a limit on the number of users within that group or role. C(195) Test whether the ERKS supports an authorised individual to add users with different user roles in a user group. C(196) Test whether the ERKS supports an authorised individual to add user groups into another user group, e.g. adding Group A with five users and Group B with ten users into

[40] A user must be allowed to be a member of more than one user group and/or one user role.

(d) Security and Access Control		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		Group C (which has existing 50 users); C(197) Test whether the ERKS supports an authorised individual to assign a user to more than one user group or user role. C(198) Test whether the ERKS allows an authorised individual to remove one or more users from a user group or a user role. Such removal should **not** erase traces of actions performed by the user(s).
	(c) assign access to system functions to a user according to the user groups or user roles;	C(199) Test whether the ERKS supports an authorised individual to assign users (including authorised individuals such as records managers) to access to different system functions according to the user group or user role that they belong to. C(200) Regarding C(199), test whether the ERKS allows a user to use system functions such as searching for and retrieving a record according to his/her access rights.
	(d) modify the access rights and attributes [41] of individual users, user groups and user roles;	C(201) Test whether the ERKS supports an authorised individual to change the access rights of individual users and user groups. For example, change the access rights of a

[41] For example, they include login name and user password.

(d) Security and Access Control		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		user/user group from one part to another part of a records classification scheme. C(202) Test whether the ERKS supports an authorised individual to change the access rights of a user role. C(203) Test whether the ERKS supports an authorised individual to modify attributes such as resetting the password of an individual user and changing the name of a user group and a user role.
	(e) create, assign and modify[42] security classifications of aggregations and records[43];	C(204) Test whether the ERKS supports an authorised individual to create security classifications according to requirements of Security Regulations. C(205) Test whether the ERKS supports an authorised individual to create a new security classification to address specific security needs of the B/D concerned. C(206) Test whether the ERKS supports an authorised individual to assign appropriate security classification to aggregations. For example, the ERKS applies a given

[42] The ERKS must support the modification of security classification of all records within a part in one single operation and provide suitable warning and await confirmation before completing the operation.

[43] A user must be allowed to assign the security classification of a record during the records capturing process.

(d) Security and Access Control		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		default value that is selected by an authorised individual. C(207) Test whether the ERKS supports a user to assign the security classification of a record during the records capturing process. C(208) Test whether the ERKS supports an authorised individual to change the security classification of all records within a part in a single operation. The ERKS should provide suitable warning to the authorised individual and await confirmation as appropriate before completing the operation. C(209) Test whether the ERKS denies a record with a higher security classification to be filed into a part with a lower security classification. C(210) Test whether the ERKS supports an authorised individual to change the security classification of an aggregation. Then test whether the ERKS only allows the aggregation to be accessed by user with a security clearance being equal to or higher than the new security classification of the aggregation. For example, after a folder is downgraded from CONFIDENTIAL to RESTRICTED, a user with RESTRICTED security clearance should become able to access the folder, assuming that the user has access

(d) Security and Access Control		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		rights to the folder. C(211) Test whether the ERKS supports an authorised individual to change the security classification of a record. Then test whether the ERKS only allows the record to be accessed by user with a security clearance being equal to or higher than the new security classification of the record. C(212) Regarding C(210) and C(211), the test should include browsing, navigating, searching, selecting and retrieving aggregations and records in the records classification schemes, as well as accessing records by using the links transmitted by the ERKS. Please see also C(11), C(133) C(155), C(157), C(158) and C(171). C(213) Regarding C(210) and C(211), test whether the ERKS denies a change which will result in a part with a lower security classification containing a record(s) with a higher security classification. C(214) Regarding C(210) and C(211), test whether the ERKS supports entering a reason why the security classification of an aggregation or a record is changed.

(d) Security and Access Control		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
	(f) create, assign and modify the security clearance of users;	C(215) Test whether the ERKS supports an authorised individual to create values of security clearance as specified in **Annex 3** and **Annex 5** of **RKMS**. C(216) Test whether the ERKS supports an authorised individual to create a new security clearance to address specific security needs of the B/D concerned. C(217) Test whether the ERKS supports an authorised individual to assign appropriate security clearance to a user at system configuration time or later. C(218) Test whether the ERKS supports an authorised individual to change the security clearance of a user. Then test whether the ERKS only allows the user to access to aggregations and records with his/her new security clearance being equal to or higher than the security classification of the aggregations and records. C(219) Regarding C(218), the test should include browsing, navigating, searching, selecting and retrieving aggregations and records in the records classification schemes, as well as accessing records by using the links transmitted by the ERKS. Please see also C(11), C(133), C(155), C(157), C(158) and C(171).

(d) Security and Access Control		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
	(g) deny access by users to system functions, aggregations or records after a specified date[44]; and	C(220) Test whether the ERKS supports an authorised individual to deny a user accessing to system functions, aggregations or records after a specified date.
	(h) review the security classifications of aggregations and records, the access rights of users, user groups and user roles, and the security clearance of users on a routine or an ad hoc basis.[45]	C(221) Test whether the ERKS provides efficient and effective means to support an authorised individual to review the security classifications of aggregations and records on a routine or an ad hoc basis. C(222) Test whether the ERKS provides efficient and effective means to support an authorised individual to review the access rights of users, user groups and user roles and the security clearance of users on a routine or an ad hoc basis.
	The ERKS must support the authorised individual to perform the above functions in an efficient and easy manner.[46]	

[44] Where B/Ds have a large number of users, they may consider implementing the functionality "to allow access by users to system functions, aggregations or records after a specified date" to enhance efficiency in managing user accounts.

[45] Users may be involved in the review, e.g. to give advice on whether the existing security classification of a record should be downgraded having regard to the sensitivity of the record after a period of time. The ERKS must support an authorised individual to seek comments from users for completion of the review.

[46] For example, the ERKS must support an authorised individual to move a user from a user group to another user group without having to delete the user from the ERKS and re-enter the user's details.

(d) Security and Access Control		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
37	The ERKS must control access (including access to different system functions) at the level of the user, user group or user role as well as at the record and aggregation levels.	C(223) Test whether the ERKS controls access (including access to different system functions) at the level of the user, user group or user role. C(224) Test whether the ERKS controls access (including access to different system functions) at record and aggregation levels. For example, test whether the ERKS controls access to a class or sub-class and their associated metadata by a user, user group or user role.
38	The ERKS must automatically capture and keep unalterable[47] audit trails about - (a) type of actions, including but not limited to those listed at **Appendix 5** to **FR of an ERKS**; (b) the records classification scheme, aggregations and records or other entities (e.g. a records retention and disposal schedule) on which the action is taken; (c) administrative parameters and system activities, e.g. reconfiguration of audit trails; (d) the user who initiated and/or carried out the action;	C(225) Test whether the ERKS automatically captures and keeps audit trails for those actions specified in **Appendix 5** to **FR of an ERKS**. Information should be captured include - (a) the type of action (which should be human understandable and the description should be consistent); (b) the entity on which the action is taken (documenting the unique identifier and other information of the entity including the metadata value before and after the completion of the action if there is a change to

[47] The term "unalterable" in FR of an ERKS means that it must be impossible for any user, authorised individual or system administrator to change or delete any part of the audit trails. The audit trail data may, however, be exported for off-line storage if required, so long as its integrity remains intact.

(d) Security and Access Control		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
	and (e) date and time of the action for as long as required.	metadata). Under some circumstances, system activities, e.g. changing system configuration may not involve an entity; (c) the user who initiated and/or carried out the action (documenting the user identifier and other information of the user); and (d) date and time of the action (which should accurately reflect the date and time of the action). C(226) Attempt to amend or alter the audit trail by an authorised individual with "unlimited" access rights to the ERKS. The ERKS must deny changing the audit trail data. C(227) Attempt to amend or alter the audit trail by a user. The ERKS must deny changing the audit trail data. C(228) Test whether the audit trail data relating to an aggregation or a record is linked to the system identifier of that aggregation or record.
39	The ERKS must support an authorised individual to manage audit trails, including but not limited to the following -	

(d) Security and Access Control		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
	(a) searching and retrieving audit trail data;	C(229) Test whether the ERKS supports an authorised individual to - (a) search and retrieve all audit trail data about a record, an aggregation or other entities within a specified date/time range; (b) search and retrieve all audit trail data within a specified date/time range; (c) search and retrieve all audit trail data for a specified action/event such as export of records within a specified date/time range; (d) search and retrieve all audit trail data for a specified repository within a specified date/time range if multiple repositories have been implemented; and (e) search and retrieve all audit trail data for actions performed by a user within a specified date/time range.
	(b) generating ad hoc or pre-defined reports on specified audit trail data;	C(230) Test whether the ERKS provides options to generate an ad hoc report on all or selected parts of the audit trail. For example, generating a report on the actions of a user within a specified date/time range.

(d) Security and Access Control		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		C(231) Test whether the ERKS provides options to generate a pre-defined report on all or selected parts of the audit trail.
	(c) reconfiguring[48] audit trails; and	C(232) Test whether the ERKS supports an authorised individual to reconfigure parameters including which actions have to be recorded automatically in the audit trail. The ERKS should record such reconfiguration of audit trails in the audit trail.
	(d) exporting, transferring and purging audit trail data under a strict and controllable manner.	C(233) Test whether the ERKS supports an authorised individual to export in secure processes all or selected parts (e.g. all audit trail data about an aggregation) of audit trail data. The ERKS should ensure that such an export does not affect the audit trail data stored in the ERKS. C(234) Test whether the ERKS supports an authorised individual to transfer in secure processes all or selected parts of audit trail data out of the ERKS. C(235) Test whether the ERKS supports purging of selected audit trail data under a strict and controlled manner. It is expected that such a purge action should **not** be

[48] Reconfiguration here includes making changes to the settings of audit trails so that the functions for which information is automatically stored can be selected. The system must ensure that such changes are stored in the audit trails.

(d) Security and Access Control		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		automatically performed and should require manual confirmation. Such a purge action should be recorded in the audit trail. *[Note: It is preferable that the manual confirmation should be conducted at least twice.]*

(e) Retention and Disposal		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
40	The ERKS must support an authorised individual to create, maintain, modify, delete[49] and manage records retention and disposal schedules indicating the period of time records (regardless of their physical form) are to be retained[50] in an active and inactive state.	C(236) Test whether the ERKS supports an authorised individual to create, maintain, modify, delete and manage a set of records retention and disposal schedules that are applicable to aggregations of different levels and types in order to specify the following - (a) an event trigger (please see **Annex 3** of **RKMS**), e.g. closing a part; (b) an external event trigger (please see **Chapter 3** of **RKMS**); (c) the retention period to be completed (from one day to 99 years); (d) a specified future disposal date; and (e) the disposal action(s) to be performed. Disposal action at (e) must be implemented with (a) and (c), (b) and (c), or (d). C(237) Test whether the ERKS automatically assigns a unique system identifier to a records retention and disposal

[49] Changes to, or deletions of, records retention and disposal schedules must be controlled carefully to minimise the risk of records being destroyed inappropriately.
[50] The retention period must be defined from one day to 99 years in accordance with RKMS.

(e) Retention and Disposal		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		schedule. C(238) Test whether the ERKS supports an authorised individual to assign a textual title to a records retention and disposal schedule. C(239) Test whether the ERKS triggers the commencement of the prescribed retention period if an "Event trigger - internal" such as "Part closed" as defined in **Annex 5** of **RKMS** has been applied to trigger the commencement of retention period of an aggregation. C(240) Test whether the ERKS triggers the commencement of the prescribed retention period when an authorised individual notifies the ERKS that a specified event (i.e. external event trigger as defined in **Chapter 3** of **RKMS**) has occurred and the effective date on which the event occurred. C(241) Test whether the ERKS supports an authorised individual to define a set of properties such as title, description, unique system identifier, and retention period for each records retention and disposal schedule. Please refer to **Annex 2** and **Annex 3** of **RKMS**. C(242) Test whether the ERKS allows an authorised individual to

(e) Retention and Disposal		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		modify a records retention and disposal schedule regardless of whether this schedule has been assigned to aggregations. Please see also C(253). C(243) Test whether the ERKS denies a user creating, maintaining, modifying, deleting and managing records retention and disposal schedules.
41	The ERKS must support an authorised individual to create, maintain, modify, delete and manage a listing with instructions for the authorised disposal of records (regardless of their physical form) including but not limited to destruction, transfer to another B/D (such as the Government Records Service), transfer outside the Government or review by the B/D or the Government Records Service.	C(244) Test whether the ERKS supports an authorised individual to create, maintain, modify, delete and manage a listing of authorised disposal actions (i.e. disposal instructions). The authorised disposal actions are set out in the Disposal action encoding scheme, **Annex 5** of **RKMS**. Please see also C(236) and C(241). C(245) Test whether the ERKS supports an authorised individual to add a disposal action to the listing. C(246) Test whether the ERKS supports an authorised individual to revise a disposal action in the listing. C(247) Test whether the ERKS supports an authorised individual to delete a disposal action from the listing. The deletion should **not** erase traces of actions performed by an authorised individual.

