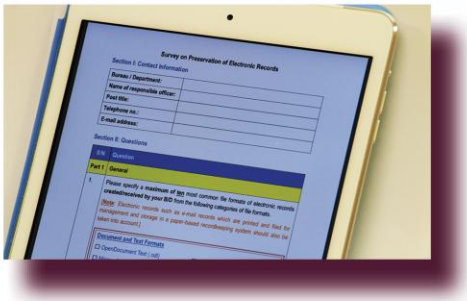
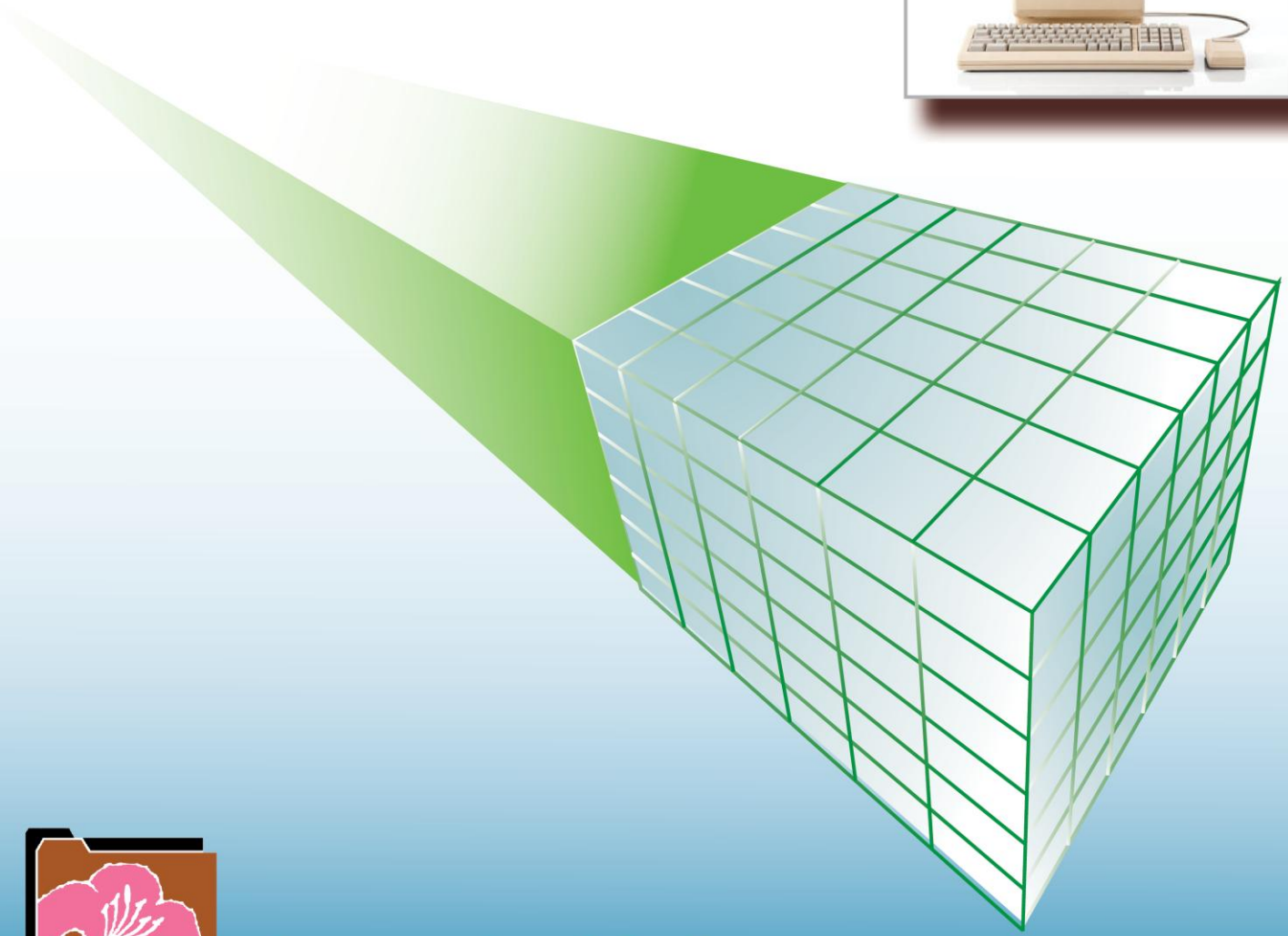
A Handbook on Preservation of Electronic Records





Government Records Service

A HANDBOOK ON PRESERVATION OF ELECTRONIC RECORDS

GOVERNMENT RECORDS SERVICE

JULY 2013

Blank page

Table of Contents

Blank page

Foreword

Records are valuable resources of the Government. They are required in every function and activity in bureaux and departments (B/Ds) and are the basis on which decisions are made, services provided and policies developed and communicated. Proper management of records is therefore an important common function of B/Ds to comply with legal and regulatory requirements, meet business and operational needs, and to demonstrate accountability.

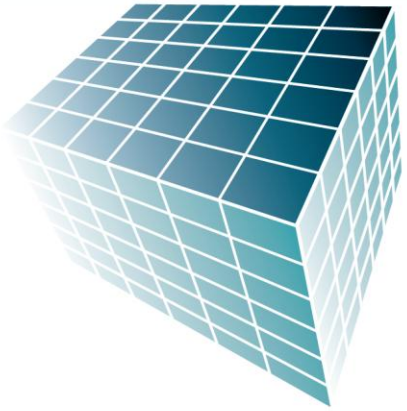
Use of electronic means to conduct business and deliver public services has become increasingly commonplace in B/Ds. Arising from such trend, more and more government records have been created and received in electronic form. Electronic records come in a wide variety of formats: audio recordings, databases, e-mails, images, spreadsheets, texts, etc. These large quantities of electronic records produced today and designed to be accessed on computers are at risk of becoming inaccessible, incomprehensible or lost to posterity in light of rapid technological changes and obsolescence, unless specific policies, strategies and techniques are developed and adopted timely to manage and preserve them for as long as they are required to serve legal, regulatory, business, operational, evidence and archival purposes.

To gauge the need for preservation of electronic records, and assess the measures and practices currently adopted by B/Ds to address the pertinent challenges on this subject, an inter-departmental task force led by the Government Records Service (GRS) with members from the Office of the Government Chief Information Officer (OGCIO) conducted a government-wide survey on preservation of electronic records in 2012. The findings of the survey have reflected that there is a clear business need for B/Ds to take proper measures and actions to preserve electronic records under their custody to minimise and mitigate risks of inaccessibility and unusability of electronic records in the long run.

Arising from the findings of the survey, it is considered necessary to enhance the awareness of proper preservation of electronic records and promote best practices in this regard to B/Ds, particularly records management staff and staff of Information Technology Management Units. Against this background, this handbook has been developed by GRS. Special thanks must go to the colleagues of OGCIO who have made valuable contributions to the preparation of this handbook from the technical perspective.

GRS is now pleased to promulgate ***A Handbook on Preservation of Electronic Records*** for reference by B/Ds.

Blank page



CHAPTER 1

Introduction

Has your B/D taken sufficient and proper actions to ensure that electronic records can be found, opened, worked with, understood and trusted in the way that records users need, for as long as they are required?

Chapter 1
Introduction

Purpose

1.1 This handbook provides guidelines for B/Ds to establish and implement a departmental preservation programme; and to adopt proper measures and practices to preserve their electronic records to meet legal and regulatory requirements, business and operational needs and evidence purpose.

Scope

1.2 This handbook focuses primarily on **preservation of electronic records** created, received and managed [1] by B/Ds in the following computing environments–

(a) in an **unstructured** computing environment under which–

(i) business processes and workflow are not well-defined;

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

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

(b) in a **structured** computing environment[2] under which–

(i) business processes are typically highly structured;

(ii) well-established tools and techniques are employed to develop applications and information systems supporting the processes; and

(iii) accountability for the design, development and maintenance of information systems (including the integrity of the data generated in the information systems) has been assigned.

1.3 Preservation of non-electronic records[3] in B/Ds and archival records in

[1] B/Ds are responsible for preserving their electronic records irrespective of whether the management and storage of those records are undertaken by themselves direct or by a third party such as a service provider providing records management services to the B/D concerned.

[2] Examples of records created in a structured computing environment include leave records stored in Electronic Leave Application and Processing System (e-LAPS) or funding applications stored in the Electronic Administrative Computer Projects Committee (e-ACPC) System.

[3] For assistance in preservation of non-electronic records, B/Ds may seek advice from the Preservation Service Office of GRS.

electronic form transferred to the Public Records Office (PRO) of GRS for permanent retention fall beyond the scope of this handbook.

1.4 Readers are requested to note that this handbook is not intended to be developed as a set of "how-to-do" guidelines. Instead of attempting to specify in detail what actions and practices need to be and how they should be implemented, this handbook aims to provide a starting point for enhancing awareness of preservation of electronic records; and to advise a set of technology-independent principles and general good practices in this regard. The main advantage in taking this approach is to ensure that this handbook should outlive any particular technology, and thus will be of value when following generations of software, storage and other devices come into play in future.

Key terminology

1.5 E-government initiatives and the wide adoption of information systems including business systems and desktop computers have resulted in exponential growth of electronic records in B/Ds. In the context of this handbook, **electronic records** refer to records generated in digital form by an information system, which can be (a) transmitted within an information system or from one information system to another, and (b) stored in an information system or other medium[4].

1.6 **Preservation of electronic records** encompasses a broad range of activities designed to maintain the authenticity[5], integrity[6], reliability[7] of records; and extend the usability[8] of electronic records by protecting them from technology obsolescence, media failure, physical loss, etc.

1.7 When important concepts and principles associated with preservation of electronic records are discussed in this handbook, their definitions are provided as appropriate. Readers are also directed to the glossary of key records management (RM) terms on GRS' dedicated electronic records

[4] Section 2, Electronic Transactions Ordinance (Cap. 553). Electronic records created in common office applications such as Microsoft Word 2010 fall within the scope of electronic records as described in this handbook.

[5] An authentic record is one that can be proven (a) to be what it purports to be; (b) to have been created or sent by the person purported to have created or sent it; and (c) to have been created or sent at the time purported.

[6] The integrity of a record refers to its being complete and unaltered.

[7] A reliable record is one whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.