(e) Retention and Disposal		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
42	The ERKS must -	
	(a) link the retention periods and disposal actions for records, through the records classification scheme, to any aggregation (i.e. inheritance principle); and	C(248) Test whether the ERKS provides an effective mechanism (which should minimise manual efforts and errors) to allocate a pre-defined records retention and disposal schedule to a class or sub-class; and allows but not requires, that retention and disposal schedule to be inherited by all child aggregations of this class or sub-class. The ERKS should ensure that any new aggregation created under this class or sub-class inherits the retention and disposal schedule by default. C(249) Regarding C(248), if the applied records retention and disposal schedule at the class or sub-class level is changed, test whether any child aggregations that inherited the original records retention and disposal schedule automatically inherits the new schedule. Test whether any new child aggregation on creation inherits the new schedule by default. Test whether any child aggregation that has had its specific records retention and disposal schedule allocated retains its own schedule and it will continue to take precedence over any inherited settings. The ERKS should support such action to be taken place as and when required until the

(e) Retention and Disposal		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		aggregations and records therein are finally disposed of. Please see also C(253) and C(254). C(250) Regarding C(248) and C(249), test whether the ERKS displays clearly the **allocated** and **inherited** records retention and disposal schedules differently in order to distinguish the way in which the schedules have been applied. C(251) Test whether the ERKS restricts the ability to change default records retention and disposal schedules for aggregations and records therein, to an authorised individual.
	(b) support the application of the same records retention and disposal schedules to both electronic and non-electronic records managed by a hybrid folder.	C(252) Test whether the ERKS supports to apply one single records retention and disposal schedule to a hybrid folder and such records retention and disposal schedule should take effect on both electronic and non-electronic records managed by the hybrid folder.
43	The ERKS must allow an authorised individual to change the default records retention and disposal schedules for aggregations and records therein, at any level of the records classification scheme and at any time, in order to support retention and disposal exceptions.	C(253) Test whether the ERKS supports an authorised individual to change the default records retention and disposal schedule of an aggregation upon the commencement of the retention period of the applied schedule. For any child aggregations that inherited the original records

(e) Retention and Disposal		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		retention and disposal schedule, the ERKS should ensure that the change is assigned immediately to the child aggregations. Please see also C(249). *[Note: B/Ds should note that it is **not** recommended to modify the retention period and/or the disposal action of a records retention and disposal schedule so as to enable a change to the retention period and/or disposal action of an aggregation. This is because a modification of the records retention and disposal schedule will trigger a universal change to the retention period and/or disposal action of all aggregations that this schedule has been applied. Such an accidental change with wide implications should be avoided.]* C(254) Test whether the ERKS supports an authorised individual to change the records retention and disposal schedule applied on an aggregation prior to executing the final disposal action of the aggregation. The ERKS should ensure that the change assigned immediately to the child aggregations that inherited the original records retention and disposal schedule. Please see also C(249).
44	The ERKS must support an authorised individual to set and lift disposal hold on aggregations and records	C(255) Test whether the ERKS supports an authorised individual to place a disposal hold on an aggregation, e.g. a folder,

(e) Retention and Disposal		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
	therein.	and records therein to the effect that any disposal actions, e.g. destruction, for the aggregation and records therein, as well as any parent aggregations of that aggregation, are effectively paused and cannot be executed until the hold is removed. C(256) Regarding C(255), test whether the ERKS supports an authorised individual to assign a textual title to and enter a reason for a disposal hold. C(257) Regarding C(255), test whether the ERKS prevents any aggregation and records therein which have a disposal hold placed on them from being deleted by an authorised individual, outside of the disposal process. The ERKS must also prevent any parent aggregation of such aggregation from being deleted by an authorised individual. The ERKS must not allow such deletions. C(258) Regarding C(255), test whether such disposal hold placed on an aggregation and records therein is not affected by a re-classification of that aggregation. For example, if a folder with a disposal hold in place is re-classified from one sub-class to another sub-class in the records classification scheme, the disposal hold should continue to be in place with the folder after the re-classification,

(e) Retention and Disposal		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		while the disposal hold with the folder should no longer have any effect on the originating parent sub-class. C(259) Test whether the ERKS supports an authorised individual to lift a disposal hold on an aggregation, e.g. a folder and records therein to the effect that the affected aggregation and records therein can be identified and disposed of in the usual manner by the ERKS disposal mechanism. For aggregation of which the disposal hold is lifted, the ERKS should ensure that the parent aggregation(s) of that aggregation can be identified and disposed of in the usual manner by the ERKS disposal mechanism (on the assumption that there is no other disposal hold applied to the parent aggregation(s) and the child aggregations/records therein). C(260) Test whether the ERKS clearly indicates those aggregations that a disposal hold is in place and supports an authorised individual to identify, retrieve and generate reports on the aggregations where a disposal hold has been applied. C(261) Test whether the ERKS restricts the ability to place and lift a disposal hold to an authorised individual.

(e) Retention and Disposal		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
45	The ERKS must support an authorised individual to identify folders and parts due for disposal according to their authorised records retention and disposal schedules.	C(262) Test whether the ERKS provides efficient and effective means (which should minimise manual efforts and errors) to enable an authorised individual to identify folders, sub-folders (if implemented) and parts due for disposal according to their applied records retention and disposal schedules at one single operation. The ERKS should **not** require an authorised individual to find out whether a folder is due for disposal one by one. C(263) Test whether the ERKS recognises that a conflict arises in case two records retention and disposal schedules are in force for an aggregation and informs an authorised individual to take proper action to resolve the conflict. C(264) Test whether the ERKS alerts an authorised individual the existence of non-electronic records within a folder, sub-folder (if implemented) or a part when the folder, sub-folder or part is going to be exported, transferred or destroyed. For example, the ERKS provides a listing of those folders containing non-electronic records.
46	The ERKS must allow an authorised individual to	C(265) Test whether the ERKS supports an authorised individual

(e) Retention and Disposal		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
	authorise an automatic execution of destruction of electronic records[51] according to the approved records retention and disposal schedule, from all repository media[52] such that the records cannot be reconstructed. *[Note: For non-electronic records, of which the contents are stored outside the ERKS, it is necessary for an authorised individual to arrange destruction of the non-electronic records.]*	to authorise the automatic destruction action to an aggregation(s) with electronic records (including records with multiple components and compound records) stored therein in a single process according to the approved records retention and disposal schedule(s). The ERKS should ensure that - (a) all components of an electronic record(s); and (b) all constituent records of a compound record(s) stored in the aggregation(s) are destroyed together. C(266) Test whether the ERKS supports an authorised individual to authorise an automatic execution of destruction of electronic records from all repository media according to the approved records retention and disposal schedule. C(267) Test whether the ERKS performs the action in an informed and structured manner; manual confirmation must always be provided before the ERKS executes a disposal action on an aggregation and records therein. C(268) Attempt to restore the destroyed aggregations and records. The ERKS should ensure that the destruction

[51] The ERKS must ensure that all components of a record and all records of a compound record are disposed of in an integrated manner.

[52] Media include physical media such as DVDs.

(e) Retention and Disposal		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		of aggregations and records is beyond reconstruction. C(269) Test whether the ERKS supports automatic creation of a stub replacing the aggregation that has been destroyed or transferred out of the ERKS. The ERKS should be able to clearly differentiate between existing and destroyed aggregations within the records classification scheme. *[Note: For C(265) to C(269) above, B/Ds should note only those records that have been approved by the GRS Director for destruction can be destroyed. B/Ds should make reference to GC No. 2/2009 about records retention and disposal.]*
47	The ERKS must -	
	(a) support an authorised individual to export and transfer aggregations and records in specified format(s) with associated metadata and audit trails. Specifically, the system must ensure that -	C(270) Test whether the ERKS supports an authorised individual to select aggregations and records with associated metadata and audit trails for export or transfer. C(271) Test whether the ERKS supports an authorised individual to export and transfer selected aggregations and records in specified format(s) with associated metadata in a single operation without losing the integrity of the data. It is **not** acceptable for the ERKS to repeat the entire export action for each individual aggregation or record.

(e) Retention and Disposal		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		The data should be exported or transferred in a structured manner so that it can be easily verified and the relationships among aggregations and among aggregations and records can be re-created if the data is imported at a later stage. C(272) Test whether the ERKS supports an authorised individual to export a copy of audit trail data associated with the selected aggregations and records for export. C(273) Test whether the ERKS produces a report detailing any failure to export or transfer aggregations and records. The ERKS should identify any aggregations or records which have generated processing errors during export or transfer, any aggregations or records that have not been successfully exported.
	(i) the content and structure of the electronic records are not degraded;	C(274) Regarding C(271), check whether the contents and structure of electronic records after export or transfer have not been degraded.
	(ii) all components of an electronic record (when the record consists of more than one component) and all records of a compound record are exported as an integral unit;	C(275) Regarding C(271), check whether electronic records with multiple components and compound records are exported or transferred as an integral unit.

(e) Retention and Disposal		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
	(iii) all links between the record and its metadata and audit trails are retained; and	C(276) Regarding C(271) and C(272), check whether all links between the record and its metadata and audit trails are retained. Indicators showing the links between records, metadata and audit trails include using the unique system identifier of a record to search for audit trail of that record.
	(iv) all links [53] between electronic records and aggregations are maintained; and	C(277) Regarding C(271), check whether all links between electronic records and aggregations are maintained.
	(b) support an authorised individual to export and transfer metadata and audit trails of non-electronic records in specified format and ensure that all links between the metadata of non-electronic records and the aggregations are maintained.[54]	C(278) Test whether the ERKS supports an authorised individual to export and transfer metadata and audit trails of non-electronic records in specified format. C(279) Regarding C(278), test whether the links between the metadata of non-electronic records and the aggregations are maintained.

[53] There may be cases in which the links between an electronic record and its related aggregation(s) may not be retained. For example, the cross-references of an electronic record to its related folder(s) will be delinked if the related folder(s) are not exported or transferred in connection with the electronic record to be exported or transferred. B/Ds should consider the implications of such loss of contextual information to the authenticity, integrity, reliability and usability of the electronic record and take appropriate remedial actions, e.g. provision of the contextual information in a printed format.

[54] Similar to an electronic record, there may be cases in which the links between a non-electronic record and its related aggregation(s) may not be retained. Please see the example quoted in footnote 53.

(e) Retention and Disposal		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
48	The ERKS must support an authorised individual to review the records retention and disposal schedules of aggregations on a regular or an ad hoc basis and revise/change the records retention and disposal schedules applied to the aggregations and records therein after the review, if necessary.	C(280) Test whether the ERKS supports an authorised individual to access the records classification scheme on a regular or an ad hoc basis and decide on the future records retention and disposal schedule of an aggregation and make necessary revisions to the schedule of the aggregation. C(281) Test whether the ERKS supports an authorised individual to make review comments or enter a reason for the review decision into the aggregations' metadata.

(f) Metadata		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
49	The ERKS must -	
	(a) support an authorised individual to create, modify and delete metadata elements and/or values (of metadata elements) of aggregations, records and other entities; and	C(282) Test whether the ERKS supports an authorised individual to specify the allowable values for a metadata element and restricts users to input or select only allowable value(s) for a metadata element. C(283) Test whether the ERKS supports an authorised individual to perform the following - (a) adding a new metadata element with specified allowable values other than those specified in RKMS for an entity other than records and aggregations. It is assumed that the values of the metadata element are editable; (b) rename a metadata element of an entity; (c) adding additional allowable values to a metadata element; (d) modifying the metadata values such as “Title” of a disposal hold; (e) deleting the new metadata element created under (a) above; and

(f) Metadata		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		(f) ensuring that metadata values that are not changeable for an entity such as "System identifier" prescribed in RKMS remain unchangeable throughout the life cycle of records. Please see also C(57) and C(290).
	(b) in the case of creation, allow the authorised individual to define, and subsequently modify the formats[55], sources, entry modes[56] of the metadata elements, and determine whether entry of a value is mandatory or optional.	C(284) Test whether the ERKS supports an authorised individual to define the formats, sources and entry modes of the new metadata elements as created under C(57)(a), C(57)(b) and C(283)(a) and specify the entry of the metadata value as mandatory. C(285) Test whether the ERKS supports an authorised individual to modify the formats, sources and entry modes of the new metadata elements as created under C(57)(a), C(57)(b) and C(283)(a). Change the entry of the metadata value as optional.
50	The ERKS must -	
	(a) support an authorised individual to create and define different metadata profiles for different levels	C(286) Test whether the ERKS supports an authorised individual to create a specific metadata profile (with different

[55] The formats include alphabetic, alphanumeric, numeric, date and logical (i.e. Yes/No, True/False).

[56] Entry modes here refer to whether the metadata element values are to be entered and maintained by manual entry, from selection or automatic capture by the system.

(f) Metadata		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
	and types of aggregations, records and other entities[57]; and	metadata elements, different metadata values, different obligation levels of the metadata elements, etc.) for - (a) different levels of aggregations (i.e. a class, sub-class, folder, sub-folder (if implemented) and part); (b) different types of aggregations (i.e. physical, electronic and hybrid); (c) different record forms (i.e. electronic and non-electronic records); and (d) other entities such as a records retention and disposal schedule.
	(b) allow an authorised individual to restrict the viewing or modification of metadata values by user, user group, or user role.	C(287) Test whether the ERKS supports an authorised individual to specify whether a user, user group or user role have the right to modify or view metadata values. The ERKS should enforce the restrictions once the authorised individual has put them in effect.
51	The ERKS must -	

[57] The ERKS must not present any practical limitation on the number of metadata elements allowed for an aggregation, a record and other entities.

(f) Metadata		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
	(a) ensure metadata to be persistently linked to the associated aggregations, records and other entities[58] as specified in RKMS and by the B/D concerned; and	C(288) Test whether the ERKS ensures that metadata are persistently linked to the associated aggregations, records and other entities as specified in RKMS and by the B/D concerned. Such linkage should be maintained even though the associated entities have been re-classified. Metadata should be linked to their associated entities when they are exported or transferred.
	(b) support validation of metadata values [59] and prevent the alteration of metadata elements and values, unless authorised (Please see **Requirements 49 and 50**).	C(289) Test whether the ERKS supports creation of pre-defined rules and measures to validate the values of metadata elements. C(290) Test whether the ERKS restricts the alteration of metadata elements and values to those authorised individuals specified by the B/D concerned. In any event, the ERKS should deny any change to the values for metadata elements that are not editable such as "System identifier", "Electronic signature identifier", "Encryption indicator" and "Date disposed" by an authorised individual.