[8] A usable record is one that can be located, retrieved, presented and interpreted. It should be capable of subsequent presentation as directly connected to the business activity or transaction that produced it.

management (ERM) web page hosted on the Government's intranet, Central Cyber Government Office (CCGO) http://grs.host.ccgo.hksarg/erm/s11/11.html for more information on various RM concepts and terms used in this handbook.

Audience

1.8 This handbook is primarily intended for use by–

(a) Departmental Records Managers (DRMs) who are responsible for, among others, overseeing the departmental RM programme of B/Ds;

(b) Records managers and other RM staff assisting DRMs in planning and executing day-to-day management of records;

(c) Heads of Information Technology Management Units (ITMUs) and other IT staff of B/Ds who are responsible for planning, developing and administering IT systems in B/Ds; and

(d) system developers and consultants who assist B/Ds in developing, managing and administering IT systems to manage and store records and provide consultancy services to B/Ds on RM matters.

Structure of the handbook

1.9 Other than this chapter, this handbook is organised into four chapters as follows–

Chapter 2:	Need for Proper Preservation of Electronic Records
Chapter 3:	Roles and Responsibilities for Preserving Electronic Records
Chapter 4:	Establishment and Implementation of a Departmental Preservation Programme
Chapter 5:	Good Practices for Preserving Electronic Records

Further information

1.10 Enquiries arising from this handbook should be addressed to the following officers in GRS and OGCIO respectively–

General preservation, archival administration and RM matters

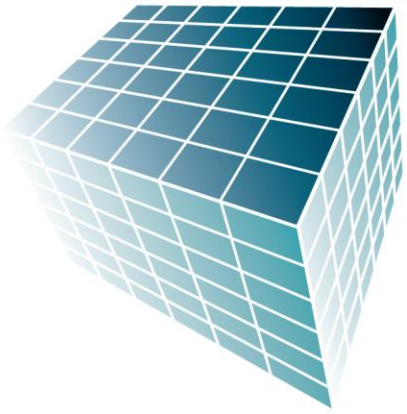
Government Records Service
Preservation Service Office
Post title: Curator (Preservation Service) Tel: 2195 7808 Lotus Notes e-mail: PSO/GRS/HKSARG Internet e-mail: psoinfo@grs.gov.hk
Public Records Office
Post title: Senior Assistant Archivist (Public Records)3 Tel: 2195 7774 Lotus Notes e-mail: PRO/GRS/HKSARG Internet e-mail: proinfo@grs.gov.hk
Record Systems Development Office
Post title: Senior Executive Officer (Record Systems Development)2 Tel: 2195 7792 Notes e-mail: RSDO/GRS/HKSARG Internet e-mail: rsdoinfo@grs.gov.hk

Information technology (IT) matters

Office of the Government Chief Information Officer
Business Transformation Division
Post title: Senior Systems Manager (Business Transformation)7 Tel: 2961 8006 Notes e-mail: Jenny CY Woo/OGCIO/HKSARG Internet e-mail: jcywoo@ogcio.gov.hk Post title: Systems Analyst (Business Transformation)7D Tel: 2961 8265 Notes e-mail: Howard JM Roy/OGCIO/HKSARG Internet e-mail: hjmroy@ogcio.gov.hk

Electronic records must be properly managed and preserved to meet legal and regulatory requirements, business and operational needs and evidence purpose.

Blank page



CHAPTER 2

Need for Proper Preservation of Electronic Records

If electronic records are inaccessible, incomprehensible or lost because you haven't managed and preserved them properly, is your B/D able to operate legally, effectively, efficiently and demonstrate accountability?

Chapter 2

Need for Proper Preservation of Electronic Records

Introduction

2.1 This chapter examines the challenges of preserving electronic records over time and explains the importance of proper preservation of electronic records.

Electronic records and their characteristics

2.2 Government records are evidence of official business and the basis on which decisions are made, services provided and policies developed and communicated. They can either be non-electronic records, e.g. paper and microfilm records, or electronic records.

2.3 Electronic records are created in a wide variety of formats: audio recordings, databases, e-mails, images, multi-media presentations, spreadsheets, word-processed documents, etc. They may be born digital or they may have been converted into digital form from their original format through digitisation such as scanning; and communicated and transmitted electronically.

2.4 **Electronic records require specific hardware and software to ensure that they are accessible, retrievable and understandable by users**[9]. As such, they are **technology dependent** and require proactive actions to manage and preserve to ensure their authenticity, integrity, reliability and usability for as long as they are required to meet legal and regulatory requirements, business and operational needs and evidence purpose.

2.5 Electronic records must possess **content**[10], **context**[11] and **structure**[12] to be of value as evidence. This means that an electronic record–

[9] For example, some text documents are created or saved in a popular format, Microsoft Word (.doc or .docx since Microsoft Word 2007). In order to view Microsoft Word documents, a user needs access to multiple computer technologies: the appropriate software that can view Microsoft Word documents, the right operating system and the hardware and software to run the computer in the first place. As well, the user will need a way to connect the computer to the media on which the documents are stored, such as a computer's hard disk drive or a CD-ROM storage device.

[10] Information or idea the record contains.

[11] Information about the circumstances in which the record is created, transmitted, maintained and used (e.g. who created it, when, to whom was it sent, why).

(a) has information content that is, and continues to be, an accurate reflection of what occurred at a particular date and time;

(b) can be placed in context so that the circumstances of its creation and use can be understood in conjunction with its information content; and

(c) can be reconstructed electronically when required so that each component is brought together as a whole and presented in an intelligible way.

2.6 In light of the characteristics of electronic records specified in paragraphs 2.3, 2.4 and 2.5, the significant challenges of preserving electronic records are different from those of paper records[13]. B/Ds need to understand the nature of, and unique challenges associated with, the preservation of electronic records so that suitable and specific preservation measures and practices can be planned and implemented in their organisations.

Challenges of preserving electronic records

Has your B/D taken timely actions to preserve electronic records stored in obsolete computer systems or storage media?

2.7 Preserving electronic records over long periods presents a number of complex challenges including technology obsolescence, media fragility and possible physical damage to hardware and storage media. These challenges

[12] Physical and/or logical format of the record, and the way parts of the record related to each other (e.g. the structure of an e-mail record covers its header, body, attachments and corresponding reply).

[13] The principal obstacle to preservation of paper records is the physical decay of the records themselves. Paper records can become damaged through excessive handling and as a result of deterioration caused by the acids in the paper fibres, leaving documents brittle and discoloured over time.

pose major risks of difficulties in maintaining the continued authenticity, integrity, reliability and usability of electronic records over time.

2.8 Computer technology evolves at a rapid rate. As such, technology obsolescence is bound to occur in hardware, operating systems, storage media and software applications. Upgrades and new versions of hardware and software come onto the market from time to time[14]. The speed of changes in technology means that the timeframe during which action must be taken is very much shorter than for paper. This can result in electronic records created using older hardware and software becoming inaccessible in their original form after a relatively short period of time. Technology obsolescence is generally regarded as the greatest technical threat to ensuring continued access to electronic records.

2.9 Like technology obsolescence, media fragility and physical damage to hardware and storage media can render electronic records stored therein inaccessible and unreadable. Storage media such as magnetic tapes and optical disks are subject to deterioration and can fail suddenly due to material instability, improper storage environment (e.g. exposure to ultraviolet (UV), heat and high humidity), inadequate hardware maintenance, natural disasters, etc.

2.10 In view of the above risks, B/Ds should be mindful of the fact that electronic records cannot be maintained simply by keeping them in storage media in secure controlled conditions. Neither is the writing of electronic records to removable storage media as a back-up routine alone able to mitigate the risk of technology obsolescence.

2.11 Electronic records being rendered inaccessible, incomprehensible and unusable in view of technology obsolescence, media fragility and physical damage will jeopardise B/Ds' capability to comply with legal and regulatory requirements; and cause significant detriment to their business, evidence and accountability needs. If electronic records appraised to have archival value become inaccessible and unusable, it will result in loss of documentary heritage. Therefore, it is imperative for B/Ds to take concerted actions to overcome these challenges and mitigate the negative impacts of the associated risks.

Government-wide survey on preservation of electronic records

2.12 The challenges of preserving electronic records necessitate us to accord more attention and efforts to deal with the risk involved.

[14] For example, there have been upgrades to Windows software since it was first introduced and it would now be very difficult to convert from earlier versions to the current versions.

2.13 In 2012, GRS and OGCIO jointly conducted a government-wide survey to gauge the need for preservation of electronic records in B/Ds and assess the effectiveness of current preservation measures and practices adopted by B/Ds. All government B/Ds were invited to respond to a questionnaire survey containing 22 questions about the retention of their electronic records, computer systems in which their electronic records were managed and stored; and the current practices and measures adopted to preserve those electronic records.

2.14 A total of 74 B/Ds and offices set out at **Appendix** responded to the survey as at 31 December 2012, which represents a response rate of about 92.5%. **The findings of the survey have demonstrated a clear business case for B/Ds to take timely and proper measures and actions to preserve their electronic records**. A gist of the findings of the survey is summarised below–

(a) About 72% of all electronic records (around 1,617 terabytes (TB)) have to be managed and/or kept for a further period of seven years or longer with the base date starting from 1 July 2012 onwards. These electronic records in question were managed and/or stored in 896 information systems, representing about 76% of all the 1,180 information systems reported in the survey (Figure 1 refers).

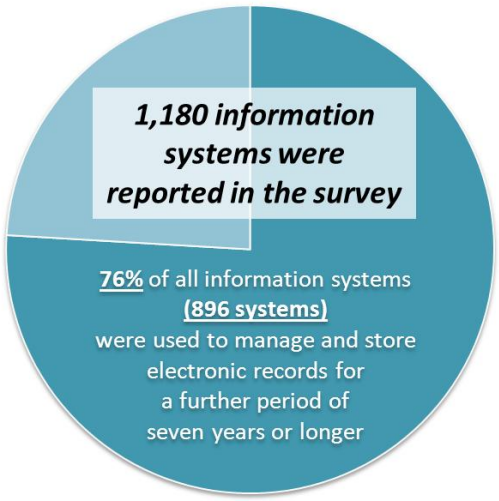


Figure 1: Information systems used to manage and/or store electronic records that needed to be managed and/or kept for a further period of seven years or longer

(b) 69 responding B/Ds and offices out of a total number of 74 advised that that they had to manage and keep some of their electronic records for a further period of seven years or longer. Therefore, a great majority of B/Ds need to proactively preserve their electronic records.