[58] Examples of other entities specified in RKMS include a user and a records retention and disposal schedule.

[59] For example, the system provides validation of date format of the metadata values.

(f) Metadata			
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**	
52	The ERKS must maintain and manage metadata associated with records and aggregations throughout the whole life cycle of records and support the retention of a range of metadata beyond the life of aggregations and records therein. *[Note: A set of aggregation level metadata to be retained after destruction or transfer of the aggregations and records therein is specified in RKMS.]*	C(291)	Test whether the ERKS ensures that metadata associated with records and aggregations created and captured in the ERKS are secure from unauthorised access, alteration and deletion and are kept throughout the life cycle of records.
		C(292)	Test whether the ERKS supports the management and retention of selected metadata elements after an aggregation has been destroyed.

(g) Language Support		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
53	The ERKS must support the full Chinese language character set for all software applications, utilities, viewers, drivers, Application Programme Interfaces (APIs), etc. The relevant design should be based on the ISO 10646/Unicode (i.e. to permit the system to index and manage Traditional and Simplified Chinese as well as any other characters specific to the recording of information in Hong Kong both in the past and the present) and also support the Hong Kong Supplementary Character Set.	C(293) Test whether the ERKS supports use and display of English and/or Traditional Chinese in all user interfaces as specified by the B/D concerned. C(294) Test whether the ERKS supports use and display of metadata values in English, Traditional Chinese and Simplified Chinese and ensures that the metadata values are searchable and retrievable. C(295) Test whether the ERKS supports full text search and retrieval of records with contents in - (a) Traditional Chinese only; (b) Simplified Chinese only; (c) English only; (d) Traditional Chinese and Simplified Chinese; (e) Traditional Chinese and English; (f) Simplified Chinese and English; and (g) Traditional Chinese, Simplified Chinese and English. C(296) Test whether the ERKS supports the use and display of the latest version of the Hong Kong Supplementary Character Set, including in metadata values.

(h) Administration		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
54	The ERKS must -	
	(a) provide flexible reporting facilities for an authorised individual to request for reports on statistics and management information based on selected criteria[60], on a regular or an ad hoc basis. Such reports and information must include but are not limited to the following -	C(297) Test whether the ERKS provides reporting tools for an authorised individual to create regular (e.g. daily, weekly, monthly, half-yearly and yearly) or ad hoc reports based on selected criteria. The ERKS should ensure that an authorised individual is able to determine the sorting criteria of information to be included in a report. C(298) Test whether the ERKS supports an authorised individual to generate a pre-defined report based on report templates and/or saved report requests. C(299) Test whether the ERKS allows viewing and printing of reports and storing them in electronic form. C(300) Test whether the ERKS creates time periods for reports by using a date range. C(301) Test whether the ERKS generates user-defined reports documenting statistics and management information as specified by the B/D concerned. C(302) Test whether the ERKS supports flexible printing of labels

[60] For example, an authorised individual may compile statistics on the quantity of records based on any selected security classification.

(h) Administration		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		for physical aggregations and non-electronic records.
	(i) quantity, movement, location and transaction statistics[61] of aggregations and records;	C(303) Test whether the ERKS supports creation of regular or ad hoc reports showing the actual quantity, movement and locations of aggregations and records, e.g. a report showing the quantity of records with CONFIDIENTIAL security classification in a sub-class in megabytes. C(304) Test whether the ERKS supports creation of regular or ad hoc reports showing transactions statistics of aggregations and records such as the number of records captured into an aggregation. C(305) Regarding C(303) and C(304), test whether the ERKS allows sorting and totalling of information to be displayed in the report based on user-defined criteria. For example, a report shows the quantity of CONFIDENTIAL folders by sub-class.
	(ii) metadata and audit trails;	C(306) Test whether the ERKS supports creation of regular or ad hoc reports showing metadata of entities. C(307) Test whether the ERKS supports creation of regular or ad hoc reports showing audit trail data based on a specified

[61] For example, an authorised individual may compile statistics on the quantity of records captured into a folder within a period of time.

(h) Administration		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		entity such as a class, sub-class, folder, user, date range. C(308) Regarding C(306) and C(307), test whether the ERKS allows sorting and totalling of information to be displayed in the report based on user-defined criteria.
	(iii) records classification;	C(309) Test whether the ERKS supports creation of regular or ad hoc reports showing the structure of a records classification scheme and aggregations created in the records classification scheme and any other reports specified by the B/D concerned for records classification.
	(iv) records retention and disposal;	C(310) Test whether the ERKS supports creation of regular or ad hoc reports for the management of records retention and disposal including the following and any other reports specified by the B/D concerned - (a) a report listing all records retention and disposal schedules and sorted by user-defined criteria; (b) a report listing all aggregations to which a specified records retention and disposal schedule is applied and sorted by user-defined criteria; (c) a report listing the records retention and disposal schedules that have been applied (including

(h) Administration		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		inherited and allocated schedules) to a specific aggregation(s) and sorted by user-defined criteria; (d) a report listing all aggregations to which no records retention and disposal schedules have been applied and sorted by user-defined criteria; (e) a report listing all aggregations that are due for final disposal by a specified date or a date range and sorted by user-defined criteria; (f) a report listing all aggregations that a disposal hold has been applied and sorted by user-defined criteria; (g) a report listing aggregations and records that have been imported, exported or transferred and sorted by user-defined criteria; (h) a report listing aggregations and records that have failed to be exported or transferred; and (i) a report listing the stubs of aggregations that have been destroyed or transferred and sorted by user-defined criteria.
	(v) users' activities;	C(311) Test whether the ERKS supports creation of regular or ad hoc reports on actions performed by users and

(h) Administration		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		authorised individuals (e.g. capturing of records, creation of folders, destruction of records, export of records and charged-out of non-electronic records) and the affected entities.
	(vi) security and access control; and	C(312) Test whether the ERKS supports creation of regular or ad hoc reports on - (a) user profiles and information including membership of user groups and user roles; (b) access rights of users, user groups and user roles; (c) security classifications of aggregations and records; and (d) security clearance of users.
	(vii) system management [62], administrative parameters[63], etc. of the system; and	C(313) Test whether the ERKS supports an authorised individual to monitor the storage space of the ERKS through reporting facilities. C(314) Test whether the ERKS supports an authorised individual to monitor quantities, performance and exceptions of

[62] For example, an authorised individual may generate a report detailing any failure during a transfer, export or destruction operation.
[63] For example, an authorised individual may generate a report about the changes to users' access rights.

(h) Administration		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		the ERKS through reporting facilities. C(315) Test whether the ERKS allows creation of reports reporting on the outcome of system management activities such as outcome of an export, a transfer or a records destruction process.
	(b) include features of sorting, totalling and summarising report information and support an authorised individual to print and export reports into pre-defined formats for use in other applications and restrict users' access to selected reports.	C(316) Test whether the ERKS provides features to create reports, sort its information according to users' preference and select the information included in a report. C(317) Test whether the ERKS includes features to total and summarise information of reports. For example, creating a report covering all records in a class, totalling the number of records under the class and summarising the types of folders under this class. C(318) Test whether the ERKS supports an authorised individual to export reports into pre-defined formats (such as Microsoft Excel and PDF formats) as defined by the B/D concerned for further use in another software application. C(319) Test whether the ERKS restricts access to selected reports by users according to the decision of the B/D

(h) Administration		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		concerned.
55	The ERKS must support an authorised individual to -	
	(a) print administrative information of the ERKS such as records retention and disposal schedules, lists of user groups, records classification scheme, metadata profiles, etc.; and	C(320) Test whether the ERKS supports printing of the following information and other information as specified by the B/D concerned - (a) a list of user roles defined for carrying out functions and activities of the ERKS (including those defined by the B/D concerned); (b) a list of user groups with specified access rights; (c) a list of all electronic folders, hybrid folders, or physical folders (with their titles, classification codes and security classifications) and all sub-classes (with their titles, classification codes and security classifications) within a sub-class; (d) a list of all sub-classes (with their titles, classification codes and security classifications) within a class; (e) a list of classes with all their child sub-classes, folders, sub-folders (if implemented) and parts (with the titles, classification codes and security classifications of the classes and their child

(h) Administration		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
		aggregations) within a records classification scheme; (f) the whole records classification scheme; (g) a list of records retention and disposal schedules; (h) the metadata profile of each entity such as a record; and (i) other administrative parameters. ***Where*** the information to be printed exceeds one page, the ERKS should support printing of multiple pages in one go.
	(b) specify printing settings for records, metadata and other data within the ERKS that can meaningfully be printed.[64]	C(321) Test whether the ERKS supports an authorised individual to specify the format, contents and sequence of the administrative information to be printed as specified in C(320).
56	The ERKS must -	
	(a) support an authorised individual to indicate[65] that	C(322) Test whether the ERKS provides an effective mechanism

[64] For example, an authorised individual may specify the format and sequence of the selected metadata for printing.
[65] This indication should be included as a metadata element.

(h) Administration		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
	selected aggregations and records contain, or are considered to be, vital records[66]; and	for an authorised individual to indicate selected aggregations contain, and selected records are, vital records. The effective mechanism should minimise manual efforts and errors. C(323) Test whether the ERKS provides an effective mechanism for an authorised individual to indicate selected aggregations no longer contain, and selected records no longer are, vital records. The effective mechanism should minimise manual efforts and errors.
	(b) support replication of vital records onto other storage media for off-site storage separated from "full" back-ups[67] of ERKS data and restoration of vital records ("vital" back-up) entirely independently of, and at a different time to, "full" restoration, to cope with emergency or a disaster.[68]	C(324) Test whether the ERKS supports an authorised individual to perform a back-up of vital records separate from a "full" back-up. C(325) Test whether the ERKS supports an authorised individual to restore a "vital" back-up. Afterwards the ERKS should be fully functional to facilitate users to retrieve and access such vital records.
57	The ERKS must store and protect records, aggregations,	C(326) Test whether the ERKS stores records, aggregations,

[66] The ERKS must allow an authorised individual to indicate that selected aggregations and records no longer contain, or are considered to be, vital records. This action must be logged in the audit trails.

[67] The ERKS must provide scheduled and automated regular back-up of all or specified ERKS data and support recovery if needed.

[68] After recovering from a "vital" back-up, the ERKS must be fully operational to facilitate access to vital records.

(h) Administration		
Mandatory functional requirement as specified in FR of an ERKS		**Checkpoint**
	record indices, associated metadata and all other information required to manage them in the ERKS.	record indices, associated metadata and all other information required to manage them in the ERKS. C(327) Test whether the ERKS complies with Security Regulations, Baseline IT Security Policy and IT Security Guidelines to protect the storage of records, aggregations, record indices, associated metadata and all other information required.
58	***Where*** multiple repositories (in multiple physical locations) are implemented, the ERKS must store and protect records, aggregations, record indices, associated metadata and all other information required to manage them in the repositories of the ERKS.	C(328) ***Where*** multiple repositories are implemented, test whether the ERKS stores records, aggregations, record indices, associated metadata and all other information required to manage them in the repositories of the ERKS. C(329) ***Where*** multiple repositories are implemented, test whether the ERKS complies with Security Regulations, Baseline IT Security Policy and IT Security Guidelines to protect the storage of records, aggregations, record indices, associated metadata and all other information required in all repositories of the ERKS.

OPTIONAL REQUIREMENTS

(i) Workflow		
Optional functional requirement as specified in FR of an ERKS		**Checkpoint**
59	The ERKS should support a user to route aggregations and/or records in a controlled way to user(s), user group(s), user role(s), etc. for specific actions, e.g. seek approval.	C(330) Test whether the ERKS supports a user to route a number of records (not less than five) to a user group or user role (containing not less than five users) for specific actions such as seeking comments on a draft report. C(331) Test whether the ERKS supports a user to route a number of records (not less than five) and a number of aggregations (not less than five) to a number of users in a sequential order for a specific action. C(332) Test whether the ERKS supports a user to route a number of records (not less than five) and a number of aggregations (not less than five) to a number of users in parallel for a specific action such as collating a return. C(333) Test whether the ERKS denies a user's access to a record or an aggregation which the user does not have the access rights or sufficient security clearance even if the workflow assigns him/her an action upon that aggregation or record.
60	The ERKS should support an authorised individual and a user to initiate and/or perform records management	C(334) Test whether the ERKS provides pre-defined workflows to support an authorised individual to initiate and/or

(i) Workflow		
Optional functional requirement as specified in FR of an ERKS		**Checkpoint**
	functions.[69]	perform a records management function such as notifying a user group of creation of a new folder and providing a link to the newly-created folder to a user group. C(335) Regarding C(334), test whether the ERKS supports a user(s) to receive the workflow initiated by an authorised individual and perform the records management function as required in the workflow. The ERKS should inform a user of the receipt of a workflow requiring his action. C(336) Test whether the ERKS provides pre-defined workflows to support a user to initiate and/or perform a records management function such as sending a request to reserve the use of a physical folder by a future date. C(337) Test whether the ERKS maintains the relationships among the records such as comments, views and approvals generated in the workflow during the workflow process and after the completion of the workflow.

[69] For example, an authorised individual in the position of a Records Manager may initiate a workflow to route folders (in the form of a hyperlink) that are due for a review of their records retention and disposal schedules to users for the latter to review the cases from business perspective.

(i) Workflow		
Optional functional requirement as specified in FR of an ERKS		**Checkpoint**
61	The ERKS should support an authorised individual to define, add, amend and maintain pre-programmed workflows involving the use of records.	C(338) Test whether the ERKS supports an authorised individual to change a pre-programmed workflow such as changing the pre-defined recipient(s) of the next step in a workflow. C(339) Test whether the ERKS supports an authorised individual to create a new workflow such as a two- or three-step workflow and save the created workflow for subsequent use. C(340) Regarding C(339), test whether the ERKS supports a user to use the new workflow and route a number of records to the workflow for sending to another user(s), a user group or a user role for action such as seeking comments on those records. C(341) Regarding C(339), test whether the ERKS supports the authorised individual to delete a step within the workflow and save the change to the workflow. Test whether a user can use the revised workflow and route a number of records for sending to another user(s), a user group or a user role for action.

Appendix 2

Evaluation of an electronic recordkeeping system for compliance with the Recordkeeping Metadata Standard for the Government of the Hong Kong Special Administrative Region

Part I - Overview

This appendix provides guidelines for bureaux and departments (B/Ds) to evaluate the compliance of an electronic recordkeeping system (ERKS) with requirements regarding the creation, capture, use, management and maintenance of recordkeeping metadata as specified in the ***Recordkeeping Metadata Standard for the Government of the Hong Kong Special Administrative Region*** (RKMS) (version 1.1).

2. To assist B/Ds in evaluating how well an ERKS creates, captures, uses, manages and maintains recordkeeping metadata in accordance with requirements prescribed in RKMS, a total of 24 key checkpoints have been specified in **Part II**. B/Ds should, on the basis of these key checkpoints, draw up comprehensive test cases that suit their business, operational and records management context to test an ERKS in the context of system acceptance tests and user acceptance tests. B/Ds should also test the import, export and/or transfer of recordkeeping metadata if their ERKSs have implemented requirements pertaining to Application Profile (AP) 3 and/or AP4 as specified in RKMS.[1] For existing ERKSs, B/Ds should conduct a compliance assessment according to the circumstances set out in paragraph 2.9 of **Chapter 2**.

3. B/Ds should note that the checkpoints specified in **Part II** only covers requirements of recordkeeping metadata as specified in RKMS. Other checkpoints related to metadata as specified in the ***Functional Requirements of an Electronic Recordkeeping System*** (FR of an ERKS) are included in checkpoints C(282) to C(292)

[1] AP2 of RKMS specifies a subset of metadata elements to be exported or transferred with records, aggregations and other entities (if required) from an information system (other than an ERKS) to an ERKS for the latter to properly manage and store the records. It falls beyond the scope of this appendix to test whether an information system complies with requirements pertaining to AP2 of RKMS. An ERKS which imports metadata elements with records, aggregations and other entities (if required) exported or transferred from an information system should comply with requirements pertaining to AP1. B/Ds should make reference to RKMS and the ***Recordkeeping Metadata Standard for the Government of the Hong Kong Special Administrative Region: Implementation Guidelines*** for guidance to evaluate the compliance of an information system with AP2 of RKMS.

of **Appendix 1** to the manual. These two appendices should be read together. B/Ds may add other checkpoints if deemed necessary such as validating the compliance of an ERKS with B/D-specific entities, metadata elements and values and/or encoding schemes as prescribed in their departmental recordkeeping metadata standards.

4. Upon completion of a testing of an ERKS, B/Ds should determine the appropriate rating of the ERKS as prescribed in paragraph 2.18 of **Chapter 2**.

5. Key records management terms used in this appendix are consistent with those of RKMS. Please refer to **Annex 8** of RKMS for a glossary of key records management terms.

Part II – Key checkpoints

6. A total of **24** key checkpoints (C(342) to C(365)) covering requirements on entities, encoding schemes and recordkeeping metadata pertaining to AP1, AP3 and AP4 as defined in RKMS are specified in the following table. Readers are requested to note that -

(a) "**the ERKS**" denoted in the following table refers to the ERKS being tested and evaluated;

(b) the term "**test**" is used when the ERKS, a user or an authorised individual as appropriate shall execute an action and it is expected that the action shall be successfully completed;

(c) B/Ds should assume that there is more than one authorised individual in their organisations. Authorised individuals may have access to different records classification schemes (if multiple records classification schemes have been implemented), different parts of a records classification scheme (if a single records classification scheme has been implemented) and/or different system functions according to their roles. For example, an authorised individual may include the Departmental Records Manager, records managers, registry staff and system administrator(s); and

(d) checklists set out in the following table are closely related to those checkpoints specified in **Appendix 1** to the manual because recordkeeping metadata support effective and efficient management of records throughout the life cycle of records.

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
C(342)	Test whether the ERKS applies recordkeeping metadata specified in RKMS to all electronic and non-electronic records (regardless of their formats and media) managed by the system. (See **section 1.3** of RKMS for details.) **<u>Points to note</u>:** (a) Some metadata elements defined in RKMS are applicable to both electronic records and non-electronic records, e.g. "Title" and "Security classification" while some metadata elements are specific to electronic records, e.g. "Electronic signature indicator" or to non-electronic records, e.g. "Location - home" and "Medium". (b) Some metadata elements defined in RKMS are specific to a particular type of records, e.g. "Encryption indicator" is applicable to an e-mail or e-Memo record only. (c) Please see related checkpoints C(90), C(91), C(112) to C(113) of **Appendix 1** to the manual.	✓	✓	✓
C(343)	Test whether the ERKS creates, captures, uses, manages and maintains **sufficient, accurate, complete** and **consistent metadata elements and values** for the **16 entities**[2] defined in **section 3.4.2** of RKMS to ensure the authenticity, integrity, reliability and usability of records throughout their life cycle.	✓	✓	✓

[2] Entities defined in RKMS are (1) Records Classification Scheme; (2) Class; (3) Sub-class; (4) Folder; (5) Sub-folder; (6) Part; (7) Record; (8) Component; (9) Disposal Hold; (10) Retention and Disposal Schedule; (11) Event History; (12) Event Trigger; (13) Mandate; (14) Stub; (15) User; and (16) Group. The entity **Sub-folder** is optional for use while the entity **Event History** is recommended for implementation in an ERKS.

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	The ERKS must - (a) adopt definitions, rules and encoding schemes and comply with requirements pertaining to AP1 as specified in **Chapter 3**, **Chapter 4**, **Annex 1** (Metadata elements by application profile), **Annex 2** (Entities and their metadata elements), **Annex 3** (Metadata element definition tables) and **Annex 5** (Encoding schemes) of RKMS to create, capture, use, manage and maintain metadata elements and their permitted values for - (i) metadata of **mandatory** and **conditional mandatory** obligation levels of all entities (except for the entities **Sub-folder** which is optional for use and **Event History** which is recommended for implementation) defined in **section 3.4** of RKMS; (ii) metadata of **recommended** and **optional** obligation levels (if these metadata have been implemented by B/Ds in their ERKSs) of all entities (except for the entities **Sub-folder** which is optional for use and **Event History** which is recommended for implementation) defined in **section 3.4** of RKMS; (iii) metadata of **mandatory** and **conditional mandatory** obligation levels of entities, namely **Sub-folder** and **Event History** (if these entities have been implemented by B/Ds in their ERKSs); and (iv) metadata of **recommended** and **optional** obligation levels (if these metadata have been implemented by B/Ds in their ERKSs) of			

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	entities, namely **Sub-folder** and **Event History** (if these entities have been implemented by B/Ds in their ERKSs); (b) adopt definitions, naming and numbering conventions, rules and encoding schemes and comply with requirements pertaining to AP3 and/or AP4 (if the latter two APs have been implemented in the ERKS) as specified in **Chapter 3**, **Chapter 4**, **Annex 1** (Metadata elements by application profile), **Annex 2** (Entities and their metadata elements), **Annex 3** (Metadata element definition tables) and **Annex 5** (Encoding schemes) of RKMS to create, capture, use, manage and maintain metadata elements and their permitted values for - (i) metadata of **mandatory** and **conditional mandatory** obligation levels of all entities (except for the entities **Sub-folder** which is optional for use and **Event History** which is recommended for implementation) defined in **section 3.4** of RKMS; (ii) metadata of **recommended** and **optional** obligation levels (if these metadata have been implemented by B/Ds in their ERKSs) of all entities (except for the entities **Sub-folder** which is optional for use and **Event History** which is recommended for implementation) defined in **section 3.4** of RKMS; (iii) metadata of **mandatory** and **conditional mandatory** obligation levels of entities, namely **Sub-folder** and **Event History** (if these			

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	entities have been implemented by B/Ds in their ERKSs); and (iv) metadata of **recommended** and **optional** obligation levels (if these metadata have been implemented by B/Ds in their ERKSs) of entities, namely **Sub-folder** and **Event History** (if these entities have been implemented by B/Ds in their ERKSs); and (c) adopt encoding schemes with definitions, rules and requirements specified for the properties of encoding schemes set out at **Annex 5** of RKMS to create or capture permitted value(s) for specific metadata elements defined at **Annex 3** of RKMS. (See **section 2.6**, **Chapter 3**, **Chapter 4**, **Annex 1**, **Annex 2**, **Annex 3**, **Annex 5** and **Annex 7** of RKMS for details.) **<u>Points to note</u>**: To demonstrate that the ERKS meets this checkpoint, the ERKS should - (a) have the recordkeeping metadata with the same definition as those specified in RKMS though an ERKS solution may not adopt the same naming and numbering conventions for recordkeeping metadata as specified in RKMS;			

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	<u>Example 1 illustrating compliance</u> The RKMS specifies the metadata element "Date time captured" for a record. It is permitted to have an ERKS to use another naming such as "Date time filed" to describe the metadata element "Date time captured" with the same definition. B/Ds should note that when the metadata element "Date time filed" with its value(s) are exported or transferred from the ERKS to another ERKS or to the Public Records Office (PRO) of GRS, the naming of "Date time filed" should be converted into "Date time captured" as specified in **AP3** or **AP4** of RKMS. Please see C(357), C(358), C(360) and C(361). (b) be able to convert the values of the encoding schemes in the ERKS into the values of corresponding encoding schemes as specified in RKMS for export or transfer of metadata values as specified in **AP3** or **AP4** of RKMS;			

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	<u>Example 2 illustrating compliance</u> The value of metadata element of "Date created" should be in the date format (viz. YYYY-MM-DD) as specified in the "Date encoding scheme" specified in RKMS. B/Ds may allow users to select or input in an ERKS a value for "Date created" in other date formats, e.g. DD-MM-YYYY or in free text, e.g. 21st December, 2009. But when the values of the metadata element of "Date created" are exported or transferred under **AP3** or **AP4**, B/Ds should convert the format DD-MM-YYYY into YYYY-MM-DD as stipulated in that of RKMS. (c) ensure that different entities have the correct set of metadata elements and permitted values specified in RKMS; (d) demonstrate that metadata elements and values serve their purposes as specified in RKMS in a proper manner in the ERKS; and			

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	Example 3 illustrating non-compliance The value of the recordkeeping metadata element "System identifier" should be unique within an ERKS so as to enable identification of an entity uniquely across the ERKS. In case an ERKS assigns the same value of the "System identifier" to two entities, it means that this ERKS fails to ensure that the purpose of the metadata element "System identifier" is fulfilled. Rectification should be carried out to redress the problem. **Example 4 illustrating non-compliance** The recordkeeping metadata element "Relation - has enclosure" should be implemented together with another metadata element "Relation - is enclosure of" to link a record and its enclosure in physical form. If a B/D only implements one of the two metadata elements in the ERKS, the purposes of these two metadata elements will be compromised. (e) demonstrate that recordkeeping metadata values for entities are accurate, complete, consistent and reliable.			

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	Example 5 illustrating non-compliance An ERKS allows inheritance of metadata values from a higher level aggregation to its child aggregations at the system configuration but does not support automatic updating of metadata values through inheritance. Any subsequent updating of metadata values of the higher level aggregation will cause inconsistencies in metadata values between this aggregation and its child aggregations. For example, the value of the metadata element "Owner" of a sub-class has been changed but the value of this metadata element of its child aggregations remains unchanged. This will cause doubt on the integrity and accuracy of metadata values.			
C(344)	Test whether the ERKS supports creation and capture of values for metadata elements of records and other entities defined in RKMS. The ERKS should ensure that **permitted** values are created or captured **as soon as possible** when the entity is created or when an event affecting the entity occurs. (See **sections 2.5**, **2.7**, **2.8**, **Chapter 4** and **Annex 3** of RKMS for details.)	✓	✓	✓

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	<u>Example 1 illustrating non-compliance</u> The values of recordkeeping metadata elements including "Title", "Date time captured", "Creator name", "Creator organization name", "System identifier" and "Security classification" of a record should be created or captured in the ERKS at the time of capturing the record so as to ensure the authenticity, reliability and integrity of the record. If the ERKS allows those metadata values to be created or captured at any time after the capture of the record into the system, this will compromise the purposes set out in **section 1.2** of RKMS. **<u>Example 2 illustrating compliance</u>** The value of the recordkeeping metadata element "Date disposed" should be system-generated or user-generated immediately once an aggregation was disposed of according to the approved records retention and disposal schedule. This is to ensure that a disposal event is properly and timely documented.			