(c) Some electronic records reportedly have to be kept for very long periods exceeding seven years. A total of 41 B/Ds and offices (55% of all 74 responding B/Ds and offices) reported that some of their electronic records have to be kept for at least a further period of 20 years or longer.

(d) Potential risks of inaccessibility and unusability of electronic records stored in 'ageing' or legacy information systems may arise if no timely system upgrades are to be taken. Among 896 information systems that are currently used to manage and/or store electronic records for a further period of seven years or longer, 46% (409 systems) of them have not been upgraded, enhanced or re-developed since their live-run (Figure 2 refers).

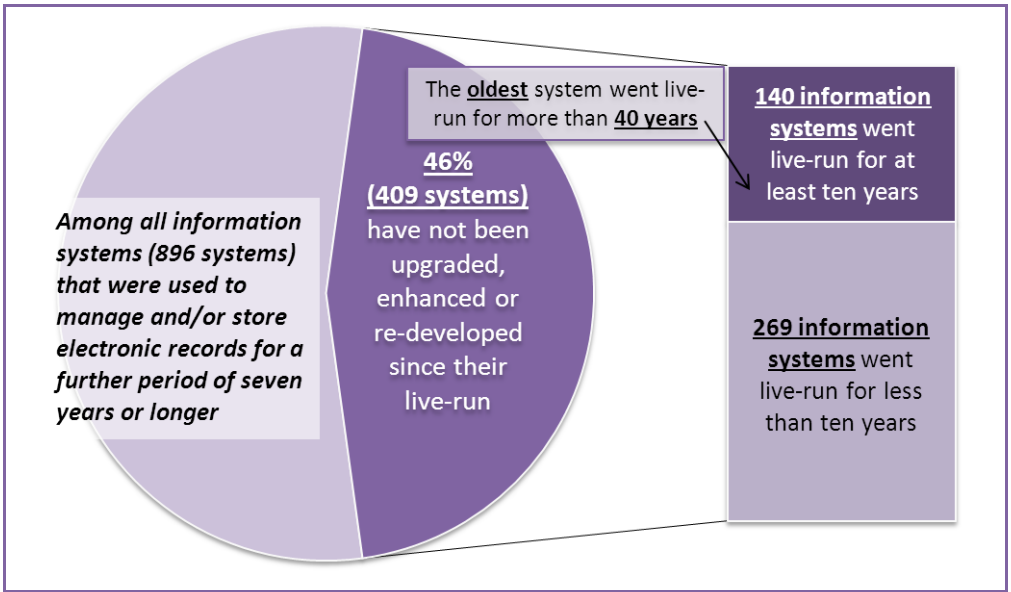


Figure 2: Information systems which have not been upgraded, enhanced and/or re-developed since their live-run

(e) The awareness of proper preservation of electronic records has to be enhanced. It is observed that–

(i) 487 systems (54% of all 896 reported information systems used to manage and/or store electronic records for a further period of seven years or longer) have been upgraded since their live-run but 42% of them (204 systems) did not possess built-in functionality to preserve electronic records;

(ii) Only 27 B/Ds and offices (36% of all responding B/Ds and offices) have conducted file format migration for their electronic records in the past seven years; and

(iii) For 49 B/Ds and offices (66% of all responding B/Ds and offices) that have managed and/or stored electronic records in off-line

storage media, only 15 of them have conducted media renewal and/or media migration to preserve electronic records stored in off-line storage media.

2.15 The findings of the government-wide survey have pinpointed that timely actions and measures should be taken by B/Ds to preserve their electronic records to eliminate or mitigate the identified major risks associated with technology obsolescence and media fragility.

Need for proper preservation of electronic records

2.16 The significant challenges: technology obsolescence, media fragility and physical damage of hardware and storage media caused by various factors put electronic records at great risk. When an electronic record becomes inaccessible and unreadable, it is usually lost for good. As such, B/Ds should proactively preserve electronic records to ensure their continuous authenticity, integrity, reliability and usability for as long as they are required.

2.17 Proper preservation of electronic records enables B/Ds to–

(a) protect the legal, financial and other interests of the Government, their organisations, their employees and the public;

(b) comply with legal and regulatory requirements and government directives;

(c) serve continuous business and operational needs, e.g. to make informed decisions and answer media enquiries;

(d) ensure the legal admissibility of electronic records to meet evidence purpose;

(e) fulfil the obligation to properly manage and preserve electronic records with potential archival value[15] or have been appraised to have archival value prior to transfer to PRO of GRS for appraisal and/or permanent retention;

[15] For the prescribed retention periods and disposal actions of administrative records, B/Ds should follow the guidelines set out in ***General Administrative Records Disposal Schedules*** (GARDS) promulgated by GRS. For administrative records and programme records (specific retention and disposal schedules are required to be established and approved by GRS) that are required to be transferred to PRO of GRS for appraisal, PRO will conduct an appraisal, to determine whether those records have archival value. If so, B/Ds are required to transfer those records with archival value to PRO for permanent retention.

(f) avoid causing damage to the reputation of the Government as a whole and their organisations due to inaccessibility, unusability or loss of electronic records to demonstrate an open and accountable Government; and

(g) avoid high recovery costs to reconstruct electronic records that have become unreadable.

What electronic records should be preserved

2.18 Records, including electronic records are commonly understood to have a life cycle from creation to final disposal[16]. Records once created and received in the course of business transactions may be retained for a short period of time, say two to three years, e.g. routine administrative records relating to building management of government premises. While some may be required for a long period of time, say seven years or longer, e.g. leave records of civil servants may be kept until the officers concerned have left the service, the retention periods of records should comply with legal and regulatory requirements; adhere to government directives[17]; meet business and operational needs; and serve evidence purpose.

2.19 **From preservation perspective, the longer the retention periods of the electronic records have, the higher the risks of inaccessibility and unusability of those records**. Therefore, proactive actions and measures should be adopted to **preserve electronic records that should be retained for seven years or longer** upon their creation as they are subject to risks of generations of technology changes throughout their life cycle. For those electronic records that have an approved retention period **not exceeding seven years**, B/Ds should take actions to preserve them if there is identified imminent threat to their continued accessibility and usability or where the situation warrants immediate actions.

2.20 Under the Government's Electronic Information Management Strategy as promulgated by OGCIO in May 2011, B/Ds should adopt or implement an electronic recordkeeping system (ERKS)[18] to manage both electronic and non-electronic records in an integrated and consistent manner. To support B/Ds to

[16] Please refer to Diagram 1 in Chapter 3.

[17] For the prescribed retention periods and disposal actions of administrative records, B/Ds should follow the guidelines set out in GARDS promulgated by GRS.

[18] An ERKS is an information 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. It is primarily designed to manage and store electronic records created and received in an unstructured computing environment.

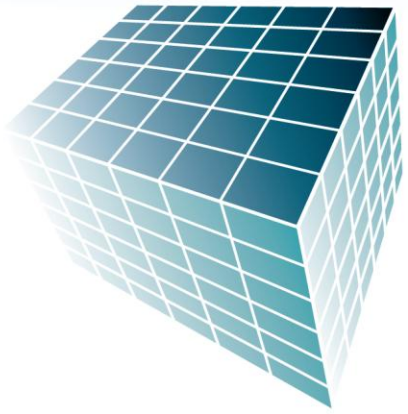
meet the challenge of file format obsolescence, the functionality of an ERKS as prescribed in the ***Functional Requirements of an Electronic Recordkeeping System*** developed by GRS includes the feature to render electronic records into pre-defined formats for preservation in addition to the native formats of the electronic records[19]. That said, the challenges of technology obsolescence in hardware and storage media, media fragility and physical damage should still be closely monitored and dealt with.

2.21 IT systems other than ERKSs and removable storage media are equally vulnerable to technology obsolescence, media fragility and physical damage. Therefore, B/Ds should also formulate strategies and implement suitable measures to preserve electronic records managed and/or stored in these IT systems and removable storage media.

B/Ds should plan for and implement preservation of electronic records to meet challenges of rapid technological changes, media decay and physical damage to hardware and storage media.

[19] Please refer to Requirement 32 of the ***Functional Requirements of an Electronic Recordkeeping System*** developed by GRS (http://grs.host.ccgo.hksarg/erm/s04/431.html).

Blank page



CHAPTER 3

Roles and Responsibilities for Preserving Electronic Records

Has your B/D defined clearly the roles and responsibilities to manage and preserve electronic records stored in information systems?

Chapter 3

Roles and Responsibilities for Preserving Electronic Records

Introduction

3.1 This chapter highlights the important roles and responsibilities of B/Ds to preserve electronic records throughout the life cycle of records and advises the support and assistance rendered by GRS and OGCIO in this regard.

Management perspective

3.2 The e-government initiative has resulted in development of more and more information systems in B/Ds to meet their specific business and operational needs; and to deliver public services in a more speedy and convenient manner. Some of those information systems are unique to individual B/Ds and have created, received and stored a large quantity of electronic records. Electronic records once created and received in the course of business transactions are managed and kept in B/Ds to serve legal and regulatory requirements, business and operational needs and evidence purpose according to the approved retention and disposal schedules. Upon the expiry of the approved retention periods, B/Ds should timely arrange disposal of the records[20].

3.3 As IT is a rapidly advancing field, it appears implausible that B/Ds will not need to preserve some of their electronic records through generations of technological changes in hardware, software and file formats. The rate and magnitude of the technological changes falls quite beyond the control of B/Ds but presents a formidable challenge of maintaining the authenticity, integrity, reliability and usability of electronic records. **Lack of institutional response to or delay in taking preservation measures will unquestionably increase the risk of inaccessibility, unusability and loss of electronic records**. Therefore, it is essential that B/Ds are aware of the value and characteristics of their electronic records and execute due diligence to properly manage and preserve them.

3.4 As many challenges and difficulties associated with preservation of electronic records requires concerted efforts to deal with, GRS and OGCIO render RM and IT advisory support and facilitation respectively to assist B/Ds in

[20] For electronic records that have been appraised by PRO of GRS to have archival value, B/Ds are required to transfer them to PRO for permanent retention upon the expiry of the approved retention periods.

developing viable preservation programmes, and adopting suitable measures and practices to preserve their electronic records effectively and properly.

3.5 In terms of preservation of electronic records, the roles and responsibilities among GRS, OGCIO and B/Ds are illustrated in Diagram 1 below.