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	<u>Example 3 illustrating compliance</u> For a record which is scanned where no Event History instance is created, the following technical information should be system-generated or user-generated immediately in the "Remark" metadata in the following sequence: (1) a unique digitisation identifier for a scanned record (usually assigned by the scanning facility) or a unique identifier assigned to the physical container storing the original record after scanning; (2) the operating scanner model; (3) name and version of the imaging software; (4) driver version; (5) image resolution; (6) colour depth; (7) compression; (8) date of scanning; and (9) agent who scanned the record to safeguard the authenticity of the scanned record. **<u>Points to note</u>:** (a) Please see related checkpoints C(19) to C(20), C(77) to C(81), C(91), C(95), C(104) and C(112) to C(115) of **Appendix 1** to the manual. (b) Please see also requirements regarding creation, capture, use, management and maintenance of metadata set out in **Chapter 4** of RKMS.			
C(345)	Test whether the ERKS **automatically** creates or captures metadata values as far as practicable through various means such as automatic capture, system generation or inheritance; and uses encoding schemes	✓	✓	✓

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	to control values permitted for a metadata element as far as practicable. (See **section 6.2** and **Annex 3** of RKMS for details.) **<u>Points to note</u>:** (a) Please see related checkpoints C(19) to C(20), C(77) to C(81), C(91), C(95), C(104) and C(112) to C(115) of **Appendix 1** to the manual. (b) Modes of creation and capture of metadata include system generation, automatic capture, inheritance and manual input. For each metadata element prescribed in RKMS, the modes of creation, capturing and inheritance of its metadata value(s) are specified in its corresponding metadata element definition table at **Annex 3** of RKMS under the properties "capturing mode", "inheritance" and "source".			
C(346)	Test whether the ERKS **persistently describes and maintains the relationships including interdependencies among metadata elements and their values** as defined in RKMS, particularly at **Annex 3** and **Annex 7** so as to ensure the authenticity, integrity, reliability and usability of records and to reflect changes and other events that have affected the records and other entities. (See **section 2.10**, **Annex 3** and **Annex 7** of RKMS for details.)	✓	✓	✓

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	<u>An example illustrating compliance</u> The recordkeeping metadata element "Relation - has attachment" should be implemented together with another metadata element "Relation - is attachment of" to link between a record and its attachment(s). B/Ds must manage an e-mail with its attachment(s) as a single unit in the form of a compound record with these two metadata elements. The ERKS should demonstrate and maintain such persistent relationship between an e-mail and its attachment(s) to ensure that they are managed as a single unit. For instance, the ERKS should ensure that a search of an e-mail record will enable a user to retrieve its attachment(s) as well. **<u>Point to note</u>:** The relationships among metadata elements are also illustrated and described in the XML schema at **Annex 7** of RKMS.			
C(347)	Test whether the ERKS persistently **describes and maintains the relationships among entities and instances of entities** throughout the life cycle of records in accordance with the followings - (a) entity-relationship models detailed in **sections 3.5 to 3.10** and in **sections 3.12** and **3.13** of RKMS; (b) parent-child relationship set out in **sections 3.14** and **3.15** of RKMS; (c) event-driven relationship set out in **sections 3.14**	✓	✓	✓

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	and **3.16** of RKMS; and (d) associative relationship set out in **sections 3.14**, **3.17 to 3.19** of RKMS. (See **sections 3.5 to 3.10** and **3.12 to 3.19** of RKMS for details.)			
C(348)	Test whether the ERKS manages e-mail records or e-Memo records with attachment(s) in electronic form in the form of compound records. The ERKS should use metadata elements "Relation - has attachment" and "Relation - is attachment of" to describe and maintain the relationship between the parent record and child record(s) of a compound record. (See **sections 3.14**, **3.17** and **3.18** of RKMS for details.) **Points to note:** (a) The parent record and child record(s) of a compound record should be managed as a single unit as stipulated in **Requirement 11** of FR of an ERKS. (b) Please see related checkpoints C(88), C(89), C(116), C(163), C(265) and C(275) of **Appendix 1** to the manual.	✓		
C(349)	***Where*** the ERKS manages electronic records (other than e-mail/e-Memo records) with attachment(s) in electronic form in the form of compound records, test whether the ERKS uses metadata elements "Relation - has attachment" and "Relation - is attachment of" to describe and maintain the relationship between the parent record and child record(s) of a compound record.	✓		

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	(See **sections 3.14**, **3.17** and **3.18** of RKMS for details.) **<u>Points to note:</u>** (a) B/Ds should note that management of electronic records (other than e-mail records/e-Memo records) with attachment(s) in electronic form as compound records in an ERKS is not made mandatory. Nevertheless, it is recommended that B/Ds should adopt this approach as far as practicable. The parent record and child record(s) of a compound record should be managed as a single unit as stipulated in **Requirement 11** of FR of an ERKS. (b) Please see related checkpoints C(88), C(89), C(116), C(163), C(265) and C(275) of **Appendix 1** to the manual.			
C(350)	***Where*** the ERKS manages records with enclosure(s) in physical form in the form of compound records, test whether the ERKS uses metadata elements "Relation - has enclosure" and "Relation - is enclosure of" to describe and maintain the relationship between the parent record and child record(s) of a compound record. (See **sections 3.14**, **3.17** and **3.18** of RKMS for details.) **<u>Points to note</u>**: (a) B/Ds should note that management of electronic records with enclosure(s) in physical form as compound records in an ERKS is not made mandatory. Nevertheless, it is recommended that B/Ds should adopt this approach as far as practicable. The parent	✓		

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	record and child record(s) of a compound record should be managed as a single unit as stipulated in **Requirement 11** of FR of an ERKS. (b) Please see related checkpoints C(88), C(89), C(116), C(163), C(265) and C(275) of **Appendix 1** to the manual.			
C(351)	***Where*** the ERKS manages the following records as a single unit, test whether the ERKS creates a compound record (of which its parent record is a virtual record) to describe and maintain their relationship - (a) a record with the same intellectual contents but expressed in different languages, dialects or scripts (using metadata elements "Relation - has language" and "Relation - is language of" to describe and maintain the relationship between the virtual record and child records); (b) a record with multiple versions (using metadata elements "Relation - has version" and "Relation - is version of" to describe and maintain the relationship between the virtual record and child records); (c) a record with rendition(s) (using metadata elements "Relation - has format" and "Relation - is format of" to describe and maintain the relationship between the virtual record and child records); and (d) two or more compound records (using metadata elements defined in **section 3.17** of RKMS to describe the associative relationships). (See **sections 3.14** and **3.17 to 3.19** of RKMS for	✓		

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	details.) **<u>Points to note</u>**: (a) B/Ds should note that management of records at (a) to (d) above as compound records in an ERKS is not made mandatory. ***Where*** B/Ds choose to adopt this approach, the parent record and child record(s) of a compound record should be managed as a single unit as stipulated in **Requirement 11** of FR of an ERKS. (b) Please see related checkpoints C(88), C(89), C(96), C(117), C(163), C(265) and C(275) of **Appendix 1** to the manual.			
C(352)	Test whether the ERKS ensures that metadata values that are unchangeable such as "System identifier" prescribed in RKMS remain unchangeable throughout the life cycle of records. (See **Annex 3** of RKMS for details.) **<u>Points to note</u>**: (a) The accuracy of recordkeeping metadata is important to ensure the authenticity, integrity, reliability and usability of records. (b) Please see related checkpoints C(57), C(283) and C(290) of **Appendix 1** to the manual.	✓	✓	✓
C(353)	***Where*** the **Sub-folder** entity is adopted in the ERKS, test whether the ERKS - (a) adopts the metadata elements and encoding schemes (with definitions and rules) and requirements set out in **sections 3.3 to 3.6** and **4.2**	✓	✓	✓

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	to 4.5 and at **Annex 1**, **Annex 2**, **Annex 3**, **Annex 5** and **Annex 7** of RKMS for the **Sub-folder** entity and its associated metadata; and **Point to note**: Though an ERKS solution may not adopt the same naming and numbering conventions for recordkeeping metadata of Sub-folder as specified in RKMS, B/Ds should ensure that their ERKSs have the recordkeeping metadata with the same definition as those specified in RKMS. For example, the RKMS specifies the metadata element "Title" for Sub-folder. It is permitted to have an ERKS to use another naming such as "Name" to describe the metadata element "Title" of same definition. B/Ds should note that when the metadata element "Name" with its value(s) are exported or transferred from the ERKS to another ERKS or to PRO of GRS, the naming of "Name" should be converted into "Title" as specified in AP3 or AP4 of RKMS. See C(357), C(358), C(360) and C(361). (b) describes and persistently maintains the relationships of the **Sub-folder** entity with other entities in accordance with requirements set out in **sections 3.5**, **3.6**, **3.9**, **3.10** and **3.12 to 3.16** of RKMS. (See **sections 3.3 to 3.6**, **3.9**, **3.10**, **3.12 to 3.16** and **4.2 to 4.5**, **Annex 1**, **Annex 2**, **Annex 3**, **Annex 5** and **Annex 7** of RKMS for details.)			

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	<u>Point to note</u>: B/Ds should note that implementation of entity Sub-folder in an ERKS is not made mandatory.			
C(354)	***Where*** the **Event History** entity is adopted in the ERKS, test whether the ERKS - (a) adopts the definitions, naming and number conventions, rules, encoding schemes and requirements for the **Event History** entity and event history objects and their associated metadata set out in **sections 3.23** and **4.2 to 4.5**, **Annex 1**, **Annex 2**, **Annex 3**, **Annex 5**, **Annex 6** and **Annex 7** of RKMS; and (b) describes and persistently maintains the relationships of the **Event History** entity with other entities in accordance with requirements set out in **sections 3.14** and **3.16** of RKMS. (See **sections 3.14**, **3.16**, **3.23** and **4.2 to 4.5**, **Annex 1**, **Annex 2**, **Annex 3**, **Annex 5**, **Annex 6** and **Annex 7** of RKMS for details.) **<u>Point to note</u>**: B/Ds should note that the implementation of entity Event History in an ERKS is not made mandatory. However, it is recommended that B/Ds should create, use, manage and maintain the Event History entity and event history objects with their associated metadata specified in **section 3.23**, **Annex 1**, **Annex 2**, **Annex 3**, **Annex 5** and **Annex 7** of RKMS to record audit trail data in a system-neutral format.	✓	✓	✓

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
C(355)	***Where*** an information system (other than an ERKS) - (a) integrates with the ERKS so as to enable the latter to capture and import records, aggregations and other entities (if required) with associated metadata created/received by and/or stored in the information system; or (b) exports or transfers records, aggregations and other entities (if required) with associated metadata to the ERKS for proper management and storage as specified in **AP2**; or ***where*** an ERKS exports or transfers records, aggregations and instances of other entities (if required) together with their associated metadata to **another ERKS** to meet business and/or records management purposes of **AP3**, test whether the ERKS supports import of recordkeeping metadata, records, aggregations and instances of other entities (if required) exported or transferred from the information system or another ERKS in accordance with the requirements specified for **AP1**. The ERKS must import metadata in accordance with the naming and numbering conventions, rules, encoding schemes and requirements specified at **Annex 1** (Metadata elements by application profile), **Annex 2** (Entities and their metadata elements), **Annex 3** (Metadata element definition tables) and **Annex 5** (Encoding schemes) of RKMS for - (a) metadata of **mandatory** and **conditional mandatory** obligation levels of all entities (except for the entities **Sub-folder** which is optional for use	✓		

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	and **Event History** which is recommended for implementation) defined in **section 3.4** of RKMS; (b) metadata of **recommended** and **optional** obligation levels (if these metadata have been implemented in the information system) of all entities (except for the entities **Sub-folder** which is optional for use and **Event History** which is recommended for implementation) defined in **section 3.4** of RKMS; (c) metadata of **mandatory** and **conditional mandatory** obligation levels of entities, namely **Sub-folder** and **Event History** (if these entities have been implemented in the information system); and (d) metadata of **recommended** and **optional** obligation levels (if these metadata have been implemented in the information system) for entities, namely **Sub-folder** and **Event History** which have been implemented in the information system. (See **section 1.3**, **Chapter 3**, **Chapter 4**, **Chapter 5**, **Annex 1**, **Annex 2**, **Annex 3**, **Annex 5** and **Annex 7** of RKMS for details.)			

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	<u>An example illustrating non-compliance</u> An information system exports a folder including two parts, each with 500 records with the associated recordkeeping metadata to the ERKS. If the ERKS, after bulk import of the folder, parts, records and associated metadata, is unable to maintain the relationships between records (such as an e-mail record with its attachments in the form of a compound record), between records and parts, between parts and the folder and between metadata and their associated entities, it does not meet the checkpoint C(355). **<u>Points to note</u>:** (a) B/Ds must ensure that the definitions of metadata elements and entities for which their values and instances to be **imported** to the ERKS are equivalent to the definitions of the corresponding metadata elements and entities defined in RKMS. (b) B/Ds should also test whether the ERKS supports inputting/creation of permitted metadata values for those metadata elements that are absent in the exporting information system but are required under **AP1**. For example, the values of metadata element "File format" may need to be captured for records after the bulk import of records from the exporting information system. (c) Please see related checkpoints C(29), C(31), C(83) and C(122) to C(128) of **Appendix 1** to the			

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	manual.			
C(356)	***Where*** the ERKS imports records, aggregations and instances of other entities (if required) together with their associated metadata from an information system to meet records management purposes of **AP2**, test whether the ERKS - (a) imports uniform resource identifier (URIs) (if URIs are available from the information system) together with those associated records, aggregations and instances of other entities according to the specified format defined in **Chapter 4** of RKMS; and (b) adopts the specified XML schema where applicable and complies with other related requirements set out in **Chapter 5** and **Annex 7** of RKMS to import records, aggregations and instances of other entities and values of their associated metadata. (See **sections 4.5**, **5.2 to 5.13** and **Annex 7** of RKMS for details.) **Points to note**: (a) If an information system such as an e-mail system has been integrated with the ERKS to facilitate the latter to capture records directly from the system, there may not be a need for the ERKS to adopt the specified XML schema to import records from such system. (b) B/Ds must ensure that the definitions of metadata elements and entities for which their values and instances to be **imported** are equivalent to the definitions of the	✓		

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	corresponding metadata elements and entities defined in RKMS.			
C(357)	***Where*** the ERKS exports or transfers records, aggregations and instances of other entities (if required) together with their associated metadata **to another ERKS** to meet business and/or records management purposes of **AP3**, test whether metadata are exported or transferred in accordance with the naming and numbering conventions, rules, encoding schemes and requirements specified at **Annex 1** (Metadata elements by application profile), **Annex 2** (Entities and their metadata elements), **Annex 3** (Metadata element definition tables) and **Annex 5** (Encoding schemes) of RKMS for - (a) metadata of **mandatory** and **conditional mandatory** obligation levels of all entities (except for the entities **Sub-folder** which is optional for use and **Event History** which is recommended for implementation) defined in **section 3.4** of RKMS; (b) metadata of **recommended** and **optional** obligation levels (if these metadata have been implemented by the ERKS) of all entities (except for the entities **Sub-folder** which is optional for use and **Event History** which is recommended for implementation) defined in **section 3.4** of RKMS; (c) metadata of **mandatory** and **conditional mandatory** obligation levels of entities, namely **Sub-folder** and **Event History** (if these entities have been implemented by the ERKS); and (d) metadata of **recommended** and **optional** obligation levels (if these metadata have been		✓	

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	implemented by the ERKS) for entities, namely **Sub-folder** and **Event History** (if these entities have been implemented by the ERKSs). (See **sections 3.2**, **4.6** and **4.7**, **Annex 1**, **Annex 2**, **Annex 3** and **Annex 5** of RKMS for details.) **Points to note**: (a) B/Ds must ensure that the definitions of metadata elements and entities for which their values and instances to be **exported** or **transferred** are equivalent to the definitions of the corresponding metadata elements and entities defined in RKMS. (b) Please see related checkpoints C(270), C(271), C(276), C(278) and C(279) of **Appendix 1** to the manual.			
C(358)	***Where*** the ERKS exports or transfers records, aggregations and instances of other entities (if required) together with their associated metadata to another ERKS to meet purposes of **AP3**, test whether the ERKS - (a) assigns a unique URI to each record and each instance of other entities to be exported or transferred according to the specified format defined in **Chapter 4** of RKMS; and (b) adopts the specified XML schema and complies with other related requirements set out in **Chapter 5** and **Annex 7** of RKMS to export or transfer instances of entities and values of their associated metadata. (See **sections 4.5**, **5.2 to 5.13** and **Annex 7** of RKMS for		✓	

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	details.) **<u>Point to note</u>**: B/Ds must ensure that the definitions of metadata elements and entities for which their values and instances to be **exported** or **transferred** are equivalent to the definitions of the corresponding metadata elements and entities defined in RKMS.			
C(359)	***Where*** the ERKS imports records, aggregations and instances of other entities (if required) together with their associated metadata from another ERKS for records management purposes of **AP3**, test whether the ERKS (the receiving ERKS) - (a) imports URIs together with those associated records, aggregations and instances of other entities according to the specified format defined in **Chapter 4** of RKMS; and (b) adopts the specified XML schema and comply with other related requirements set out in **Chapter 5** and **Annex 7** of RKMS to import records, aggregations and instances of other entities and values of their associated metadata. (See **sections 4.5**, **5.2 to 5.13** and **Annex 7** of RKMS for details.) **<u>Points to note</u>**: (a) B/Ds must ensure that the definitions of metadata elements and entities for which their values and instances to be **imported** are equivalent to the definitions of the corresponding metadata elements and entities	✓		

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	defined in RKMS. (b) B/Ds should also test whether the ERKS supports inputting/creation of permitted metadata values for those metadata elements that are absent in the exporting information system but are required under **AP1**. For example, the values of metadata element "File format" may need to be captured for records after the bulk import of records from the exporting information system. (c) Please see related checkpoints C(122) to C(128) of **Appendix 1** to the manual.			
C(360)	***Where*** the ERKS transfers records with archival value, aggregations and instances of other entities (if required) together with their associated metadata to PRO of GRS, test whether the ERKS transfers metadata in accordance with the naming and numbering conventions, rules, encoding schemes and requirements specified at **Annex 1** (Metadata elements by application profile), **Annex 2** (Entities and their metadata elements), **Annex 3** (Metadata element definition tables) and **Annex 5** (Encoding schemes) of RKMS for - (a) metadata of **mandatory** and **conditional mandatory** obligation levels of all entities (except for the entities **Sub-folder** which is optional for use and **Event History** which is recommended for implementation) defined in **section 3.4** of RKMS; (b) metadata of **recommended** and **optional** obligation levels (if these metadata have been implemented by the ERKS) of all entities (except			✓

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	for the entities **Sub-folder** which is optional for use and **Event History** which is recommended for implementation) defined in **section 3.4** of RKMS; (c) metadata of **mandatory** and **conditional mandatory** obligation levels of entities, namely **Sub-folder** and **Event History** (if these entities have been implemented by the ERKS); and (d) metadata of **recommended** and **optional** obligation levels (if these metadata have been implemented by B/Ds in their ERKSs) for entities, namely **Sub-folder** and **Event History** (if these entities have been implemented by the ERKS). (See **sections 1.3**, **3.2**, **4.6** and **4.7**, **Annex 1**, **Annex 2**, **Annex 3** and **Annex 5** of RKMS for details.) **Points to note**: (a) B/Ds must ensure that the definitions of metadata elements and entities for which their values and instances to be **transferred** are equivalent to the definitions of the corresponding metadata elements and entities defined in RKMS. **An example illustrating non-compliance** The permitted values of metadata element "Record form" should comply with the "Record form encoding scheme" specified in RKMS viz. "electronic" or "non-electronic". If an ERKS transfers values such as "born digital", "scanned" or "physical" of this metadata element to PRO of GRS, the ERKS fails to meet this checkpoint.			

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	(b) Please see related checkpoints C(270), C(271), C(276), C(278) and C(279) of **Appendix 1** to the manual.			
C(361)	***Where*** the ERKS transfers records with archival value, aggregations and instances of other entities (if required) together with their associated metadata to PRO of GRS, test whether the ERKS - (a) assigns a unique URI to each record and each instance of other entities to be transferred according to the specified format defined in **Chapter 4** of RKMS; and (b) adopts the specified XML schema and complies with other related requirements set out in **Chapter 5** and **Annex 7** of RKMS to transfer records with archival value, aggregations and instances of other entities together with values of their associated metadata. (See **sections 4.5**, **5.2 to 5.13** and **Annex 7** of RKMS for details.) **Point to note**: B/Ds must ensure that the definitions of metadata elements and entities for which their values and instances to be **transferred** are equivalent to the definitions of the corresponding metadata elements and entities defined in RKMS.			✓
C(362)	Test whether the ERKS provides controlled processes to make changes to metadata elements and values and encoding schemes and restrict the amendments of metadata elements/values and encoding schemes to	✓	✓	✓

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	those authorised individuals. (See **sections 6.6** and **6.7** of RKMS for details.) **<u>Points to note</u>**: (a) B/Ds should ensure that any revisions made to metadata elements and values and encoding schemes of records and other entities would not compromise the authenticity, integrity, reliability and usability of records. (b) The ERKS should ensure that metadata values that are unchangeable such as "System identifier" prescribed in RKMS remain unchangeable throughout the life cycle of records. The ERKS must not allow an authorised individual to amend or delete metadata values that are unchangeable.			
C(363)	Test whether the ERKS protects and stores metadata properly and back up metadata in the same way as records to which they apply. (See **section 6.7** of RKMS for details.) **<u>Point to note</u>**: Please see related checkpoints C(181), C(182), C(188), C(224), C(290) to C(292) and C(326) to C(329) of **Appendix 1** to the manual.	✓		

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
C(364)	Test whether the ERKS retains metadata for as long as the records to which they apply and maintains a number of selected metadata elements for aggregations that have been destroyed or transferred in the form of a "Stub" defined in RKMS. (See **section 6.7** of RKMS for details.) **Points to note**: (a) Aggregations that have been destroyed or transferred will be replaced by stubs. (b) Please see related checkpoint C(269), C(291) and C(292) of **Appendix 1** to the manual.	✓		
C(365)	***Where*** B/Ds have developed their departmental recordkeeping metadata standards which may include additional entities, metadata elements and values and/or encoding schemes in addition to those specified in RKMS, test whether the ERKS is flexible and scalable to cater for B/D-specific metadata requirements on entities, recordkeeping metadata and/or encoding schemes in addition to those specified in RKMS. Test whether those **B/D-specific entities, metadata elements and values, entities and/or encoding schemes built in the ERKS** comply with the following - (a) B/D-specific metadata elements should fall within the six categories of metadata elements as defined in **section 2.4** of RKMS; (b) properties of B/D-specific metadata elements should be defined in accordance with the metadata element definition table set out in	✓		

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	Table 6 of **section 4.7** including the obligation level of metadata elements as specified in **section 4.6** of RKMS; (c) B/D-specific encoding schemes should be defined in accordance with the principles set out in **paragraphs 6.6.50 to 6.6.57** of RKMS and properties defined in accordance with **paragraph 4.9.1** of RKMS; and (d) the simple name, XML name and unique URI of B/D-specific metadata elements, encoding schemes and entities should be defined in accordance with the naming and numbering conventions as specified in **sections 4.2 to 4.4** of RKMS. (See **sections 2.4**, **4.2 to 4.4**, **4.6**, **4.7**, **4.9** and **6.6** of RKMS for details.) **Points to note**: (a) B/Ds should ensure that B/D-specific metadata elements and values, entities and/or encoding schemes built in the ERKS - (i) will not compromise the purposes of or be in conflict with the metadata elements, encoding schemes and entities specified in RKMS; (ii) will not jeopardise the authenticity, integrity, reliability and usability of records; (iii) comply with the relevant legal and regulatory requirements, government regulations and standards; and (iv) comply with the Government's records management policy and requirements and			

S/N	Checkpoint	Checkpoint pertaining to AP		
		AP1	AP3	AP4
	best records management principles. (b) In case there are discrepancies between RKMS and B/D's departmental recordkeeping metadata standard, requirements specified in RKMS should take precedence.			

Appendix 3

Evaluation of the implementation and enforcement of proper departmental records management policies, practices and procedures for effective management of records in an electronic recordkeeping system

Part I - Overview

This appendix provides guidelines for bureaux and departments (B/Ds) to conduct a **self-assessment**[1] to evaluate the implementation and enforcement of proper departmental records management (RM) policies, practices and procedures for effective management of records in an electronic recordkeeping system (ERKS).

2. A **checklist**, with a total of **68** checkpoints, is provided at **Part II** to assist B/Ds in evaluating their performance and effectiveness in developing, establishing and implementing departmental RM policies, practices and procedures as well as performing RM functions, processes and activities in an ERKS. The evaluation includes the following key aspects -

Section A	Departmental RM policies and responsibilities
Section B	Records capture and registration
Section C	Records classification and organisation
Section D	Records storage
Section E	Security and access control of records
Section F	Records tracking
Section G	Records retention and disposal
Section H	Vital records protection
Section I	Monitoring and auditing
Section J	Training
Section K	System management
Section L	System back-up and recovery
Section M	System maintenance
Optional	
Section N	Scanning procedures and processes[2]

[1] This is a specific self-assessment focusing on implementation and enforcement of departmental policies etc. **for effective management of records in an ERKS**, and is different from other self-assessment reviews which may be initiated by GRS.

[2] Where B/Ds adopts scanning to convert non-electronic records into digitised records for management and

Section O	Use of third party services[3]

3. B/Ds may add other issues in the checklist if deemed necessary having regard to their specific business, operational and RM needs. Upon completion of the self-assessment, B/Ds should rate their performance in implementation and enforcement of departmental RM policies, practices and procedures for effective management of records in an ERKS in accordance with the performance indicators prescribed in paragraph 2.21 of **Chapter 2** and document recommendations and suggested improvements in **Part III** of this appendix to take timely follow-up actions.

Part II - Checklist

4. Readers are requested to note that -

(a) all checkpoints set out in **Part II** have been designed to the effect that responses to those checkpoints where applicable are expected to be in the affirmative so as to demonstrate that the B/D concerned has adhered to the best RM practices in the specific areas. In general, the more responses to the checkpoints fall in the expected category (i.e. affirmative), the higher the confidence of the B/D should be able to satisfy itself that it fares well in respect of implementing and enforcing departmental RM policies, practices and procedures for compliance with the Government's RM policies and requirements;

(b) "**the ERKS**" in the following table refers to the ERKS being tested and evaluated; and

(c) "**N/A**" denotes "**not applicable**". B/Ds should explain the reason for non-applicability of individual checkpoint.

storage in an ERKS, they should assess the issues set out in **section N**.

[3] Where B/Ds outsource RM services e.g. scanning of paper records pertaining to an ERKS to a third party, they should assess the issues set out in **section O**.

A.	Departmental RM policies and responsibilities				
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
1.	Has my B/D developed and established departmental RM policies?				
2.	Have the departmental RM policies defined clearly and adequately the roles and responsibilities (including RM staff, records users and IT staff) and the interrelationship of the staff who use, perform and manage RM functions, activities and processes in the ERKS?				
3.	Have the departmental RM policies been properly authorised, documented and promulgated to staff members?				
4.	Have adequate RM practices, procedures and guidelines **been established** for compliance and reference by staff to use, manage and maintain the ERKS so as to ensure the authenticity, integrity, reliability and usability of records managed by the ERKS. [**Note**: The guidelines, practices and procedures should include but are not limited to the following: • what, when and how records and recordkeeping metadata should be created and captured (please read S/N 9 in conjunction with this one); • roles and responsibilities for creating, capturing, managing and maintaining records, aggregations and recordkeeping				

A.	Departmental RM policies and responsibilities				
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
	metadata in the ERKS; • how to ensure that records and recordkeeping metadata are properly created, captured, kept and maintained; • who, when and how to determine, apply, revise and review the access rights and security of records, aggregations, recordkeeping metadata and audit trail data; • who, when and how to approve adoption of a new records classification scheme(s) and revision to the existing records classification scheme(s); • who, when and how to create classes, sub-classes, folders and parts in the records classification scheme(s) of the ERKS; • rules and guidelines for organising records classification scheme(s), assigning titles and classification codes for classes, sub-classes, folders and parts; • rules and guidelines for titling records; • who, when and how to establish, revise and review records retention and disposal schedules; • who, when and how to endorse disposal of records; • who, when and how to perform disposal of records; and • who, when and how to identify, select and				

A.	Departmental RM policies and responsibilities				
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
	protect vital records.]				
5.	Have the RM roles and responsibilities to use, manage and maintain the ERKS been assigned to staff of appropriate level and skills (e.g. the system administrator should possess the technical skills and knowledge in managing the ERKS)?				
6.	Has segregation of roles and responsibilities been implemented to perform RM functions, activities and processes in the ERKS?				
7.	Have the roles and responsibilities, guidelines, practices and procedures underpinning the use, management and maintenance of the ERKS (including those set out in S/N 2, 4, 5 and 6 above) and subsequent revisions to them been **properly documented**?				
8.	Have appropriate actions been taken to manage legacy filing systems such as a paper-based recordkeeping system to ensure that records stored therein are authentic, complete, secure and usable for as long as required? [**Note**: In case a B/D chooses to keep legacy filing systems for use, this question must be answered.]				