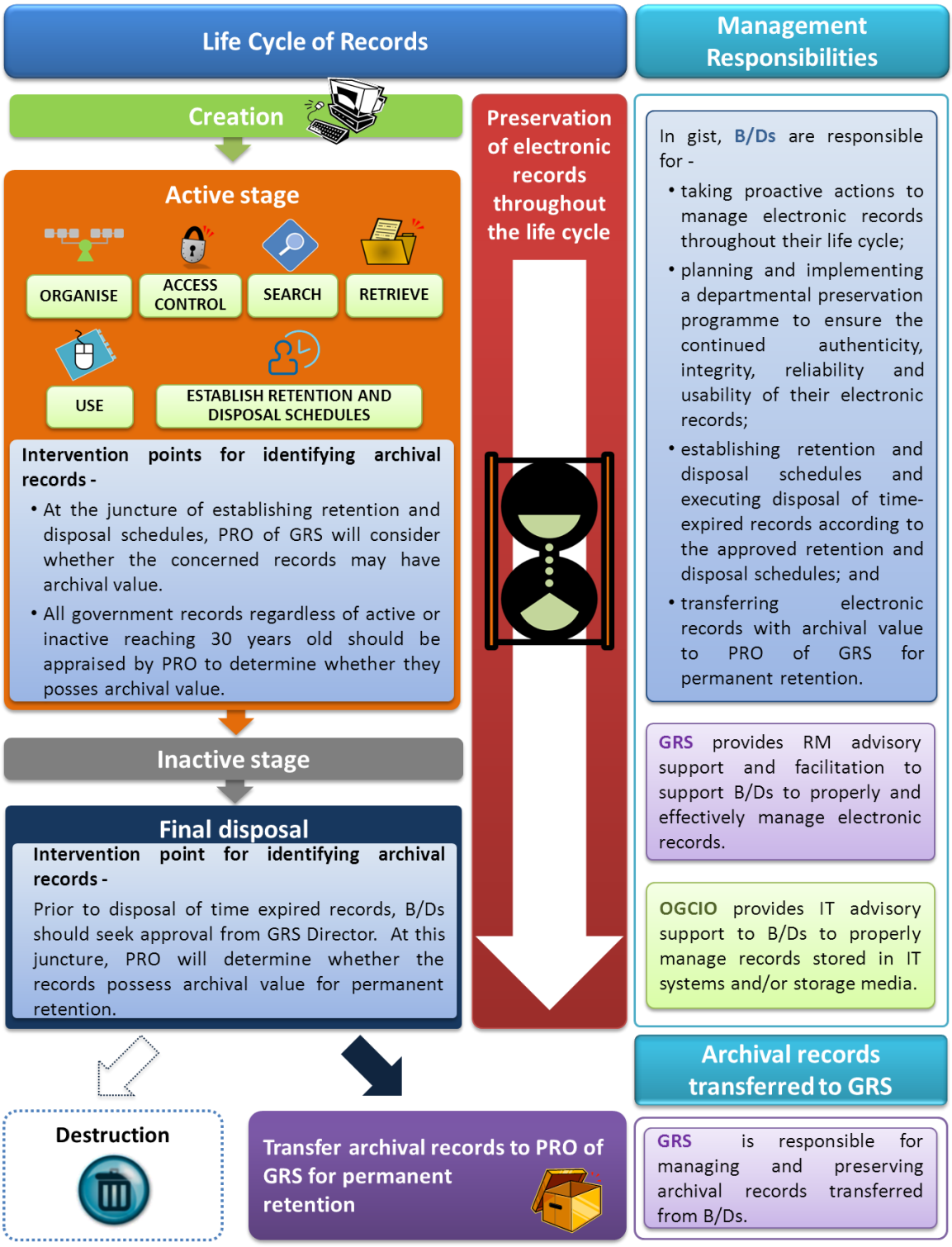


Diagram 1: Management Responsibilities for Preserving Electronic Records

Roles and responsibilities of B/Ds

3.6 Undoubtedly, B/Ds plays a key role in preserving electronic records during the life cycle of records as those records are managed, used and stored in their organisations[21]. In gist, B/Ds are responsible for–

(a) planning and implementing a departmental preservation programme(s) to deal with challenges of preservation of electronic records in their organisations. Details are set out in Chapter 4;

(b) putting in place timely and suitable measures and practices to preserve electronic records for as long as they are required to serve continuous legal and regulatory requirements, business and operational needs and evidence purpose;

(c) establishing retention and disposal schedules for all programme records[22] in electronic form managed by and/or stored in structured and unstructured computing environments. B/Ds should execute disposal of time-expired electronic records according to approved retention and disposal schedules or GARDS[23] as appropriate. It is a waste of valuable resources and efforts to preserve electronic records that are kept for short periods, say less than seven years unless there is an imminent risk of inaccessibility, unusability and loss of such records due to technology obsolescence, media fragility and other reasons. Timely disposal of time-expired records minimises preservation efforts;

(d) being watchful of technological changes and identifying potential risks of electronic records under their custody, such as obsolete systems and file formats, and media deterioration;

(e) monitoring and reviewing the effectiveness of preservation measures and practices adopted in their organisations on a regular basis;

(f) reporting loss of electronic records to GRS due to unavailability and inaccessibility of those records;

(g) properly managing and preserving electronic records with potential archival value[24] until and unless PRO of GRS has appraised and determined their archival value; and

[21] For electronic records that are stored in data centres operated by service providers, B/Ds are still responsible for taking proper actions to preserve them for as long as they are required.
[22] Programme records are records created or received by a B/D whilst carrying out the primary functions, activities or mission for which the B/D was established. Records of this nature are unique to each B/D.
[23] Please see footnote 17.
[24] Please see footnote 15.

(h) properly managing and preserving electronic records appraised with archival value until and unless they have been successfully transferred to PRO for permanent retention.

3.7 **The success and sustainability of preservation of electronic records requires concerted efforts of different stakeholders in B/Ds**. It is of utmost importance for B/Ds to define clearly the roles and responsibilities of key stakeholders and the governance in planning, implementing and reviewing the departmental preservation programme in their organisations. In this connection, B/Ds may consider establishing a governance structure with representatives from business units, departmental RM staff and IT staff of ITMU to formulate departmental strategies and practices to deal with preservation of electronic records.

Support and assistance from GRS and OGCIO

3.8 Being the central RM agency of the Government, GRS is responsible for, among others, formulating government RM policies and programmes; and monitoring RM practices of B/Ds. As far as preservation of electronic records is concerned, GRS is responsible for–

(a) formulating standards, guidelines and good practices in collaboration with OGCIO for compliance and reference by B/Ds;

(b) providing RM advisory support and assistance to assist B/Ds in preserving electronic records properly and effectively;

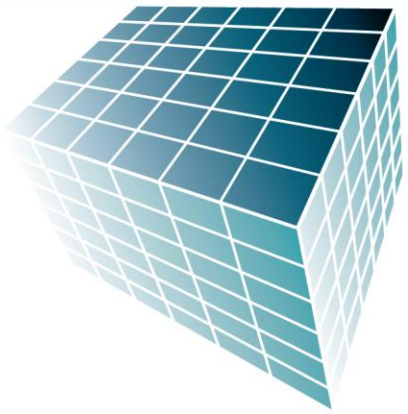
(c) appraising electronic records with potential archival value, prescribing requirements for transfer of electronic records with archival value from B/Ds to GRS; and

(d) managing and preserving archival records under GRS' custody.

3.9 OGCIO, which provides IT services and support within the Government, is responsible for providing IT advice to assist B/Ds in tackling technical issues to preserve electronic records.

B/Ds are responsible for managing and preserving their electronic records while GRS undertakes preservation of electronic records with archival value transferred from B/Ds.

Blank page



CHAPTER 4

Establishment and Implementation of a Departmental Preservation Programme

Has your B/D formulated or considered to formulate a departmental preservation programme to preserve electronic records?

Chapter 4

Establishment and Implementation of a Departmental Preservation Programme

Introduction

4.1 This chapter advises B/Ds to formulate a viable departmental preservation programme(s) to implement preservation of electronic records from an organisational perspective.

Need for a departmental preservation programme

4.2 Preservation of electronic records is complex requiring an integrated approach that combines the organisational context, RM principles, technological implementation, and requisite resources. To ensure that sufficient resources and attention will be accorded to preserving electronic records timely and effectively, **it is recommended that B/Ds should formulate a departmental preservation programme covering all electronic records that should be preserved**. Such programme should form part and parcel of a departmental RM programme and be suitably incorporated in the Departmental IT Projects Portfolio to plan for timely technology upgrade/redevelopment as appropriate.

4.3 Preservation of electronic records requires concerted efforts of different stakeholders in B/Ds. **DRMs and Heads of ITMUs as appropriate should take the lead to plan, co-ordinate, implement and review the departmental preservation programme** and the associated preservation measures, actions and practices from an organisational level to ensure effectiveness and continuous improvement of the programme.

Establish and implement a departmental preservation programme

4.4 To assist B/Ds in planning, execution and monitoring of a departmental preservation programme, a four-step approach: **Plan**, **Act**, **Check** and **Review** shown in Diagram 2 is recommended for adoption by B/Ds. Details are set out below.

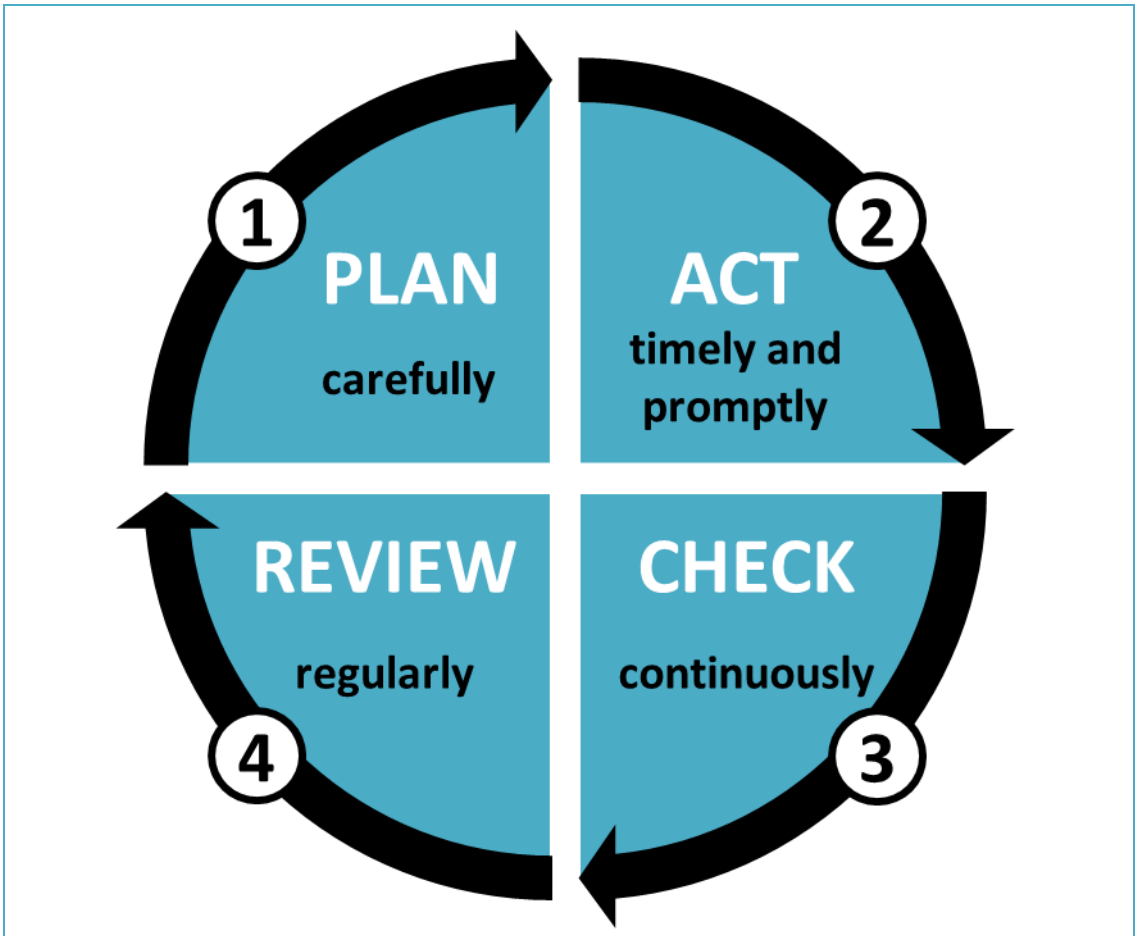


Diagram 2: Establish and implement a departmental preservation programme

STEP 1: PLAN

4.5 B/Ds should carefully plan the departmental preservation programme by taking into account their legislative obligations, Government's RM and IT directives, and their specific business and operation needs. In this step, B/Ds should draw up the programme which should include–

(a) identifying the scope of electronic records that should be preserved (including those electronic records that should be kept for seven years or longer and those electronic records that are at great imminent risk of becoming inaccessible and unusable);

(b) setting priorities of electronic records that should be preserved;

(c) identifying the potential risks, e.g. obsolete file formats that the electronic records may be exposed to; and the circumstances under which preservation measures should be taken;

(d) identifying suitable preservation measures, tools and practices having regard to the specific risks of electronic records that should be preserved;

(e) developing a practical timetable for undertaking the preservation measures and tasks. Some of the preservation measures may need to be performed at regular intervals such as refreshing removable storage media like CDs and DVDs;

(f) allocating sufficient resources and manpower to implement and monitor the programme; and

(g) assigning roles and responsibilities to implement and monitor the programme.

4.6 The departmental preservation programme should seek endorsement from senior management and be promulgated to key stakeholders for compliance and reference. B/Ds should also assess the resource implications to implement the departmental preservation programme and secure sufficient resources to take forward the programme.

STEP 2: ACT

4.7 Once the departmental preservation programme is largely formulated, B/Ds should then–

(a) perform tasks and adopt measures and practices to preserve electronic records such as conducting a condition survey to assess the deterioration of storage media in which electronic records are stored;

(b) develop proper practices and procedures, e.g. the practices and procedures to refresh storage media and migrate electronic records from the existing ageing IT systems to upgraded systems, to preserve electronic records and monitor the effectiveness of the programme;

(c) procure suitable equipment, devices and services to support preservation of electronic records;

(d) conduct testing where appropriate to assess the effectiveness of the preservation measures, practices and equipment prior to full implementation;

(e) validate the authenticity, integrity, reliability and usability of electronic records after preservation measures have been taken;

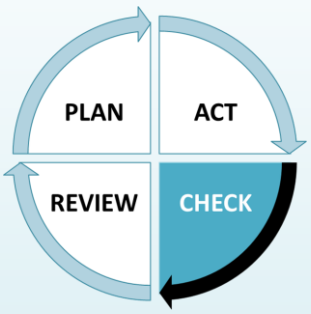
(f) provide suitable training for staff members responsible for preservation of electronic records; and

(g) properly document the procedures and practices to preserve electronic records.

4.8 In the event that there is an immediate risk of inaccessibility, unusability and loss of electronic records, B/Ds should take timely actions to address the problem prior to the formulation of the departmental preservation programme.

STEP 3: CHECK

4.9 In this step, B/Ds should–



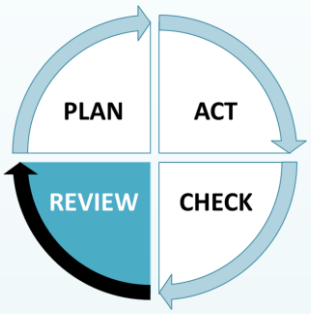
(a) monitor and evaluate the effectiveness of their departmental preservation programme on an on-going basis;

(b) be watchful of technological changes in hardware, software, file formats and storage media; and

(c) determine the use of appropriate electronic storage media and file formats to keep electronic records newly created and received in their organisations.

STEP 4: REVIEW

4.10 B/Ds should review and revise the programme as appropriate on regular intervals, say two to three years or as and when necessary having regard to technological changes and their business and operational needs. The review should assess–



(a) the scope of electronic records that should be preserved. For example, a change in the retention periods and disposal actions of electronic records may necessitate a review of whether preservation should be required;

(b) whether the resources input of the programme is sufficient and cost-effective;

(c) whether the practices and procedures, and roles and responsibilities should be revised and refined having regard to technological changes and operational needs; and

(d) whether the documentation of the programme is adequate and accurate.

STEP 4: REVIEW (CONTINUED)

4.11 Upon the completion of a review, B/Ds should–

(a) update or revise the preservation practices and procedures as appropriate;

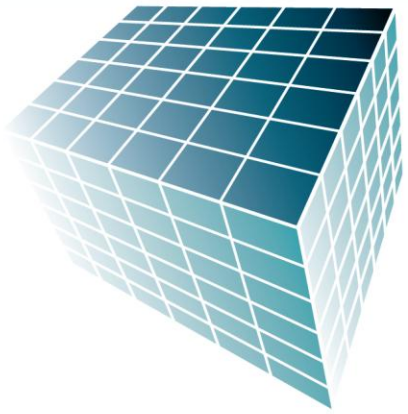
(b) update the documentation of the programme as appropriate;

(c) arrange proper training for relevant staff members as appropriate; and

(d) arrange testing of the revised preservation measures and practices.

B/Ds should develop a departmental preservation programme to plan, implement, monitor and review preservation of their electronic records.

Blank page



CHAPTER 5

Good Practices for Preserving Electronic Records

Has your B/D determined the appropriate preservation measures and actions to preserve electronic records? Is your B/D doing right to preserve electronic records?

Chapter 5

Good Practices for Preserving Electronic Records

Introduction

5.1 This chapter advises general good practices and measures to preserve electronic records.

Life-cycle management and preservation of electronic records

5.2 Preservation of electronic records differs greatly from that of paper records as the medium of paper is relatively stable after many years of their creation. It is widely acknowledged that a robust life-cycle management approach should be taken to manage and preserve electronic records once they are created or received in the face of constantly changing technology. The rationale for adopting this approach is to ensure that electronic records retain their essential qualities, i.e. authenticity, integrity, reliability and usability with their logical and physical structure, content and context intact to the extent necessary for their continuing trustworthiness as records for as long as they are required.

5.3 As preservation of electronic records cannot and should not be delayed until the end of the life cycle of records, **it is inextricably intertwined with the on-going management activities of electronic records**. In fact, some measures such as establishing proper security of electronic records achieve dual purposes of proper management and preservation of electronic records to maintain their integrity.

5.4 Given that this handbook focuses primarily on preservation of electronic records, there is little mention of best RM practices for management of electronic records. Nevertheless, it does not mean that proper management of electronic records is not important nor it should be separated from preservation activities. B/Ds should make reference to RM standards, practices and guidelines promulgated by GRS for managing electronic records in a proper and secure manner.

Attributes and qualities of electronic records to be preserved

5.5 In order to meet legal, regulatory, business, operational and evidence requirements and purposes, B/Ds have to sustain the qualities of electronic records over time and across technological changes. To this end, electronic records should be properly managed and preserved in accordance with the following principles:

(a) fixed in its form and stable in content[25] (i.e. unchanged and unchangeable);

(b) authentic (i.e. has not been altered, changed or corrupted);

(c) identifiable uniquely in such a way that it is easy for users and information systems to distinguish between records;

(d) easily accessible and retrievable;

(e) intelligible and correctly interpreted by a computer application;

(f) human readable and understandable;

(g) interoperable and transferable (so that records, associated metadata and audit trails can be transferred from one platform to another and can then still be reproduced in the same or a similar way);

(h) auditable through the use of audit trails to confirm whether the record is unchanged or that only authorized and appropriate changes have been made;

(i) associated with persistent contextual information through the attribution of recordkeeping metadata to records; and

(j) secure against accidental loss, corruption and alteration during transfer, custody and storage.

[25] The quality of a record that ensures the documentary appearance or presentation is the same each time the record is retrieved. A simple example is when a document created in Microsoft Word is later saved as an Adobe PDF file. Although the document's digital presentation has changed–from a Microsoft Word .doc file format to an Adobe .pdf file format–the documentary presentation of the document–also called its documentary form–has not changed, and therefore we can say that the document has a fixed form. By the same token, if the same query from an information system always produces the same output as to content and documentary form, the output can be regarded as having stable content and fixed form. Reference can be made to ***A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records***, InterPARES 2 Project, June 2005 and ***Creator Guidelines—Making and Maintaining Digital Materials: Guidelines for Individuals***, InterPARES 2 Project, June 2007.