B.	Records capture and registration				
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
9.	Has my B/D issued guidelines, practices and procedures on the creation, and capture of those records including electronic records that are necessary to meet operational, fiscal, legal and other requirements? The guidelines and procedures should include, but are not limited to, the following - • what records should be created; • who and when to create a record; • who and when to capture a record; • which system to capture the records into; • what recordkeeping metadata should be created for these records; and • who should have access to these records and the security of the records.				
10.	Have records users, particularly subject officers, been assigned responsibility to create and collect adequate but not excessive records to meet operational, policy, legal and financial purposes in the day-to-day business processes?				

C.	Records classification and organisation				
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
11.	Has a records classification scheme(s) which cover all records irrespective of nature or formats managed by the ERKS been developed and implemented?				
12.	Is the records classification scheme(s) established in the ERKS - • systematic, logical, consistent and scalable to facilitate accurate and complete documentation of policies, procedures and decisions for the efficient carrying out of the organisational functions, activities and transactions; • supporting accurate capturing into and easy retrieval of records from the ERKS; • facilitating establishment of robust security and access control to records managed by the ERKS; • facilitating segregation of vital records for protection; and • facilitating establishment of records retention and disposal schedules and segregation of records with different retention periods to support timely and effective disposal?				

D.	Records storage				
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
13.	Is the hardware, e.g. servers of the ERKS, stored in a safe and secure environment in accordance with the Government's and departmental IT security policy, guidelines and practices? Is it secure against unauthorised access and hazards such as fire and flooding? [**Note**: As with other information systems, an ERKS has to meet certain security regulations/requirements, and circulars and guidelines issued by the Government Chief Information Officer to process and store classified information, e.g. requirements on storage of classified information.]				
14.	Are facilities (e.g. hardware, software, etc. used in ERKS for transferring records) and procedures, e.g. data verification, available to ensure the integrity of records when records are transferred to and from storage including transfer of electronic records from one storage medium to another one?				
15.	Have proper procedures been established and adopted to demonstrate that stored records have not been changed (either accidentally or maliciously), or where changes have occurred, they have been authorised during storage?				
16.	Where records are compressed during the storage process, do the compression methods used not affect the authenticity and integrity				

D.	Records storage				
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
	they have been authorised during storage?				
16.	Where records are compressed during the storage process, do the compression methods used not affect the authenticity and integrity of the stored records in the ERKS or in electronic storage media for off-line storage?				
17.	Have proper procedures been established and adopted to test and take appropriate follow-up action on storage media at regular intervals to reduce to an acceptable level the risk of records becoming unrecoverable?				

D.	Records storage				
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
E.	**Security and access control of records**				
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
18.	Does my B/D manage access to records according to the legal and regulatory requirements, e.g. Personal Data (Privacy) Ordinance?				
19.	Have adequate security measures been put in place to protect records from unauthorised access and to prevent unauthorised and accidental loss or destruction of records managed by the ERKS?				
20.	Has the ERKS passed the recent security risk assessment and audit?				
21.	Have recommendations on security measures identified by the recent security risk assessment and audit been implemented?				
22.	Have procedures been established for dealing with actual, suspected and potential security breaches?				
23.	Are there appropriate and sufficient procedures to ensure that audit trail data are - • authentic; • understandable (the audit trail data				

D.	Records storage				
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
	provides meaningful and adequate information for officers to interpret the data); and • available as required.				
24.	Are authorised personnel able to access audit trail data?				

D.	Records storage				
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
F.	**Records tracking**				
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
25.	Are there arrangements to minimise the risk of losing records managed by the ERKS?				
26.	Have effective measures been adopted to track the physical movement of hybrid aggregations and non-electronic records managed by the ERKS?				

G.	Records retention and disposal				
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
27.	Have records retention and disposal schedules been established for all its records managed by the ERKS? Have the retention and disposal requirements been linked with the records classification scheme(s) so as to facilitate efficient and effective disposal of records at the end of the life cycle of records?				
28.	Are there guidelines which prescribe uniform records disposal procedures and consistent records disposal action to be carried out through the ERKS?				
29.	Have safeguards been instituted against unauthorised destruction of records managed by the ERKS?				
30.	Have practices and procedures been put in place for the destruction of time-expired electronic records and physical destruction of time-expired non-electronic records managed by the ERKS to avoid inadvertent destruction and leakage of sensitive information?				

G.	Records retention and disposal				
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
31.	Has the endorsement of an officer not below the rank of Senior Executive Officer or equivalent been obtained for destruction of time-expired records in accordance with approved records retention and disposal schedules? [**Note**: B/Ds may consider defining a workflow in the ERKS to standardise the procedures to seek approval for destruction of time-expired records in accordance with approved records retention and disposal schedules.]				
32.	Has the GRS Director's prior agreement been obtained before destruction of time-expired records in accordance with approved records retention and disposal schedules?				
33.	Has regular review (e.g. at least once every two years) been conducted to systematically and consistently dispose of time-expired records managed by the ERKS according to approved records retention and disposal schedules?				

H.	Vital records protection				
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
34.	Have proper practices, procedures and guidelines been developed and established to identify and select vital records managed by the ERKS?				
35.	Have proper protective measures/methods, e.g. copies of vital records are stored outside the primary office site, been adopted or implemented to protect vital records managed by the ERKS?				

I.	Monitoring and auditing				
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
36.	Does my B/D conduct regular reviews on departmental RM policies and responsibilities, recordkeeping system and RM guidelines and procedures to cater for changing legal and regulatory, business, operational and RM requirements?				
37.	Does my B/D continuously monitor the compliance with established RM guidelines, practices and procedures to use, manage and maintain the ERKS?				
38.	Does my B/D identify areas requiring improvement through regular review of RM practices of sections/units and exception cases (e.g. loss or unauthorised destruction of records)?				

J.	Training				
S/N	Checkpoint	Assessment (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
39.	Have the IT and RM staff members at different levels who are responsible for operating and managing the ERKS been equipped with the necessary RM and IT concepts, principles and practices to manage the ERKS?				
40.	Is RM and ERKS training provided for records users?				
41.	Is RM and ERKS training provided for new staff as part of their induction programme?				
42.	Are refresher courses on RM provided for serving staff regularly or as and when necessary (such as after the upgrading/system enhancement of the ERKS)?				

K.	System management				
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
43.	Has sufficient documentation been established and made available covering the following aspects of the ERKS to manage and store records - • roles and responsibilities for undertaking system management; • system manual (a description of the key hardware and software components of the system); • system maintenance and monitoring; • operation and procedural manuals detailing the procedures to be followed relating to the ERKS; and • preventive and corrective actions of system malfunctioning?				
44.	Has complete and up-to-date system documentation been maintained for the ERKS?				
45.	Is the system administered by people who are trained and competent in its application to ensure that records are adequately managed over time?				
46.	Have adequate measures (e.g. media migration) been put in place to ensure the accessibility and usability of electronic records stored in the ERKS over time?				

L.	System back-up and recovery				
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
47.	(a) Is there regular back-up of records managed by the ERKS?				
	(b) Are there procedures for the back-up and verification of records and associated information in the ERKS (e.g. metadata)? Are these procedures adequately documented?				
48.	(a) Are there procedures to check that the integrity of records is not compromised as a result of a restore activity following a system failure?				
	(b) Are the procedures mentioned in (a) above adequately documented?				
49.	Are backup media maintained to a level of security (e.g. whether the backup media stored in a safe and secure manner) that ensures the authenticity of the records used in recovery situations?				
50.	Are backup media tested at regular intervals to ensure readability?				
51.	Have a business continuity plan been put in place to ensure the recovery of records and the maintenance of the integrity of records in the system, during and after an incident or a disaster?				

L.	System back-up and recovery				
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
M.	**System maintenance**				
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
52.	Is preventive maintenance of the system carried out?				
53.	Is a system maintenance log kept, which details completed preventive and corrective maintenance?				
54.	Where system access controls can be bypassed during maintenance of hardware and/or software, is personnel performing such processes strictly controlled, monitored and audited?				
55.	Have there been measures in place to ensure that records will remain authentic, unaltered, retrievable and usable in the event of system change, computer upgrades or change of software or hardware vendors?				

Optional

N. Scanning procedures and processes [**Note**: If a B/D converts non-electronic records into a digital form through scanning and keep the digitised records in the ERKS, the B/D concerned should assess the following issues relating to scanning procedures and processes.]					
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
56.	Have technical standards of scanning, including those set out below, been implemented and documented with particular reference to the need to ensure the authenticity, integrity and reliability as evidence in a court of law in respect of the specific business concerned - • file formats; • compression; • resolution; • bit depth; • forbidding or avoiding image processing, e.g. speckle (random black marks) removal and de-skewing to correct poor document alignment (rotation); • colour management; and • metadata? [**Note**: Image processing techniques can be used to improve the quality of an image. However, their use should be carefully controlled and documented, as they can affect the evidential weight of the stored images				

N. Scanning procedures and processes [**Note**: If a B/D converts non-electronic records into a digital form through scanning and keep the digitised records in the ERKS, the B/D concerned should assess the following issues relating to scanning procedures and processes.]					
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
	(Clause 6.2.5 of ISO/TR 13028:2010(E) - Information and documentation - Implementation guidelines for digitization of records.)]				
57.	Is the performance of the equipment and software used for scanning records in a manner or quality acceptable to the business need? [**Note**: For example, if the quality of the colour on a document is critical, the quality of the equipment used to render the image needs to support the capacity to retrieve and analyse this quality. If, on the other hand, it is only essential to be able to read the contents to gain the sense of the text, the quality of display could be appropriately less critical.]				
58.	Have the scanning procedures and processes and technical standards been reviewed and revised regularly and as and when required?				
59.	Have appropriate and auditable scanning procedures and processes been put in place to ensure that all the necessary information of records have been scanned and captured as accurately as possible?				

N. Scanning procedures and processes [**Note**: If a B/D converts non-electronic records into a digital form through scanning and keep the digitised records in the ERKS, the B/D concerned should assess the following issues relating to scanning procedures and processes.]					
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
60.	Have appropriate and adequate quality control procedures and measures, e.g. criteria for checking image quality, been established and adopted to check for missing images and/or images that do not meet the specified quality standards before the digitised records are captured into the ERKS?				
61.	Have the procedures and results of quality assurance processes been documented?				
62.	Have the quality control procedures and measures been reviewed and revised regularly and as and when required?				
63.	Has any use of enhancement techniques on the digitised record been well documented? [**Note**: During the scanning process, the use of techniques that enhance the digitised image to make the image have a more exact resemblance to the original record should be documented. Such procedures may, if not undertaken in routine and documented ways, attract the challenge that the image is not an authentic copy of the original record. Such techniques include "de-speckling" and "spotting" to touch up specific areas of a digital image, "blurring" to eliminate scratches, etc.]				

N. Scanning procedures and processes [**Note**: If a B/D converts non-electronic records into a digital form through scanning and keep the digitised records in the ERKS, the B/D concerned should assess the following issues relating to scanning procedures and processes.]					
S/N	**Checkpoint**	**Assessment** (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
64.	Are errors and defects in the digitised records corrected?				
65.	Have rescanning procedures been established and adopted to correct any errors identified?				
66.	Has rescanning been properly documented?				

O. Use of third party services

[**Note**: If a B/D outsources a service relating to the capture, management, storage and maintenance of the ERKS such as using cloud-based ERKS services, to a service provider, the B/D concerned should assess whether it is able to demonstrate compliance with the Government's and departmental IT and RM policies, practices and procedures by way of outsourcing.]

S/N	Checkpoint	Assessment (please tick '✓' as appropriate)			
		Yes	No	Being developed/ established	N/A (with reason)
67.	Has the contract/arrangement with the service provider clearly set out the Government's IT and RM requirements and responsibilities for the service provider to comply with?				
68.	Have sufficient measures and control been put in place to ensure that the service provider complies with the committed service requirements?				

Part III - Recommendations

Section	Category	Proposed rectification and/or recommendations for improvement
Section A	Departmental RM policies and responsibilities	[Please set out the proposed follow-up actions and improvements.]
Section B	Records capture and registration	
Section C	Records classification and organisation	
Section D	Records storage	
Section E	Security and access control of records	
Section F	Records tracking	
Section G	Records retention and disposal	
Section H	Vital records protection	
Section I	Monitoring and auditing	
Section J	Training	
Section K	System management	
Section L	System back-up and recovery	
Section M	System maintenance	
Optional		
Section N	Scanning procedures and processes	
Section O	Use of third party services	

Appendix 4

A sample test plan of an ERKS

1) Amendment history

Date	Version	Amendment description

[This section should list major changes made to the test plan.]

2) Objectives of the testing

[This section should describe the objectives of testing an ERKS including assessing the compliance of an ERKS with the ***Functional Requirements of an Electronic Recordkeeping System*** and the ***Recordkeeping Metadata Standard for the Government of the Hong Kong Special Administrative Region***.]