Active and passive preservation

5.6 Preservation of electronic records encompasses a broad range of activities. There are two overarching approaches to the preservation of electronic records: **active preservation** and **passive preservation**.

5.7 **Active preservation** refers to intervention(s) in the bit stream used to encode the content of the electronic records as may be required over time to preserve access to the content of the records and their values as evidence and as cultural heritage[26]. Put it simply, active preservation involves planning and taking actions to offset technology obsolescence of electronic records and may involve adopting new technologies that were not in existence when the electronic records were originally created and used. Measures may include–

(a) assessing potential risks of preserving electronic records over time and the anticipated impacts; and plan for proactive actions, e.g. upgrading of obsolete IT systems to deal with the identified risks;

(b) implementing a technology watch programme to track technical dependencies of electronic records such as monitoring the obsolescence of file formats of electronic records; and

(c) migrating obsolete file formats of electronic records to other formats using more current technology to preserve their accessibility.

5.8 **Passive preservation** refers to the provision of secure storage and integrity of each record manifestation[27]. Essentially, passive preservation aims to 'keep' the original electronic records intact without changing the technologies used to store or process it. Measures may include–

(a) monitoring and refreshing storage media to offset the risks of media degradation;

(b) maintaining proper access control and security of electronic records;

(c) backing up electronic records in secure off-site storage; and

(d) conducting checking on the integrity of electronic records, e.g. through the use of checksums[28].

---

[26] ***Functional Requirements for the Sustainability of Electronic Records***, The National Archives (United Kingdom), March 2006.

[27] ***Functional Requirements for the Sustainability of Electronic Records***, The National Archives (United Kingdom), March 2006.

[28] A **checksum** or **hash sum** is a small-size datum computed from an arbitrary block of digital data for the purpose of detecting errors that may have been introduced during its transmission or storage. The

5.9 B/Ds may adopt both active preservation and passive preservation in parallel to preserve their electronic records as appropriate.

Good practices for preserving electronic records

5.10 Preservation is an on-going process throughout the life cycle of electronic records. In view of rapid technological changes, preservation methods, practices and tools are also evolving. With a view to ensuring that this handbook remains useful beyond generations of technological changes, technology-dependent preservation measures and practices are excluded intentionally. Instead, general preservation practices and measures proven to be relatively long-lasting and effective are set out in this handbook for reference by B/Ds. B/Ds may select other preservation methods, practices and measures that are suitable to address their specific preservation requirements.

5.11 **Ten general good practices and measures** for adoption to preserve electronic records are set out in the following table for reference by B/Ds–

S/N	Good Practice
Active preservation	
1.	B/Ds should conduct regular surveillance of technological changes and plan for timely migration of electronic records, associated recordkeeping metadata, audit trails and other data such as indexes to ensure that all records remain accessible, readable and understandable over time even when the technology of their specific hardware and/or software become obsolete. Please see **Tips for establishing a technology watch or monitoring programme** on page 39.
2.	B/Ds should take timely actions to migrate electronic records stored in ageing and obsolete IT systems[29] to newer IT systems to avoid inaccessibility and unusability of those electronic records. Please see **Tips for migration of electronic records** on page 40.

integrity of the data can be checked at any later time by recomputing the checksum and comparing it with the stored one. If the checksums match, the data is likely not accidentally altered.

[29] Records stored in databases such as FoxPro, Visual FoxPro and dBase should be migrated to new IT systems as soon as practicable.

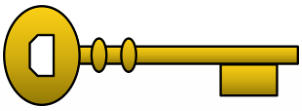
S/N	Good Practice
3.	B/Ds should consider rendering and storing electronic records to be preserved in file formats that are more conducive to long-term preservation, e.g. eXtensible Markup Language (XML), Portable Document Format for Archive (PDF/A) and Tagged Image File Format (TIFF). For electronic records to be managed and stored in an ERKS, the system functionality has built in features for rendering electronic records into pre-defined formats for preservation in addition to their native formats[30]. B/Ds should use this feature accordingly. Please see **Tips for selecting file formats to reduce vulnerability to obsolescence** on page 41.
4.	B/Ds should plan for and implement migration of electronic records in obsolete file formats to another format or to a newer version of the same format as appropriate.
Passive preservation	
5.	B/Ds should put in place adequate and proper access control and security measures to ensure the security of electronic records stored in information systems and/or storage media from data losses, virus infections and security vulnerabilities; and prevent the records from unauthorised access, tampering, alteration and erasure. B/Ds should conform to the requirements of the Security Regulations and IT security guidelines promulgated by OGCIO to handle, manage and protect electronic records according to their security classifications.
6.	B/Ds should properly keep audit logs of IT systems in which electronic records are stored to demonstrate the authenticity and integrity of the electronic records over time. B/Ds should also properly document the access and use of electronic records stored in off-line storage media to safeguard the integrity of records. [Note: Please refer to ***Functional Requirements of an Electronic Recordkeeping System*** for requirements of audit trails of electronic

[30] Please see footnote 19.

S/N	Good Practice
	records managed and stored in an ERKS.]
7.	B/Ds should keep electronic records with their associated metadata so as to ensure that sufficient contextual information is available to understand and interpret the records over time. B/Ds should also keep adequate and valid system documentation of IT systems in which electronic records are stored. The documentation is useful to understand the hardware and software required to view the records; and perform system management and maintenance.
8.	B/Ds should ensure that storage media in which electronic records are stored be kept in secured places where the environment is conducive to preserving the storage media over time. Please see **Tips for addressing media durability** on page 42. B/Ds should also handle storage media in a proper manner to extend their longevity. Please see **Tips for proper handling of storage media** on page 43. B/Ds should plan for and carry out refreshment and/or migration of storage media at regular intervals to counteract media deterioration. Please see **Tips for refreshing storage media** on page 44. B/Ds should also conduct regular checking on the conditions of the storage media to ensure that all records contained therein are accessible and readable over time.
9.	B/Ds should schedule and conduct integrity checking of electronic records stored in storage media on a regular basis to ensure that there is no corruption of electronic records. [Note: In general, if storage media are kept in good conditions, the integrity checking may be conducted every five years but if the storage media are kept in less favourable environment, the checking may need to be conducted more frequently, say 18-24 months. All supporting evidence for verifying the integrity of records such as digital signature and certificates must be kept.]

S/N	Good Practice
10.	B/Ds should back up electronic records as a routine of system management and keep an inventory of removable storage media in which electronic records are stored. B/Ds should ensure that the removable storage media are assigned with a unique identifier.

B/Ds must be proactive to plan and implement preservation of electronic records.



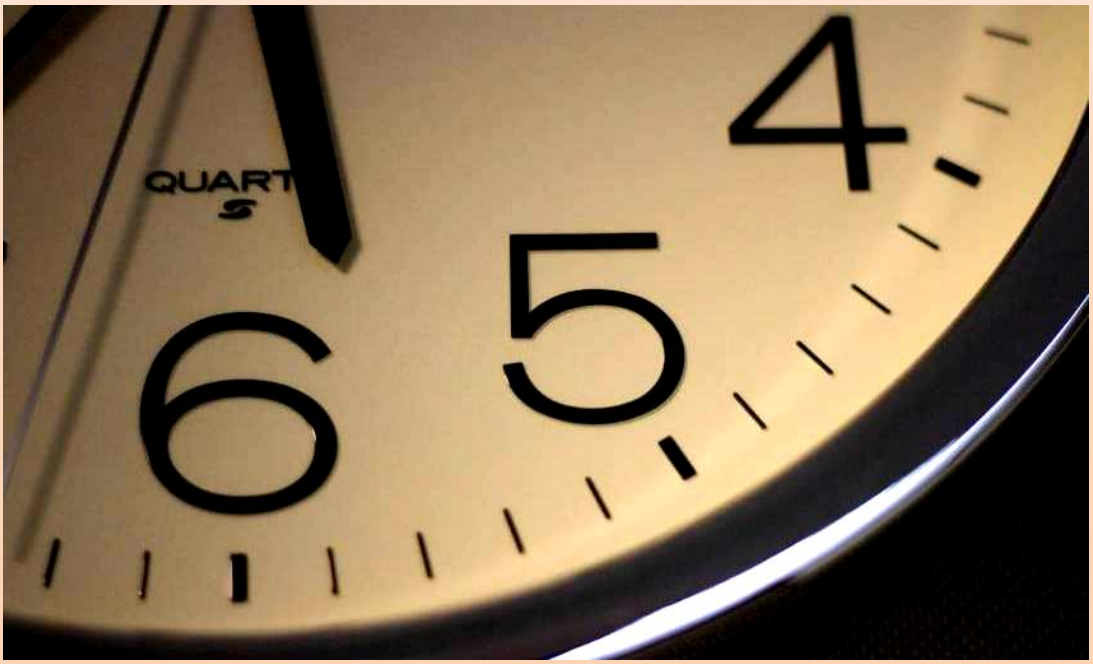
1

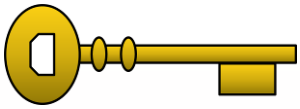
TIPS FOR ESTABLISHING A TECHNOLOGY WATCH OR MONITORING PROGRAMME:

In gist, a technology watch or monitoring programme aims to continuously monitor the current software and hardware technologies to ascertain if any of the software file formats, within which the electronic records are held, and the storage media within which the records are stored are in some way obsolescent or problematic.

The elements of a technology watch programme include–

- identifying the criteria for assessing whether a particular file format requires migration;
- identifying the criteria for assessing whether a particular type of storage media requires migration;
- establishing an effective mechanism to determine what types of intervention is required, e.g. conversion to standard industry supported format; and
- determine the time-scale and resources to undertake the necessary work before the records are irretrievably compromised.



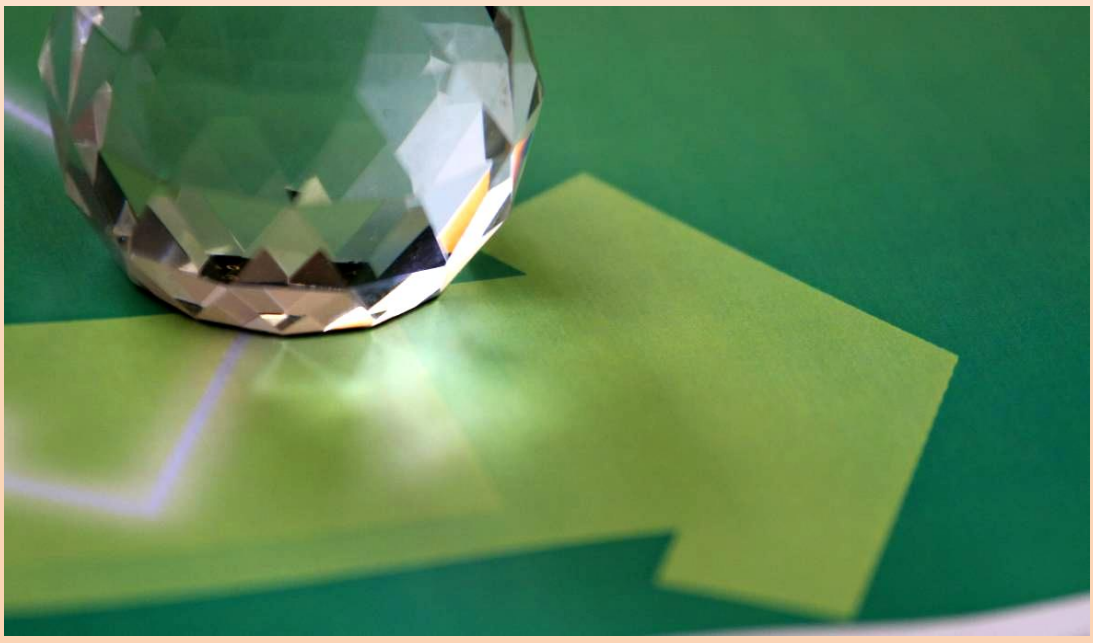


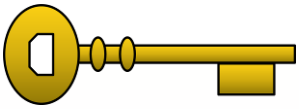
2

TIPS FOR MIGRATION OF ELECTRONIC RECORDS:

Electronic records may be stored for a considerable length of time and, importantly for longer than the lifetime of the current technology. Therefore, it is important to plan from the outset that records to be kept for seven years or longer will be subject to migration processes. Such process may involve a change of storage media; and/or computer hardware; and/or software. In conducting migration of electronic records, B/Ds should–

- develop procedures and processes to migrate the records;
- include appropriate metadata, index data and audit trails; and add metadata detailing the migration process where appropriate;
- ensure that all records need to be transferred have been transferred;
- ensure the security of the migration processes;
- ensure that authenticity and integrity of electronic records are not compromised after the migration, e.g. techniques such as audit trails and checksums should be used to document and/or manage the processes used; and
- keep records of migration processes to demonstrate that integrity has not been compromised during the processes.



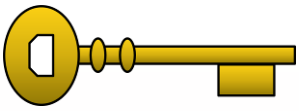


3

TIPS FOR SELECTING FILE FORMATS TO REDUCE VULNERABILITY TO OBSOLESCENCE:

File formats encode information into forms that can be processed and rendered comprehensible by specific hardware and software. File format obsolescence is bound to happen for a number of reasons such as software upgrades failing to support legacy files and supersedes of the file format itself. File format obsolescence jeopardises the accessibility and readability of electronic records. As such, the selection of file formats for creating electronic records should therefore be determined not only by the immediate requirements of the situation, but should also with long-term sustainability in mind. When selecting file formats, B/Ds should make reference to HKSARG Interoperability Framework [S18] and consider the following factors–

- whether a file format is an open format, e.g. Hyper Text Markup Language (HTML), PDF/A and Joint Photographic Experts Group (JPEG) of which the specification is publicly released. Use open formats as far as practicable;
- whether a file format has good metadata support. Metadata such as those providing information on both the provenance and technical characteristics of the file format supports preservation;
- whether a file format is a de facto format that has achieved a dominant position by public acceptance or market forces such as Microsoft Office, or a commonly adopted format. There will be a better chance for de facto and widely adopted file formats to survive in the market for a longer run;
- whether a file format has proven history of backward compatibility. Backward compatibility ensures accessibility of older versions of the file format;
- whether the estimated costs and complexity of migration of file formats are high;
- whether there is built-in error checking to allow detection of file corruption. For example, Portable Network Graphics (PNG) incorporates byte sequences to check for three specific errors. Formats that provide built-in error checking are preferable to those that do not have; and
- whether the upgrade cycle of a file format is reasonable without subject to constant or major changes over time.

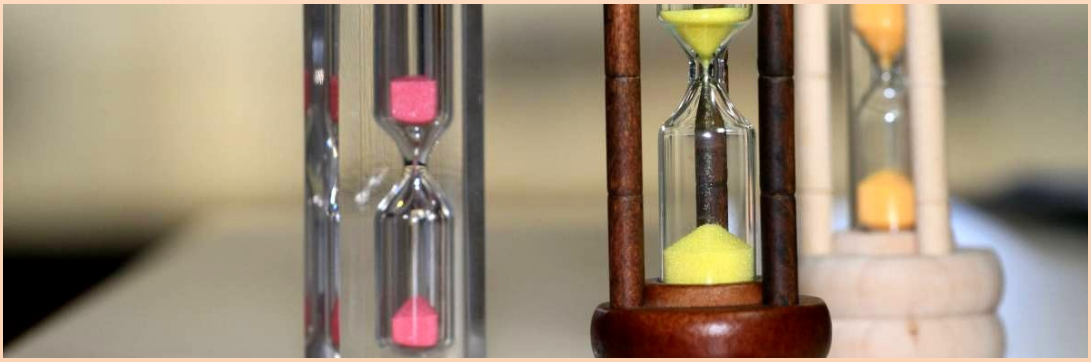


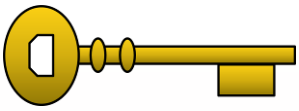
4

TIPS FOR ADDRESSING MEDIA DURABILITY:

Electronic storage media are subject to a lifespan, deterioration and destruction arising from exposure to heat, high humidity, faulty reading and writing devices, etc. Precautionary measures should be taken to help significantly reduce the risk of decay and damage of storage media. They include–

- selecting media technologies that are based upon open standards. An open standard has attained wide adoption or recognition through an authoritative standardisation body such as ISO;
- storing storage media in a stable, controlled environment. The environment should, as far as practicable, be–
  - kept an average temperature of 20°C and an average relative humidity of 40% (respective fluctuation should be no more than 2°C and 5% in 24 hours);
  - clean and dust-free and low in air pollutants especially volatile organic compounds (VOCs);
  - protected from exposure to sunlight and UV from light fixtures;
- handling storage media according to proper procedures, e.g. to avoid using solvents to clean CDs and DVDs;
- conducting regular checking such as sampling checking on the conditions of the storage media to ensure that all records contained are accessible and readable over time; and
- implementing refreshment cycles to copy all records stored in storage media into new storage media.





5

TIPS FOR PROPER HANDLING OF STORAGE MEDIA:

Besides storing storage media in secure, stable and controlled environment, proper handling also helps extend the longevity of the devices. Tips for handling storage media are set out below–

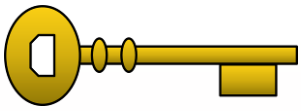
Dos

- Limit storage media access to trained and designated staff;
- Handle storage media with clean and dry hands. Lint-free glove should be used to minimise media's contact with dust and grease;
- Keep storage media in their cases when not in use;
- Re-wind magnetic tapes after each use and every one to three years; and
- Use approved markers on the top surface to label CDs and DVDs.

Don'ts

- Do not open shutters designed to protect the media cartridges;
- Do not touch exposed media surfaces (e.g. hold CDs or DVDs at edges);
- Do not leave storage media in drive after use;
- Do not bend storage media;
- Do not use solvents to clean storage media; and
- Do not remove any labels from CDs and DVDs.

Source: With adaptation from *Digital Preservation Management: Implementing Short-term Strategies for Long-term Problems, Online Tutorial Developed for the Digital Preservation Management Workshop*, Cornell University Library, 2005.



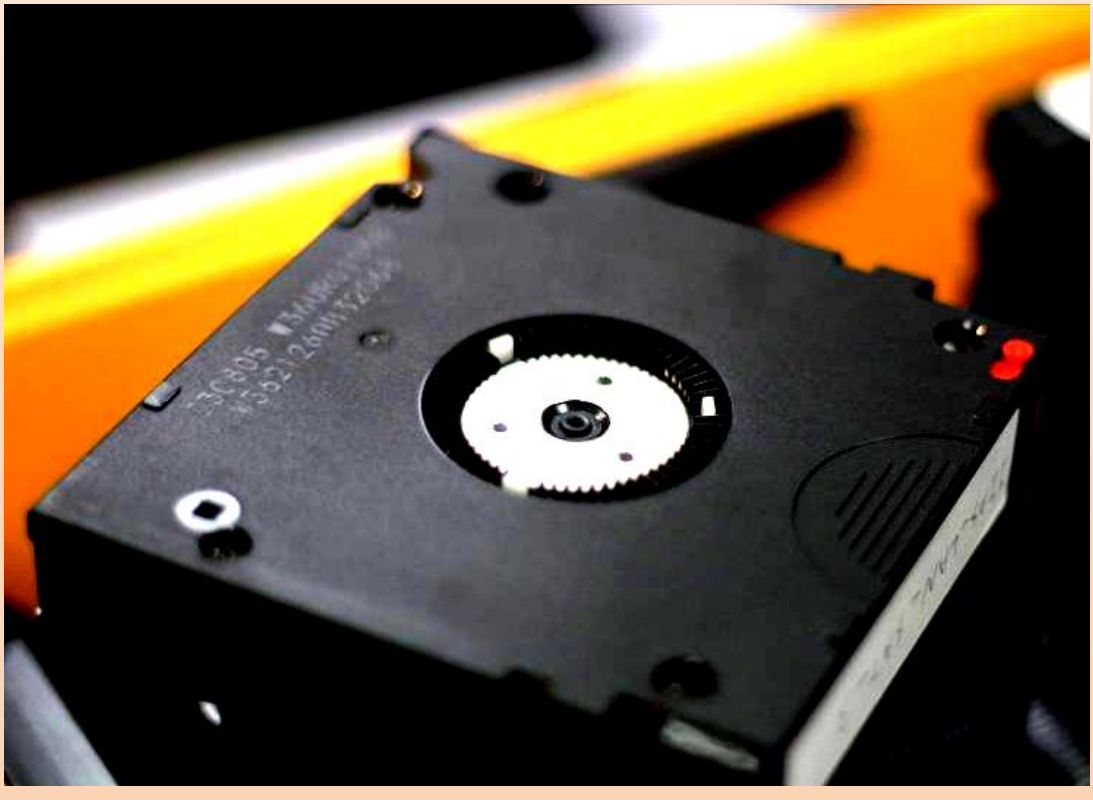
6

TIPS FOR REFRESHING STORAGE MEDIA:

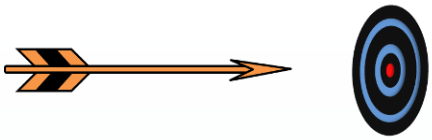
To counteract media fragility, refreshment of storage media is a common solution. Refreshing is the process of copying records and other data from one storage medium to another of the same type without change to the bit streams. For example, refreshment may copy electronic records from a CD-ROM disk to another so that records can be accessed using the same information system.

The periodic need to refresh electronic records stored onto new media is inevitable. However, selecting the best media available can reduce the frequency for refreshing records, since high quality and stable storage media should remain usable for a longer period.

In refreshing the storage media, B/Ds should ensure that proper verification or validation process is taken to ensure that the content of the electronic records stored in the storage media has been copied without corruption or loss.



Conclusion

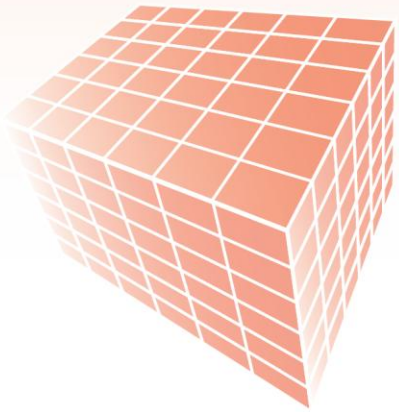


Preservation of electronic records represents a daunting challenge, at both a technical and organisational level, and many difficulties remain to be fully resolved. However, difficulties should not be seen as a justification for us to postpone action now because it is neither possible nor necessary for us to wait until all significant challenges and difficulties have been overcome before action is taken.

Establishment of a viable departmental preservation programme and adoption of timely and suitable preservation measures can significantly reduce the potential risks of inaccessibility, unusability and loss of electronic records; and greatly improve prospects for keeping valuable documentary heritage for the future generations.

Let's join hands to start the journey of preservation of electronic records.

Blank page



APPENDIX

Survey on Preservation of Electronic Records in Bureaux and Departments- Participating B/Ds and Offices

Appendix

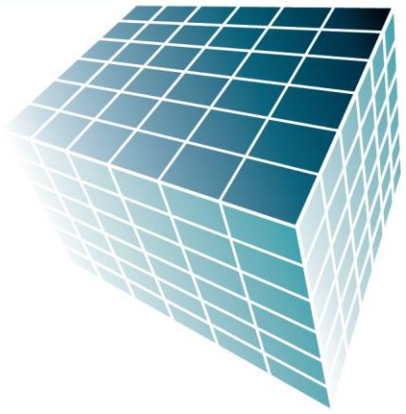
Survey on Preservation of Electronic Records in Bureaux and Departments—Participating B/Ds and Offices

We would like to thank the following B/Ds and Offices for participating in the government-wide survey conducted in 2012 on long-term preservation of electronic records.

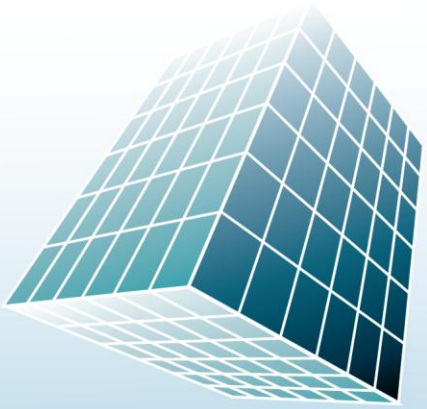
	Bureau/Department/Office
1.	Agriculture, Fisheries & Conservation Department
2.	Architectural Services Department
3.	Audit Commission
4.	Auxiliary Medical Service
5.	Buildings Department
6.	Census and Statistics Department
7.	Central Policy Unit
8.	Chief Executive's Office
9.	Chief Secretary for Administration's Office (including the Chief Secretary for Administration's Private Office, the Financial Secretary's Private Office, the Administration Wing and the Office of the Former Chief Executives)
10.	Civil Aid Service
11.	Civil Aviation Department
12.	Civil Engineering and Development Department
13.	Civil Service Bureau
14.	Commerce and Economic Development Bureau (Commerce, Industry and Tourism Branch)
15.	Commerce and Economic Development Bureau (Communications and Technology Branch)
16.	Office of the Communications Authority
17.	Companies Registry
18.	Constitutional and Mainland Affairs Bureau
19.	Correctional Services Department
20.	Customs and Excise Department

	Bureau/Department/Office
21.	Development Bureau (Planning and Lands)
22.	Development Bureau (Works)
23.	Drainage Services Department
24.	Economic Analysis and Business Facilitation Unit
25.	Education Bureau
26.	Efficiency Unit
27.	Electrical and Mechanical Services Department
28.	Environment Bureau/Environmental Protection Department
29.	Financial Services and the Treasury Bureau (Financial Services)
30.	Financial Services and the Treasury Bureau (Treasury)
31.	Fire Services Department
32.	Food and Environmental Hygiene Department
33.	Government Flying Service
34.	Government Logistics Department
35.	Government Property Agency
36.	Department of Health
37.	Highways Department
38.	Home Affairs Bureau
39.	Hong Kong Monetary Authority
40.	Hong Kong Observatory
41.	Hong Kong Police Force
42.	Hong Kong Post
43.	Housing Department
44.	Immigration Department
45.	Independent Commission Against Corruption
46.	Information Services Department
47.	Inland Revenue Department
48.	Innovation and Technology Commission
49.	Intellectual Property Department
50.	Invest Hong Kong
51.	Joint Secretariat for the Advisory Bodies on Civil Service and Judicial Salaries and Conditions of Service

Bureau/Department/Office	
52.	Judiciary
53.	Department of Justice
54.	Labour and Welfare Bureau
55.	Labour Department
56.	Land Registry
57.	Lands Department
58.	Legal Aid Department
59.	Leisure and Cultural Services Department
60.	Marine Department
61.	Office of the Government Chief Information Officer
62.	Official Receiver's Office
63.	Planning Department
64.	Public Service Commission
65.	Radio Television Hong Kong
66.	Rating and Valuation Department
67.	Registration and Electoral Office
68.	Security Bureau
69.	Social Welfare Department
70.	Student Financial Assistance Agency
71.	Trade and Industry Department
72.	Transport and Housing Bureau (Transport)
73.	Transport Department
74.	Water Supplies Department



REFERENCE



Reference

- **Beagrie, N. and Jones, M. (2008)**
  Preservation Management of Digital Materials: The Handbook
  http://www.dpconline.org/advice/preservationhandbook
  Digital Preservation Coalition

- **Bradley, K. (2006)**
  Risks Associated with the Use of Recordable CDs and DVDs as Reliable Storage Media in Archival Collections–Strategies and Alternatives
  http://unesdoc.unesco.org/images/0014/001477/147782e.pdf
  Memory of the World Programme, Sub-Committee on Technology, United Nations Educational, Scientific and Cultural Organization (UNESCO)

- **British Standards Institution (2008)**
  BS 10008 Evidential Weight and Legal Admissibility of Electronic Information–Specification
  British Standards Institution

- **Brown, A. (2008)**
  Digital Preservation Guidance Note 1: Selecting File Formats for Long-term Preservation
  http://www.nationalarchives.gov.uk/documents/selecting-file-formats.pdf
  The National Archives (United Kingdom)

- **Brown, A. (2008)**
  Digital Preservation Guidance Note 2: Selecting Storage Media for Long-term Preservation
  http://www.nationalarchives.gov.uk/documents/selecting-storage-media.pdf
  The National Archives (United Kingdom)

- **Brown, A. (2008)**
  Digital Preservation Guidance Note 3: Care, Handling and Storage of Removable Media
  http://www.nationalarchives.gov.uk/documents/information-management/removable-media-care.pdf
  The National Archives (United Kingdom)

- **Cornell University Library (2005)**
  Digital Preservation Management: Implementing Short-term Strategies for Long-term Problems, Online Tutorial Developed for the Digital Preservation Management Workshop
  http://dpworkshop.org/dpm-eng/eng_index.html
  Cornell University Library

- **International Organization for Standardization (2005)**
  Technical Report ISO/TR 18492 Long-term Preservation of Electronic Document-based Information (ISO/TR 18492:2005(E))
  International Organization for Standardization

- **The International Research on Permanent Authentic Records in Electronic Systems (InterPARES) Project (2007)**
  Creator Guidelines Booklet—Making and Maintaining Digital Materials: Guidelines for Individuals
  http://www.interpares.org/ip2/display_file.cfm?doc=ip2(pub)creator_guidelines_booklet.pdf
  InterPARES Project

- **The International Research on Permanent Authentic Records in Electronic Systems (InterPARES) Project (2007)**
  Preserver Guidelines Booklet—Preserving Digital Records: Guidelines for Organisations
  http://www.interpares.org/ip2/display_file.cfm?doc=ip2(pub)preserver_guidelines_booklet.pdf
  InterPARES Project

- **Millar, L. (Ed.) (2009)**
  Training in Electronic Records Management Module 4—Preserving Electronic Records
  http://irmt.org/documents/educ_training/term%20modules/IRMT%20TERM%20Module%204.pdf
  International Records Management Trust

- **National Archives of Australia**
  Preserving Digital Records
  http://naa.gov.au/records-management/agency/preserve/e-preservation/index.aspx

- **The National Archives (2008)**
  Digital Preservation Guidance Note 4: Graphic File Formats
  http://www.nationalarchives.gov.uk/documents/information-management/graphic-file-formats.pdf
  The National Archives (United Kingdom)

- **Shipman, A. (2008)**
  Evidential Weight and Legal Admissibility of Information Stored Electronically: Code of Practice for the Implementation of BS 10008 (4th Ed.)
  British Standards Institution

- **Shipman, A. and Howes, P. (2008)**
  Evidential Weight and Legal Admissibility of Information Transferred Electronically: Code of Practice for the Implementation of BS 10008 (4th Ed.)
  British Standards Institution