3) Description of the ERKS

[This section should describe the ERKS to be tested, including its major functionality and business operations/functions that it is intended to support. This section should also clearly indicate whether the ERKS is developed from scratch or a commercial off-the-shelf solution with certain degree of system configuration and/or customisation built in. Please also describe whether the ERKS is a part/module of an integrated electronic information management (EIM) solution or the ERKS is a stand-alone system.]

4) Scope of testing

[This section should define the scope of tests such as functional test, load test and system integration test. It should also clearly set out what ERKS functionality will be tested and what will not be tested. For example, if a B/D does not implement functionality relating to multiple repositories as prescribed in Requirement 7 of the ***Functional Requirements of an Electronic Recordkeeping System***, such requirement will not be tested and that should be clearly indicated in this section.]

5) Resources required

[This section should outline the resources required including manpower to conduct the testing.]

6) Evaluation criteria

[This section should define the evaluation criteria that will be adopted to assess the acceptance of the ERKS. For example, the ERKS must pass the security risk assessment and audit conducted by an independent third party. If any standards and reference materials have been made reference to, they should also be listed.]

7) Assumptions and limitations

[This section should describe whether there are any assumptions and limitations of the test. For example, the load test has assumed that a total of 500 officers will concurrently use the ERKS at one time.]

8) Test schedule and responsible parties

[This section should outline the scheduled duration, commencement and completion dates of the test and the sequence of the testing. It should also clearly set out which parties concerned are responsible for developing and approving the test specifications including test cases, test procedures and test data; conducting the testing; re-testing and approving the test results, etc.]

9) Test documentation

[This section should provide templates to document test progress and test summary report.]

10) Other documentation

[This section should list other relevant documentation, e.g. reference materials that should be made reference to when conducting the testing of the ERKS, e.g. Security Regulations.]

-End-

Appendix 5

A sample evaluation plan of departmental RM policies, practices and procedures

1) Amendment history

Date	Version	Amendment description

[This section should list major changes made to the evaluation plan.]

2) Objectives of the evaluation

[This section should describe the objectives of the evaluation including assessing the compliance of the departmental RM policies, practices and procedures with the Government's RM policy, mandatory RM requirements as specified in GCs and CMs relating to RM notably GC Nos. 5/2006 and 2/2009 and Administration Wing CM on Establishment of Departmental Records Management Policies issued on 11 July 2012, ERM requirements and best practices.]

3) Description of departmental RM policies, practices and procedures

[This section should briefly describe the departmental RM policies, practices and procedures that have been in place governing the use, management and maintenance of an ERKS and the delineation of roles and responsibilities for using and managing the ERKS.]

4) Scope of evaluation

[This section should define the scope of the evaluation. B/Ds should ensure that RM issues specified at **Appendix 3** to the ***Manual on Evaluation of an Electronic Recordkeeping System*** should be thoroughly assessed.]

5) Evaluation methodology

[This section should set out the methodology, e.g. surveys, interviews,

documentation review and on-site inspections to be adopted to evaluate the effectiveness of implementation and enforcement of departmental RM policies, practices and procedures.]

6) Resources required

[This section should outline the resources required including manpower to conduct the evaluation.]

7) Assumptions and limitations

[This section should describe whether there are any assumptions and limitations of the evaluation.]

8) Evaluation schedule and responsible parties

[This section should outline the scheduled duration, commencement and completion dates of the evaluation. It should also clearly set out who/which parties are responsible for planning, conducting and endorsing the evaluation plan and evaluation results.]

9) Evaluation documentation

[This section should provide templates if available to document findings of the evaluation.]

10) Problem tracking and reporting

[This section should set out practices and procedures to report problems/issues that warrant special attention and ways to tackle the problems. The procedures of reporting should also be defined.]

11) Other documentation

[This section lists other relevant documentation, e.g. reference materials that should be made reference to when conducting the evaluation, e.g. departmental RM policy statement.]

-End-

Appendix 6 (a)

Sample test case 1

Category of Functional Requirement	**Records Classification and Identification**	
Unique Case No.:	2.1	
Test case description:	To test whether an ERKS is able to support the establishment of a records classification scheme for at least **five levels.**	
Related Requirement:	*Requirement 2 of FR of ERKS (related to part of the requirement highlighted in bold)* **Support a pre-defined records classification scheme in a hierarchical structure with at least five levels (down to folder level) below the root of the records classification scheme** and support the definition and simultaneous use of multiple records classification schemes in the ERKS.	
Pre-condition:	1. Login ERKS as a user with the administrator role.	
Suggested step(s):	*Action to be performed*	*Expected Result*
	1. Create a new class **Demo_Administration**.	1. The class **Demo_Administration** is created.
	2. Create a 1st tier sub-class **Demo_Personnel** under the class **Demo_Administration**.	2. The 1st tier sub-class **Demo_Personnel** is created.
	3. Create a 2nd tier sub-class **Demo_Training** under the 1st tier sub-class **Demo_Personnel**.	3. The 2nd tier sub-class **Demo_Training** is created.
	4. Create a 3rd tier sub-class **Demo_ABC Grade** under the 2nd tier sub-class **Demo_Training**.	4. The 3rd tier sub-class **Demo_ABC Grade** is created.
	5. Create an *electronic* folder **Demo_CSTDI Training** under the 3rd tier sub-class **Demo_ABC Grade**.	5. The *electronic* folder **Demo_CSTDI Training** is created.
Remarks:	To be conducted in conjunction with Case Nos. 1.1 (classification and organisation of records), 3.1.1 (initial and on-going construction of classification scheme), 4.2 (assign a classification code and allocate a textual title of aggregation) and 5.1 (Step 1 - creation of *electronic* folder).	
Test result:	☐ Passed	

(please tick "✓")	☐ Failed (Please specify steps failed:_____) ☐ Not tested (Please specify reason: _____)
Comment:	
Test completed by:	[please provide the name and post of the officer]
Date of the test:	

Appendix 6 (b)

Sample test case 2

Category of Functional Requirement	**Use of Records**	
Unique case no.	26.1	
Test case description:	To test whether an ERKS is able to support search of records and sub-classes by using different methods and support search of records containing multiple languages.	
Related requirement:	Requirement 26(a) of FR of ERKS - **Support efficient searches, including but not limited to, full text, wild card and Boolean searches on one or a combination of any of the metadata elements and on the contents (where they exist) of records in an integrated and consistent manner.** Requirement 26(b) of FR of ERKS - **Support efficient searches of records containing multiple languages including at least Traditional Chinese, Simplified Chinese and English.**	
Pre-condition:	1. The **ClassificationScheme1** has been created in Case No. 2.1. 2. The **ClassificationScheme2** has been created in Case No. 2.2. 3. The electronic record **Record1** has been captured in the *electronic* folder **Common Look and Feel - Websites and Portals** in Case No. 2.2. 4. The *electronic* folder **Demo 資料夾名称** has been created under the sub-class **Demo_Training** in Case No. 50.1**.** 5. The electronic record **Language 试点單位** has been captured in the *electronic* folder **Demo 資料夾名称** in Case No. 50.1. 6. Login the ERKS as a records user who has access right to the specified sub-classes and records of the **ClassificationScheme1** and **ClassificationScheme2**.	
Suggested step(s):	*Action to be performed*	*Expected Result*
	1. Search for the electronic record **Record1** by using the keyword "**Common Look and Feel**" and the metadata element "date created" for the date falling within the period	1. The ERKS should be able to locate the specified record.

Category of Functional Requirement	Use of Records	
	from **July to August 2010**.	
	2. Search for sub-classes with the title starting with the English characters "**Demo"** by using wild card search. Limit the scope of search at the sub-class level.	2. The ERKS should be able to return search results containing sub-classes with the title starting with the English characters **"Demo"**. They are: • **Demo_ABC Grade** • **Demo_Common Grades** • **Demo_Consultancy Study** • **Demo_Personnel** • **Demo_Training (PRM-002)** • **Demo_Training (ADM-005-095)**
	3. Search for records containing the keywords - "**Sham Shui Po District"**, "深水埗區**"** and "深水埗区**".** Limit the scope of search at the record level.	3. The ERKS should be able to locate record(s) with such keywords including the one **Language** 试点單位**..**
Remarks:	To be conducted in conjunction with Case No. 24.1 (define search scope).	
Test result: **(please tick "✓")**	☐ Passed ☐ Failed (Please specify steps failed:_____) ☐ Not tested (Please specify reason: _____)	
Comment:		
Test completed by:	[please provide the name and post of the officer]	
Date of the test:		

Appendix 6 (c)

Test case template

Category of Functional Requirement		
Unique case no.:		
Test case description:		
Related requirement:		
Pre-condition:		
Suggested step(s):	*Action to be performed*	*Expected Result*
	1.	…
	2.	…
	…	…
	…	…
	…	…
Remarks:		
Test result: **(please tick "✓")**	☐ Passed ☐ Failed (Please specify steps failed:_____) ☐ Not tested (Please specify reason: _____)	
Comment:		
Test completed by:	[please provide the name and post of the officer]	
Date of the test:		

Blank page

Appendix 7

A sample compliance assessment report

1) Executive summary

[This section should summarise the major findings of the assessment and propose the way forward.]

2) Purpose

[This section should set out the purposes of the assessment report.]

3) Objectives of evaluation

[This section should describe the objectives of the compliance assessment including assessing the compliance of an ERKS with the ***Functional Requirements of an Electronic Recordkeeping System*** and the ***Recordkeeping Metadata Standard for the Government of the Hong Kong Special Administrative Region***; and the effectiveness of departmental RM policies, practices and procedures governing the use, management and maintenance of an ERKS for proper management of records.]

4) Scope of evaluation

[This section should describe the functionality of the ERKS being evaluated, the technical and non-functional requirements of the system to be assessed, and departmental RM policies, practices and practices governing the use, management and maintenance of the ERKS.]

5) Schedule of evaluation

[This section should list the commencement and completion dates of the compliance assessment.]

6) Evaluation plans

[This section should briefly describe the test plan and the evaluation plan as

prescribed in paragraph 3.2 of the ***Manual on Evaluation of an Electronic Recordkeeping System*** and attach a copy of the plans for reference by the approving officer.]

7) Parties responsible for the evaluation

[This section should report on the officers responsible for planning and conducting the evaluations.]

8) Key findings of evaluation

[This section should report on the key findings of the evaluation and recommend the ratings of the ERKS and the departmental RM policies, practices and procedures as specified in paragraphs 2.18 and 2.21 of the ***Manual on Evaluation of an Electronic Recordkeeping System***. It should also report on any issue that warrants the attention of the approving officer. The duly completed checklist at **Appendix 3** to the ***Manual on Evaluation of an Electronic Recordkeeping System*** should be attached for reference by the approving officer.]

9) Comments and views of key stakeholders

[This section should document views and comments provided by key stakeholders such as DRM and Head of ITMU about the report, findings and recommendations of the compliance assessment.]

10) Recommendations and way forward

[This section should propose the way forward, e.g. whether approval should be sought from GRS to dispense with print-and-file practice and actions to be taken such as system improvements having regard to the findings of the assessment.]

11) Endorsement sought

[This section should seek approval for the results and findings of the compliance assessment and recommendations.]

-End-

Appendix 8

Request form for dispensing with the print-and-file practice

I. General information

1. Name of Bureau/Department (B/D):
2. Proposed effective date to dispense with the print-and-file practice:
3. Such request is applicable to (please give a tick "✓" as appropriate): □ the whole organisation □ only to _____ [division/branch/office]

II. Information about the electronic recordkeeping system (ERKS)

4. Date of system acceptance of the ERKS:	5. No. of existing users:
6. Please choose one of the following by giving a tick "✓": □ The ERKS has been developed by my B/D. □ The ERKS has been acquired with certain degree of system configuration and/or customisation built in. □ The ERKS has been adopted (e.g. using cloud-based common ERKS services) □ Others (please specify)_____	
7. Has the ERKS satisfactorily passed the security risk assessment and audit (SRAA)? Please choose one of the following by giving a tick "✓": □ Yes (Year of the SRAA conducted: _____) □ No (Please give reason: _____) □ Not applicable (Please give reason: _____)	
8. Please choose one of the following compliance ratings for the ERKS by giving a tick "✓": □ Full compliance □ Moderate compliance requiring improvement □ Low to non-compliance [Note: Please see **Chapter 2** of the ***Manual on Evaluation of an Electronic Recordkeeping System*** for the performance indicators of each rating.]	

III. Departmental RM policies, practices and procedures

9. Please choose one of the following evaluation ratings in respect of departmental RM policies, practices and procedures by giving a tick "✓":
   - □ Good
   - □ Fair
   - □ Unsatisfactory

   [Note: Please see **Chapter 2** of ***Manual on Evaluation of an Electronic Recordkeeping System*** for the performance indicators of each rating.]

IV. Supporting documentation

10. Please give a tick "✓" if the following supporting documentation is provided:
    [Note: The following documentation must be provided to support a request.]
    - □ A copy of system manual documenting the system functionality of an ERKS
    - □ A copy of application user manual which should include both user and administrator functions of an ERKS
    - □ A copy of finalised test plan, test specifications including test cases, test procedures and test data
    - □ A copy of the compliance assessment report documenting the results and recommendations of the evaluation
    - □ A copy of departmental RM policies, practices and procedures underpinning the use, management and maintenance of an ERKS
    - □ Any other relevant documentation warranting the attention of GRS but has not been included above (please provide a copy of the documentation)

V. Remark

11. Please advise any other relevant considerations warranting the attention of GRS but have not been included in parts I to IV.

VI. Contact Person

12. Name of Departmental Records Manager:
13. Date of submission:
14. E-mail address:
15. Office telephone no.: