DISPOSAL OF ORIGINAL RECORDS

(FOR RECORDS THAT HAVE BEEN DIGITISED AND STORED IN A DIGITAL FORM)

Government Records Service
Revised April 2017 (with minor updates in November 2020)

Table of Contents

Revision History			
Version	Reason for change	Sections affected	Date
1	--	--	
2	(a) To introduce procedures for destruction of original records digitised and managed in an electronic recordkeeping system (b) To reduce the number of questions in the original risk analysis checklist in Annex 3 with reference to implementation experience and latest international best practices	3, 4, 7-11 Annex 3	April 2017
3	Minor update to terminology to align with government regulations	Annex 3	November 2020

Part 1
Introduction

1. Purpose

1.1 With a growing trend towards digitisation of records and preference of bureaux and departments (B/Ds) to rely on the digitised records in lieu of the original records for different purposes, this document sets out -

(a) the essential issues to be considered by B/Ds on early destruction of original records after digitisation; and

(b) the proper procedures for seeking agreement for such destruction from the Government Records Service (GRS).

2. Key Concepts

2.1 In the context of this document, an **original record** refers to a non-electronic record (e.g. a cassette tape, a letter or a microfilm) in its original form and such record has been separately digitised and stored in a digital form. The digitised version of the original record (hereafter referred to as the **digitised record** unless specified otherwise) is normally managed and stored in an information system, including an electronic recordkeeping system (ERKS)[1], or stored in an electronic storage medium for off-line and/or off-site storage (e.g. a Write-Once-Read-Many (WORM) optical disk or a compact disk (recordable) (CD-R)).

2.2 **Early destruction** denotes the destruction of original records after digitisation and before the expiry of the retention period specified in the approved records retention and disposal schedules for the original records or, in case a records retention and disposal schedule(s) has <u>not</u> been drawn up for the original records, destruction of the original records prior to disposal of the associated digitised records. The implication is that the digitised records will be relied upon in lieu of

[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.

the original records for all purposes.

2.3 The definitions of other key terms used in this document are set out at **Annex 1**.

3. Scope and Periodic Update

3.1 The procedures set out in Part 3 of this document for seeking agreement from GRS for early destruction of original records are applicable to original records which are digitised and managed in an ERKS. Those set out in Part 4 are applicable to original records which are digitised and stored in an electronic storage medium or managed in an information system other than an ERKS.

3.2 B/Ds should note that original records possessing archival value or potential archival value (i.e. those with disposal action "Permanent retention in Public Records Office", "Review by Public Records Office" or "Review by Agency and Public Records Office" as specified in GRS' Records Management (RM) Publication No. 4 - *General Administrative Records Disposal Schedules* (GARDS)[2] for administrative records or the approved records retention and disposal schedules for programme records) should be appraised and/or transferred to the Public Records Office. Except under very exceptional circumstances and with the prior agreement of the GRS Director, these original records should not be destroyed. B/Ds should also note that all government records reaching 30 years old should be appraised by the Public Records Office to determine whether or not they possess archival value. The procedures set out in Parts 3 and 4 of this document therefore are **not applicable** to these records possessing archival value or potential archival value.

3.3 This document focuses on the early destruction of original paper records as they are the major non-electronic record type in B/Ds and are most likely to be digitised. Nevertheless, the issues to be considered by B/Ds as set out at **Annexes 2 and 3** are largely applicable to the early destruction of non-electronic records in other forms such as microfilms, audio recordings and video recordings.

3.4 This document will be updated from time to time having regard to

[2] The GARDS is accessible at http://grs.host.ccgo.hksarg/cgp_publications.html.

implementation experience and the latest international best practices in this regard.

Part 2
Destruction of Original Records

4. Background

4.1 Although many records are created or received in digital format in the information era, non-electronic records will co-exist with electronic records for various reasons. In such a hybrid RM environment, B/Ds need to simultaneously manage electronic and non-electronic records created and received during the course of official business and keep them as evidence of policies, decisions, procedures, functions, activities and transactions.

4.2 In recent years, B/Ds have increasingly adopted digitisation to convert non-electronic records, particularly paper records, into a digital form through scanning or other means. The perceived benefits of using digitised records in business operations include -

(a) improving searchability and facilitating faster retrieval of records;

(b) facilitating concurrent access to and efficient transmission/distribution of records;

(c) supporting greater integration of RM activities with business processes (e.g. enabling the use of digitised records within a workflow facility to support business operation);

(d) reducing wear and tear of the original records; and

(e) reducing storage costs for non-electronic records (provided that they are no longer needed and can be disposed of after digitisation).

4.3 In view of the intrinsic advantages of digitised records in searchability, accessibility and transmission, B/Ds tend to rely on digitised records increasingly to conduct business operations. Arising from the digitisation of non-electronic records, B/Ds need to consider how the original records and the associated digitised records should be managed, including their retention and disposal. As far as the retention and disposal of the original records and the digitised records are concerned, there are three scenarios as follows -

(a) B/Ds keep the original records and the associated digitised records for the full retention period in accordance with the approved records retention and disposal schedules governing the original records and then dispose of them simultaneously;[3]

(b) B/Ds keep the digitised copies as a dispensable subsidiary to the original records (e.g. serving as duplicated copies of vital records).[4] The digitised copies are disposed of when they are no longer needed while the original records are retained and disposed of in accordance with the approved records retention and disposal schedules; or

(c) B/Ds keep the digitised records in place of the original records, retain and dispose of the digitised records in accordance with the approved records retention and disposal schedules. The original records are to be destroyed as soon as practicable after digitisation and before the expiry of the approved retention period to save records storage costs and maintenance efforts.

4.4 This document deals with the early destruction of original records set out in paragraph 4.3(c) above.

5. Risks of Destruction of Original Records

5.1 Although it may seem logical on efficiency grounds to destroy original records immediately after their digitisation and to use the digitised records in their stead, the full implications of early destruction of original records should be thoroughly and carefully assessed to safeguard the Government's interests.[5] Government records are valuable resources and vital assets to support effective decision making, meet operational requirements and protect the legal, financial and other interests of the Government and the public. They are the essential ingredients for internal and public accountability. A prudent approach should be adopted to

[3] B/Ds should determine which is the most authoritative record of the matters documented if both the original record and the associated digitised record are to be used and retained for the full retention period.

[4] Under this scenario, the original records continue to serve as the most authoritative record for conduct of business. The digitised copies of the original records are not normally used for conduct of business nor serve as evidence of official transactions.

[5] It is to the best interests of the B/D concerned to assess, **prior to** implementing a digitisation programme, the implications of early destruction of original records, notably whether such destruction will contravene legal requirements and what measures should be taken to enhance the evidential weight of the digitised records.

assess the risks associated with early destruction of original records, particularly with reference to possible adverse impacts on the legal, business, evidence and accountability needs of the Government.

5.2 Generally speaking, there are a number of risks associated with early destruction of original records. The major ones include -

(a) contravention of legal and regulatory requirements, government policy or directive;

(b) detriment to the business (e.g. operational) and accountability needs of the Government as a whole, other B/Ds and the B/D itself;

(c) detriment to the evidence needs of the Government which requires evidence that is legally admissible and carries as much evidential weight as possible. In order to serve as reliable evidence, a record must possess the attributes, namely, content, context and structure and be authentic, complete, reliable and usable. Electronic records, including digitised records, can be easily manipulated, deleted and altered without being discovered. As the digitised records will become the only evidence of official transactions if the original records are destroyed, the authenticity, integrity, reliability and usability of the digitised records may be challenged in a court of law if there are suggestions of tampering, incompetence, improper system functionality or malfunction of the information system, etc. The challenges can lead to an investigation into the information system from which the records came, including the method of storage, practices, procedures and processes of system management and operations, etc.; and

(d) digitised records being rendered inaccessible due to technological obsolescence of hardware, operating systems, storage media and software applications; media fragility and physical damage to hardware and storage media.

6. Objectives of Risk Analysis

6.1 In view of the risks associated with early destruction of original records, a B/D should conduct a risk analysis, prior to seeking agreement from GRS for the destruction, to examine -

(a) whether the early destruction of original records will contravene any legal and regulatory requirements, government policy or directive;

(b) whether the original records are required to meet business and accountability requirements of the Government as a whole, other B/Ds and the B/D itself;

(c) the likelihood of the original records being required for on-going or anticipated legal proceedings. The B/D should take into account the likelihood, if a legal case proceeds, that the case will be decided on documentary evidence as opposed to other forms of evidence;

(d) the likelihood as to whether the authenticity, integrity, reliability and usability of digitised records may be challenged in a court of law thereby reducing their legal admissibility or weight as evidence; and

(e) the capability of the B/D to ensure and demonstrate the authenticity, integrity, reliability and usability of digitised records for as long as required (so as to maximise their legal admissibility and evidential weight if being challenged in a court of law and to meet continuous legal, business, evidence and accountability needs).

6.2 The B/D should also evaluate the adverse impacts and consider appropriate actions and measures to eliminate or mitigate the risks identified (e.g. strengthening the quality assurance work of digitised records).

Part 3
Seeking Agreement for Early Destruction of Original Records Digitised and Managed in an ERKS

7. Conducting a Risk Analysis

7.1 To facilitate B/Ds to carry out the risk analysis, a checklist relating to the issues detailed in paragraph 6.1 above is set out at **Annex 2**. B/Ds should use the checklist to assess the risks associated with the proposed early destruction, notably the legal and regulatory requirements, the business and accountability needs as well as the effectiveness of the management and operation of the ERKS implemented. In addition to the major considerations set out in the checklist, B/Ds may include other items to address their specific needs.

7.2 In conducting the risk analysis, a B/D should consider not only the risks associated with the destruction and the possible adverse impacts on itself but also the interests[6] of the Government as a whole and of other B/Ds as far as possible.

8. Responsibility for Conducting Risk Analysis

8.1 The B/D concerned should assign an officer not below the rank of **Senior Executive Officer** (SEO) or equivalent to conduct the risk analysis set out at **Annex 2**. In assessing those issues set out at **Annex 2**, the responsible officer should consult relevant stakeholders, including the Head of Information Technology Management Unit (ITMU) on IT issues such as system security and management of information systems, Departmental Records Manager (DRM) on RM issues and subject officers of the records concerned on the use of original and digitised records. Their views and comments, if any, should be properly documented in Part III of **Annex 2** to facilitate the endorsement officer specified in paragraph 8.2 below to scrutinise the outcome of the risk analysis.

[6] B/Ds should note that the interests referred in paragraph 7.2 above take a broader context, which are not limited to actions/measures to be taken to avoid any possible contravention of legal requirements and to enhance the evidential weight of digitised records as stated in footnote 5. For example, the interests may include actions and measures to avoid bringing the public service into disrepute. B/Ds should critically consider the interests having regard to the subject contents of the original records.

8.2 Since early destruction of original records may impose possible adverse impacts on the legal, business, evidence and accountability needs of the B/D concerned and of the Government, it is necessary for B/Ds to designate an officer not below the rank of **Chief Executive Officer** (CEO) or equivalent to endorse the outcome of the risk analysis. Based on the outcome of the risk analysis, the B/D should determine whether the original records have to be retained to serve legal, business, accountability and evidence needs. For legal issues relating to early destruction of original records, B/Ds may seek advice where appropriate from the Department of Justice.

8.3 Having regard to the outcome of the risk analysis, the endorsement officer should also consider, in consultation with relevant stakeholders such as the DRM and Head of ITMU where appropriate, as to whether measures and actions should be taken to eliminate or mitigate the risks identified in the risk analysis.

9. Obtaining Agreement from GRS

9.1 If the B/D is satisfied that, on the basis of the risk analysis, it is justified to destroy the original records before the expiry of the approved retention period governing ~~that~~ those records, it may put up a request in writing to GRS for agreement using Form RC9 (for administrative records) at **Annex 4** or Form RC10 (for programme records) at **Annex 5**. Forms RC9 and RC10 should be endorsed by an officer not below the rank of SEO or equivalent.

10. Management of Original Records Prior to Authorised Disposal

10.1 **B/Ds should <u>not</u> destroy original records after digitisation without the prior agreement of GRS Director**. B/Ds should manage original records properly[7] until their authorised disposal. Upon receipt of GRS' agreement for early destruction of original records, B/Ds may arrange destruction in the normal

[7] It is not recommended for B/Ds to adopt day boxing (the process of accumulating the original records in chronological order, or in their digitisation sequence) to manage original records because it is rarely suited to efficient management and disposal processes given that it eliminates contextual linkages and mixes records intended for short-term retention with record subject to longer retention periods (clause 6.5.4.2 of ISO/TR 13028:2010 (E): *Information and documentation - Implementation guidelines for digitization of records*).

manner (e.g. B/Ds should designate an officer not below the rank of Executive Officer II or equivalent to ensure that the disposal process is properly supervised and the records disposal procedures as set out in Appendix IV to General Circular No. 2/2009 entitled "Mandatory Records Management Requirements" are complied with) and document the destruction properly for record purpose.

11. Handling of Paper Records in an ERKS Setting

11.1 While an ERKS possesses functionality for converting paper records into digital form and managing those digitised records, it is not necessary and usually not practical to digitise all paper records for management in an ERKS setting. B/Ds should consider the legal, security or business reasons (e.g. the copyright issues, records of SECRET security classification whose content should not be digitised and managed in an ERKS) that may prevent B/Ds from digitising the paper records. In order to maximise the benefits of implementing an ERKS, B/Ds should, from efficiency and green perspectives, consider whether paper records should continue to be created upon implementation of an ERKS, and whether the business processes should be re-engineered to minimise the creation of paper records at source.

Part 4
Seeking Agreement for Early Destruction of Original Records Digitised and Stored in Electronic Storage Media or Managed in an Information System (other than an ERKS)

12. Conducting a Risk Analysis

12.1 To facilitate B/Ds to carry out the risk analysis, a checklist relating to the issues detailed in paragraph 6.1 above is set out at **Annex 3** for assessing the risks associated with the early destruction, notably the effectiveness of the records management programme, practices and procedures as well as the information systems that manage and store the digitised records. In addition to the major considerations set out in the checklist, B/Ds may include other items to address their specific needs.

12.2 In conducting the risk analysis, a B/D should consider not only the risks associated with the destruction and the possible adverse impacts on itself but also the interests[8] of the Government as a whole and of other B/Ds as far as possible.

13. Responsibility for Conducting Risk Analysis

13.1 The B/D concerned should assign an officer not below the rank of **SEO** or equivalent to conduct the risk analysis set out at **Annex 3**. In assessing those issues set out at **Annex 3**, the responsible officer should consult relevant stakeholders, including the Head of ITMU on IT issues such as system security and management of information systems, DRM on RM issues and subject officers of the records concerned on the use of original and digitised records. Their views and comments should be properly documented in Part II of **Annex 3** to facilitate the endorsement officer specified in paragraph 13.2 below to scrutinise the outcome of the risk analysis.

[8] B/Ds should note that the interests referred in paragraph 12.2 above take a broader context, which are not limited to actions/measures to be taken to avoid any possible contravention of legal requirements and to enhance the evidential weight of digitised records as stated in footnote 5. For example, the interests may include actions and measures to avoid bringing the public service into disrepute. B/Ds should critically consider the interests having regard to the subject contents of the original records.

13.2 Since early destruction of original records may impose possible adverse impacts on the legal, business, evidence and accountability needs of the B/D concerned and of the Government, it is necessary for B/Ds to designate an officer not below the rank of **CEO** or equivalent to endorse the outcome of the risk analysis. Based on the outcome of the risk analysis, the B/D should determine whether the original records have to be retained to serve legal, business, accountability and evidence needs. For legal issues relating to early destruction of original records, B/Ds may seek advice where appropriate from the Department of Justice.

13.3 Having regard to the outcome of the risk analysis, the endorsement officer should also consider, in consultation with relevant stakeholders such as the DRM and Head of ITMU, as to whether measures and actions should be taken to eliminate or mitigate the risks identified in the risk analysis.

14. Obtaining Agreement from GRS

14.1 If the B/D is satisfied that, on the basis of the risk analysis, it is justified to destroy the original records before the expiry of the approved retention period governing those records, it may put up a request in writing to GRS for agreement with the following supporting information, as well as a request to revise or establish a records retention and disposal schedule(s) set out in paragraphs 14.2 to 14.4 below -

(a) a copy of duly completed risk analysis in the format of **Annex 3**; and

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

Programme Records

14.2 If the original records are programme records and have been covered by an approved records retention and disposal schedule(s), the B/D should submit a request to revise the schedule(s) for GRS' approval through the "Storage Allocation and Records Centre Information System" (SARCIS)[9] in conjunction with the

[9] SARCIS is accessible through the Department Portal of individual B/Ds.

written request for early destruction of original records. In particular, the B/D should provide the following information through SARCIS in the request to revise the records retention and disposal schedule(s) in addition to the other information required -

(a) the original records and the digitised records shown as separate disposal classes falling under the same records series;

(b) the title(s) of the disposal class(es), the proposed retention period, criterion for defining inactive records and disposal action for the **original records**; and

(c) the title(s) of the disposal class(es), the proposed retention period, criterion for defining inactive records and disposal action for the **digitised records**.

14.3 In case the original records to be disposed of are not governed by any approved records retention and disposal schedule(s), the B/D should draw up and submit a draft records retention and disposal schedule(s)[10] to GRS for approval through SARCIS together with the written request for early destruction of original records. The information on paragraph 14.2(a) - (c) above should be clearly set out in the draft records retention and disposal schedule(s).

Administrative Records

14.4 For administrative records, the B/D should draw up and submit a draft records retention and disposal schedule(s) to GRS for approval through SARCIS and provide the following information in the draft schedule(s) to facilitate GRS to process it in conjunction with the written request for early destruction of original records -

(a) stipulated retention period and disposal action of the **digitised records** in accordance with the GARDS; and

(b) the proposed retention period, criterion for defining inactive records and disposal action for the original records.

[10] Please refer to GRS RM Publication No. 1 - *A Practical Guide to Records Scheduling and Disposal* (accessible at http://grs.host.ccgo.hksarg/cgp_publications.html) for procedures to draw up a draft records retention and disposal schedule.

15. GRS' Responsibility

15.1 Upon receipt of a request, GRS will process draft records retention and disposal schedule(s) or proposed amendments to the existing records retention and disposal schedule(s) where appropriate as set out in paragraphs 14.2 to 14.4 above. **B/Ds should <u>not</u> destroy the original records without prior agreement of GRS Director**. This is to safeguard against premature disposal of records and disposal of records having archival value.

15.2 B/Ds should allow a lead time of **about two months** for GRS to process a case, and this may be lengthened for complex cases.

16. Management of Original Records Prior to Authorised Disposal

16.1 B/Ds should manage original records properly[11] until their authorised disposal. In case the original records are required to be kept in conjunction with the associated digitised records for the full retention period in accordance with the approved records retention and disposal schedules governing the original records, B/Ds should ensure that the original records are persistently linked[12] to the digitised ones.

17. Destruction of Original Records

17.1 Upon receipt of GRS' agreement for early destruction of original records in the context of processing the relevant draft records retention and disposal schedules or amendments to those existing schedules covering the original records and the associated digitised records, a B/D may seek GRS Director's prior agreement to destroy the original records by submitting disposal requests through SARCIS upon

[11] It is not recommended for B/Ds to adopt day boxing (the process of accumulating the original records in chronological order, or in their digitisation sequence) to manage original records because it is rarely suited to efficient management and disposal processes given that it eliminates contextual linkages and mixes records intended for short-term retention with record subject to longer retention periods (clause 6.5.4.2 of ISO/TR 13028:2010 (E): *Information and documentation - Implementation guidelines for digitization of records*).

[12] The link between an original record and the associated digitised record is usually documented by using identification methods such as barcoding technology.

the expiry of their retention period as specified in the approved records retention and disposal schedules or approved amendments to existing schedules. The B/D should document the destruction properly for record purposes.[13]

17.2 In case there are changes to the legal, business, accountability and evidence requirements or any other factors that call for a review of the early destruction of the original records, B/Ds should revisit the issue and submit a fresh assessment to GRS, following the procedures set out in paragraphs 18.1 and 18.2 below.

[13] As a best practice set out in clause 6.5.2 of ISO/TR 13028:2010(E): *Information and documentation - Implementation guidelines for digitization of records*, B/Ds should document the authorisation for destruction and the execution of destruction of an original record in the metadata associated with the digitised record.

Part 5
Monitoring and Review

18. Regular Review

18.1 Monitoring and review are essential for managing risks as the likelihood, the magnitude and the possible impacts of risks will change. For cases not involving an ERKS (i.e. Part 4 of this document is relevant), a B/D should monitor and review the risks associated with early destruction of original records according to the issues[14] set out at the prevailing **Annex 3** on a regular basis, say **once every two years** or more often as necessitated by its unique circumstances such as after a relevant court ruling. The results and findings of the review should be properly documented. In particular, the B/D should review whether any changes in system functionality, operation and management of information systems (in which digitised records are managed and stored) will affect the authenticity, integrity, reliability and usability of the digitised records thus reducing their legal admissibility and weight as evidence.

18.2 If after the review, the B/D considers that the early destruction of original records for a particular records series should be revoked in view of legal, business, accountability or evidence requirements, they should document the justifications and discontinue destruction with immediate effect. Afterwards, the B/D should submit a revised records retention and disposal schedule covering the original records to GRS for approval through SARCIS as soon as possible.

18.3 For cases involving an ERKS (i.e. Part 3 of this document is relevant), B/Ds should follow the guidelines set out in Chapter 5 of the ***Manual on Evaluation of an Electronic Recordkeeping System***[15] for on-going use, management and maintenance of their ERKSs.

[14] A B/D should also consider whether there are other relevant issues to be assessed having regard to their specific business needs.

[15] ***Manual on Evaluation of an Electronic Recordkeeping System*** is available at http://grs.host.ccgo.hksarg/erm/s04/4232.html.

19. Removal and Mitigation of Risks

19.1 In the course of conducting the risk analysis set out in paragraph 7.1 or 12.1 or the review set out in paragraph 18.1 above, a B/D may identify imminent and/or potential risks associated with early destruction of original records which, in many cases, can be appropriately dealt with or minimised. The B/D should ensure that timely measures and actions are taken to remove or mitigate the risks and evaluate the effectiveness of these measures before making further consideration for destruction of the original records. Remedial measures and actions taken should be properly documented to demonstrate B/Ds' commitment to and effectiveness of handling risks which in turn will enhance the organisational confidence in making a decision to destroy the original records earlier.

References

Archives New Zealand, ***Digitisation standard*** (2007)

British Standards Institution, BS 10008:2014 ***Evidential weight and legal admissibility of electronic information – Specification***

British Standards Institution, ***Evidential weight and legal admissibility of information stored electronically – Code of practice for the implementation of BS 10008*** (2014)

British Standards Institution, ***Evidential weight and legal admissibility of electronic information – Compliance workbook for use with BS 10008:2014*** (2014)

International Organization for Standardization, ISO 15489-1:2016(E) ***Information and documentation – Records management – Part 1: Concepts and principles***

International Organization for Standardization, ISO/TR 13028:2010(E) ***Information and documentation – Implementation guidelines for digitization of records***

National Archives of Australia, ***Check-Up 2.0*** (2010)

National Archives of Australia, ***Destruction of source or original records after digitisation, conversion or migration*** (2015)

Queensland State Archives, Australia, ***Digitisation Disposal Policy Toolkit – Assessing Eligibility of Paper Records for Early Disposal after Digitisation*** (2014)

Queensland State Archives, Australia, ***Digitisation Disposal Policy Toolkit – Technical Specifications*** (2014)

State Records of South Australia, Australia, ***General Disposal Schedule No. 21 for management and disposal of source documents and digitised versions after digitisation*** (Version 4)

Glossary

Term	Definition
Access	The right, opportunity, or means of finding, using or retrieving information.
Administrative records	Records created or received during the course of day-to-day administrative activities that deal with finance, accommodation, procurement and supplies, establishment, human resources and other general administrative activities.
Audit trail	Data that allows the reconstruction of a previous activity, or which enables attributes of a change (such as date/time, operator (i.e. responsible user)) to be stored so that a sequence of events can be reconstructed in their correct chronological sequence.
Authenticity	An authentic record is one that can be proven to (a) be what it purports to be; (b) have been created or sent by the agent purported to have created or sent it; and (c) have been created or sent when purported. [Internal note: Amended to follow ISO 15489-1:2016.]
Bit depth	The number of bits used to describe the colour of each pixel. Greater bit depth allows a greater range of colours or shades of grey to be represented by a pixel. [Internal note: Adopted from **Digitisation Disposal Policy Toolkit - Technical Specifications**.]
Capture (verb)	Capturing records is used to mean all of the processes involved in getting a record into an information system, including an electronic recordkeeping system (e.g. registration, classification and addition of metadata).
Colour management	Means of attempting to ensure that the image looks the same across a range of different output devices (e.g. printers and monitors).
Compression	Process of reducing the size of a data file (usually an image) by the use of a computerised algorihm that encodes redundnat information into a more compact form [Internal note: Follow ***Evidential weight and legal admissibility of information stored electronically – Code of practice for the implementation of BS 10008 (2014)***. Previous version was adopted from the guidelines of ERKS pilot project.] (a)
Content	Information or ideas the record contains.

Term	Definition
Context	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).
Destruction	Process of eliminating records, beyond any possible reconstruction.
Digital	In the context of this document, the word "digital" is used to mean the same as "electronic".
Digitisation	Process of converting a non-electronic record (e.g. a paper record, a photograph and an audio recording) into an electronic representation. Examples of digitisation include scanning or imaging, taking digital photographs of the original records, or converting analogue voice recordings to digital media. [Internal note: Follow RKMS.]
Digitised record	A record which is converted from a paper document, a microfilmed document or other records (e.g. a cassette tape) into a digital form. [Internal note: Follow RKMS.]
Document (noun)	Recorded information or object which can be treated as a unit. *Note: A document may be on paper, microform, magnetic or any other electronic medium. It may include any combination of text, data, graphics, sound, moving pictures or any other forms of information. A single document may consist of one or several components. Documents differ from records in several important respects. The term is used to mean information that has not been captured as a record.*
Electronic record	A record generated in digital form by an information system, which can be (a) transmitted within an information system or from one information system to another, and (b) stored in an information system or other medium. (Electronic Transactions Ordinance (Cap. 553))
Electronic recordkeeping system (ERKS)	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.

Term	Definition
Electronic storage media	In the context of this document, they mean memory devices in computers (e.g. hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory medium, in which the digitised records are stored for off-line and/or off-site storage.
File format	The internal structure and/or encoding of a record or component which allows it to be presented into human-accessible form. *Note: Examples include -* *a) TIFF (a bit-mapped format for graphics);* *b) PDF/A v1 (an archival file format for portable documents);* *c) TXT (ASCII plain text file format);* *d) XML v1.0 (a file format for extensible markup language which itself relies on ASCII plain text); and* *e) Many proprietary file formats produced by desktop applications such as office suites.*
Government record	A government record is any recorded information in any physical format or media created or received by a bureau/department (B/D) during its course of official business and kept as evidence of policies, decisions, procedures, functions, activities and transactions.
Greyscale	Black and white in addition to a range of intermediate greys. [Internal note: Adopted from **Digitisation Disposal Policy Toolkit - Technical Specifications**.]
	[Item removed]
Inactive records	Records which are no longer required or rarely required for the conduct of business or reference. [Internal note: Adopted from P1 without mentioning of intermediate storage.]
Information system	The infrastructure, processes, and technologies used to store, generate, manipulate, and transmit information to support an organisation.
Integrity	A record that has integrity is one that is complete and unaltered. [Internal note: Amended to follow ISO 15489-1:2016.]

Term	Definition
Lossless compression	Data file compression technique where the decompressed image is identical to the original uncompressed image. [Internal note: Follow ***Evidential weight and legal admissibility of information stored electronically – Code of practice for the implementation of BS 10008 (2014)***. Previous version was copied erroneously from a previous version of the document.]
Lossy compression	Data file compression technique where the decompressed image may not be identical to the original uncompressed image. [Internal note: Follow ***Evidential weight and legal admissibility of information stored electronically – Code of practice for the implementation of BS 10008 (2014)***. Previous version was copied erroneously from a previous version of the document.]
Metadata	Literally defined as "data about data". In the records management context, they are data describing the context, content and structure of records and their management through time. Metadata will accrue during the life cycle of records.
Migration	Moving records from one system environment to a newer environment. This may include any combination of - (a) rendering (converting to a new file format); and (b) copying to a new kind of storage medium, or to a new instance of the same kind of storage medium, without changing file format (the latter is sometimes referred to as refreshing) [Internal note: Follow RKMS. This term appears in the risk assessment checklist in Annex 3 only. The original version of the definition is an adapted version of ISO 15489-1:2001 which was "Act of moving records from one system to another, while maintaining the records' authenticity, integrity, reliability and useability". The definition of "migration" in ISO 15489-1:2016 has been amended to "Process of moving records from one hardware or software configuration to another without changing the format". We consider that adopting the definition in RKMS, which is in a broader sense including the migration of system, medium and format, would be more suitable in the context of conducting a risk assessment.]
Non-electronic record	A record that is in hardcopy form such as paper record, microfilm and audio recording.

Term	Definition
Original record	In the context of this document, an original record refers to the non-electronic record (e.g. a cassette tape, a letter and a microfilm in its original form), and such record has been separately digitised and stored in a digital form.
Programme records	Records created and 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.
Record (noun)	In the context of this document, a record refers to a government record. *Note: A key feature of a record is that its contents cannot be changed.*
Records retention and disposal schedule	A systematic listing or description of an organisation's records which indicates the arrangements to be made for their custody, retention, and final disposition. *Note: Records retention and disposal schedules of programme records of B/Ds should be drawn up with the concurrence of the GRS Director. For the records retention and disposal schedules of administrative records, please refer to GRS' Records Management Publication No. 4 – General Administrative Records Disposal Schedules.*
Reliability	A reliable record is one (a) whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest; and (b) which can be depended upon in the course of subsequent transactions or activities. [Internal note: Amended to follow ISO 15489-1:2016.]
Resolution	A measure of the ability to capture detail in the original work, often quantified in pixels per inch (ppi).
Retention period	The time the records are to be kept after the records become inactive but before their final disposal.
Risk analysis	A systematic use of available information to determine how often specified events may occur and their likely consequences. The purpose of risk analysis is to identify the causes, effects and magnitude of risk and provide a basis for risk assessment and treatment.

Term	Definition
Scanning	A digitisation process that converts the image of a document into a digital form, by detecting the amount of light reflected from elements of a document.
Structure	Physical and/or logical format of the record, and the way parts of the record relate to each other (e.g. the structure of an e-mail record covers its header, body, attachments and corresponding reply).
Usability	A usable record is one that can be located, retrieved, presented and interpreted within a time period deemed reasonable by stakeholders. [Amended to follow ISO 15489-1:2016.]

Risk Analysis Checklist for Early Destruction of Original Records which have been Digitised and Managed in an Electronic Recordkeeping System

(Please read the Explanatory Notes at the end before completing this checklist)

Part I: General Information

Bureau / Department (B/D)	
Branch / Division / Section / Office	
^Our Ref.	

^ *This reference no. should match with that in the disposal request*

Part II: Checklist

Notes

1. Please tick "✓" as appropriate. Questions marked with an asterisk (*) (i.e. Questions 11 - 14 and 16) have been designed to the effect that answers to those questions where applicable are expected to be in the **affirmative** while for the other questions, answers to them where applicable are expected to be in the **negative**.

2. The meanings of the key terms used in the checklist are set out below -

    (a) "**original records**" means the non-electronic records in their original form and such records have been separately digitised and stored in an electronic recordkeeping system (ERKS);

    (b) "**digitised records**" means the digitised versions of the original records mentioned in (a) above; and

    (c) "**system**" means the ERKS used to manage and store the digitised records mentioned in (b) above.

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
1.	Will the destruction of the original records contravene any legal and/or regulatory requirements?				If the answer to this question is "Yes", the B/D should list the relevant legal and/or regulatory requirements and retain the original records. If in doubt, the B/D should seek legal advice as appropriate.
2.	Will my B/D breach any legislation or regulatory requirements if the original records are not maintained in a specific form (i.e. in paper form)? [Note: Where the Electronic Transactions Ordinance (Cap. 553) (ETO) applies to the original records and the associated digitised records, B/Ds should pay particular attention to sections 5A, 6, 7 and 8 of ETO. Sections 7 and 8 of ETO set out the circumstances under which a legal requirement for "presentation or retention of information in its original form" is satisfied by presenting or retaining the information in electronic form. In case of doubt, B/Ds should consult OGCIO and DoJ as appropriate.]				

		Yes	No	Not Applicable (Please provide reasons)	
3.	Does my B/D rely on, or is likely to require (e.g. the likelihood of the original records being required for on-going or anticipated legal proceedings) the original records as evidence in a court of law?				If the answer to this question is "Yes", the B/D should retain the original records.
4.	Will the interests of the Government, other B/Ds and/or my B/D in any on-going or anticipated legal action be adversely affected by the destruction of the original records?				If the answer to this question is "Yes", the B/D should retain the original records until and unless the relevant risk is removed. If in doubt, the B/D should seek legal advice as appropriate.
5.	(a) Are the nature and legal effect of the original records (e.g. contracts, title deeds, power of attorney, declarations, etc.) essential for legal or business purposes of the Government, other B/Ds and/or my B/D? (b) Will the original records be required or are likely to be required (e.g. it is likely to require the original records if they are the only ones that can substantiate the interests of the B/D) as evidence when disputes arise?				
6.	(a) Do the original records contain seals, watermarks or other features that cannot be reproduced adequately? (b) Are such features (if any) essential for legal or business purposes, policies and procedures?				

		Yes	No	Not Applicable (Please provide reasons)	
	[Note: An original record can be useful in some circumstances, e.g. for detection of fraud. Signs of forgery detectable in the original record may not be carried over into a digitised record. B/Ds should identify key records that might be the subject of fraud and which contain signatures, seals, watermarks or other features that authenticate the records.]				
7.	(a) Is there any **high risk** of the authenticity, integrity and reliability of the digitised records being subject to challenges in legal proceedings with possible adverse effects? (b) Are the risks of challenge identified at (a) above assessed to be **unacceptable** to my B/D? [Note: This refers to an assessment of the possibility of litigation, having regard to both past pattern and the nature of the issues relating to the records.]				If the answer to this question is "Yes", the B/D should retain the original records.
8.	Will the destruction of the original records contravene any government policy or directive?				If the answer to this question is "Yes", the B/D should list the relevant government policy or

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
					directive and retain the original records. If in doubt, the B/D should seek the advice of the relevant policy authority.
9.	Are there any business requirements to retain the original records? [Note: Graphical materials such as posters, leaflets, designs and brochures may need to be retained in their original format for display. Moreover, where the original record contains physical amendments or annotations that cannot be identified as such on the digitised image, B/Ds should consider whether the original records should be retained.]				
10.	Are the original records still being retrieved and used for the conduct of business? [Note: B/D should also consider the frequency and circumstances of retrievals in judging whether the original records should be retained.]				If the original records are still retrieved by users in conduct of business, the B/D should consider whether the digitised records can be relied upon in lieu of the original records for all purposes.

	S/N	Issues	Results			Remark
			Yes	No	Not Applicable (Please provide reasons)	
*	11.	Are users relying on the digitised records primarily in the normal conduct of business?				If the answer to this question is "No", the B/D should consider whether the digitised records can be relied upon in lieu of the original records for all purposes.
*	12.	Has my B/D conducted an evaluation of its electronic recordkeeping system in the context of system acceptance in accordance with the ***Manual on Evaluation of an Electronic Recordkeeping System*** (Manual), and achieved "full compliance" as prescribed in paragraph 2.18 of the Manual for the system and a "good" rating as prescribed in paragraph 2.21 of the Manual in respect of its performance and effectiveness in implementing and enforcing departmental RM policies, practices and procedures governing the use, management and maintenance of the system?				If the B/D has not achieved the said "full compliance" and "good" ratings, the B/D should not destroy the original records for the time being and should make timely improvements to its system and/or departmental RM policies, practices and procedures as appropriate.

	S/N	Issues	Results			Remark
			Yes	No	Not Applicable (Please provide reasons)	
*	13.	Has my B/D obtained the agreement of GRS to dispense with the "print-and-file" practice?				If the answer to this question is "No", the B/D should not destroy the original records for the time being and should submit a request in accordance with the Manual to seek GRS' agreement to dispense with the "print-and-file" practice on the basis of the results of a compliance assessment.

	S/N	Issues	Results			Remark
			Yes	No	Not Applicable (Please provide reasons)	
*	14.	Has my B/D conducted a fresh compliance assessment <u>after</u> the evaluation in the context of system acceptance, and achieved "full compliance" and "good" ratings as prescribed in paragraphs 2.18 and 2.21 of the Manual respectively? [Note: Compliance assessment of an electronic recordkeeping system 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.]				If the answer to this question is "Yes", the B/D should state the date when the last compliance assessment was conducted. If the B/D has not conducted a compliance assessment in the past four years, the B/D should not destroy the original records for the time being and should conduct a fresh compliance assessment.
	15.	Has any of the following occurred after the last compliance assessment - ▪ identified cases of serious non-conformity to departmental RM practices and procedures; ▪ identified incidents of serious security breach; ▪ major upgrade, revision or supplement to the hardware, software and/or the functionality of the system; or ▪ substantial revisions or update to the departmental RM policies, practices and procedures governing the use, management and maintenance of the system?				

	S/N	Issues	Results			Remark
			Yes	No	Not Applicable (Please provide reasons)	
*	16.	In connection with Question 15, has my B/D conducted a fresh compliance assessment after such events and achieved “full compliance” and “good” ratings as prescribed in paragraphs 2.18 and 2.21 of the Manual respectively?				If the B/D has not conducted a compliance assessment after such major changes or serious incidents, the B/D should not destroy the original records for the time being and should conduct a fresh compliance assessment.
	Other Issues Specific to the B/D [Note: The B/D should consider whether there are issues specific to their business environment and add the identified issues.]					
	17.					

Part III: Outcome of the Risk Analysis

Based on the outcome of the risk analysis in Part II above, I consider that the risks associated with early destruction are *acceptable / unacceptable to my B/D. I *am / am not satisfied that early destruction of the original records will **not** -

(a) contravene any legal and regulatory requirements, government policy or directive;

(b) jeopardise the Government's interests in any known or anticipated legal proceedings; and

(c) jeopardise or place unreasonable risks on the interests (including business, accountability and evidence needs) of the Government as a whole, other B/Ds and my B/D.

2. *I have consulted the relevant stakeholders and their views are as follows -

_____

_____

3. I recommend that -

*(a) the original records under review can be destroyed.

*(b) the following actions should be taken to mitigate the risks of early destruction:

_____

_____

Name of officer	
Post Title	
Rank[#]	
Date	

[#] *The risk analysis should be conducted by an officer not below the rank of Senior Executive Officer or equivalent.*

** Delete as appropriate*

Part IV: Endorsement

I *endorse / do not endorse the outcome of the risk analysis in Part III above. I agree that -

*(a) the original records under review can be destroyed.

*(b) the following actions should be taken to mitigate the risks of early destruction:

_____

_____

Name of officer	
Post Title	
Rank[#]	
Date	

[#] *The outcome of the risk analysis should be endorsed by an officer not below the rank of Chief Executive Officer or equivalent.*

** Delete as appropriate*

Explanatory Notes

Purpose of the checklist

This checklist supplements the procedures set out in the guidance document entitled "Disposal of Original Records (for records that have been digitised and stored in a digital form)" for cases where the original records are digitised and managed in an ERKS.

Applicability of the checklist

2. This checklist is applicable to cases where the original records -

(a) which have been digitised and managed in an ERKS of the B/D concerned and the associated digitised records will be stored and managed in the ERKS not shorter than the retention period specified in GRS' RM Publication No. 4 - General Administrative Records Disposal Schedules (GARDS) for administrative records or the approved records retention and disposal schedules established for programme records;

(b) whose disposal action is "Destroy" as specified in the GARDS for administrative records or the approved records retention and disposal schedules for programme records; and

(c) the ERKS of the B/D concerned has passed the evaluation in accordance with the guidelines entitled ***Manual on Evaluation of an Electronic Recordkeeping System***[1].

3. For the avoidance of doubt, original records whose disposal action is "Permanent retention", "Review by Public Records Office" or "Review by Agency and Public Records Office" as specified in the GARDS or the approved records retention and disposal schedules should not be destroyed even if the associated digitised records are stored and managed in an ERKS. This checklist is also not applicable for the destruction of original records of new series of programme records without an approved retention and disposal schedule.

4. If the original records proposed to be destroyed fall within a specific records

[1] ***Manual on Evaluation of an Electronic Recordkeeping System*** is available on the Central Cyber Government Office (http://grs.host.ccgo.hksarg/erm/s04/4232.html).

series (instead of spreading over many different records series) and the frequency of arranging such destruction is high (e.g. quarterly), the B/D concerned may consider adopting the procedures set out in Part 4 of the main body of the guidance document to revise the approved records retention and disposal schedule, instead of using this checklist.

Scope and responsibility

5. Prior to seeking GRS' agreement for early destruction of original records after they have been digitised and managed in an ERKS, B/Ds are required to evaluate the essential issues set out in Part II of this checklist in respect of the original records under review.

6. B/Ds should designate an officer not below the rank of **Senior Executive Officer or equivalent** to conduct the risk analysis and complete Parts II and III of the checklist. The completed risk analysis should be endorsed by an officer not below the rank of **Chief Executive Officer or equivalent** by completing Part IV of the checklist. The endorsement officer should not be the same person as the officer conducting the risk analysis. The officers should read carefully the main body of the guidance document before completing the checklist.

Risk analysis checklist

7. Questions 1 - 10 and 15 of the risk analysis checklist have been designed to the effect that their answers where applicable are expected to be in the **negative**, while the answers to Questions 11 - 14 and 16 where applicable are expected to be in the **affirmative** so as to demonstrate that the B/D concerned has adhered to the best practices in the specific areas.

8. B/Ds should bear in mind that there are no hard and fast rules to determine a maximum or an appropriate level of risks that a B/D can tolerate having regard to the various factors, including the importance of original records to the business operation, the likelihood, the magnitude and the possible impacts of risks. In general, the more responses to Part II fall in the expected category (i.e. affirmative or negative) in accordance with paragraph 7 above, the higher the confidence of the B/D should be able to satisfy itself that the risks of early destruction of original records will be minimised while the evidential weight of digitised records will be maximised.

Seeking agreement from GRS

9. Upon completion of a risk analysis, the relevant B/D may proceed to seek GRS' agreement for early destruction of the original records if it is satisfied that, based on the outcome of the risk analysis, such destruction -

(a) will not contravene any legal and regulatory requirements, government policy or directive;

(b) will not jeopardise the Government's interests in any known or anticipated legal proceedings; and

(c) will not jeopardise or place unreasonable risks on the interests (including business, accountability and evidence needs) of the Government as a whole, other B/Ds and the relevant B/D.

10. In addition to the above, the relevant B/D should satisfy itself that it is able to ensure and demonstrate with clear evidence the required degree of authenticity, integrity, reliability and usability of the digitised records as complete substitute for the original records for meeting continuous legal, business, accountability and evidence needs.

11. Since the original records under review may spread over a number of records series, a fresh risk analysis checklist should be completed and endorsed for each disposal request. The completed and endorsed risk analysis checklist should be properly kept by the relevant B/D but need not be submitted to GRS to seek agreement for early destruction of the original records. GRS may conduct sample check of the risk analysis checklist if necessary.

Risk Analysis Checklist for Early Destruction of Original Records which have been Digitised and Stored in Electronic Storage Media or Managed in an Information System (other than an Electronic Recordkeeping System)

Preamble

Prior to seeking GRS' agreement for early destruction[1] of original records after digitisation with a view to relying on the digitised records in lieu of the original records for all purposes, bureaux and departments (B/Ds) are required to evaluate the essential issues set out in Part II of this checklist.

2. All questions set out in Part II **except for** the following ones **have been designed to the effect that answers to those questions where applicable are expected to be in the affirmative so as to demonstrate that the B/D concerned has adhered to the best practices in the specific areas** -

(a) questions 1 to 7 relating to legal and regulatory requirements and related issues;
(b) questions 8 to 10 relating to business, accountability and evidence issues; and
(c) questions 30 and 31 relating to system security.

For those questions listed in paragraph 2(a) - (c) above, answers to them where applicable are expected to be in the **negative**.

3. B/Ds should bear in mind that there are no hard and fast rules to determine a maximum or an appropriate level of risks that a B/D can tolerate having regard to the various factors, including the importance of original records to the business operation, the likelihood, the magnitude and the possible impacts of risks. In general, the more responses to Part II fall in the expected category (i.e. affirmative or negative) in accordance with paragraph 2 above, the higher the confidence of the B/D should be able to satisfy itself that the risks of early destruction of original records will be

[1] Please see the definition of early destruction in paragraph 2.2 of the main body of the document.

minimised while the evidential weight of digitised records will be maximised.

4. Upon completion of a risk analysis, the relevant B/D may proceed to seek GRS' agreement for early destruction if it is satisfied that, based on the outcome of the risk analysis, such destruction -

(a) will not contravene any legal and regulatory requirements, government policy or directive; and

(b) will not jeopardise the Government's interests in any known or anticipated legal proceedings; and

(c) will not jeopardise or place unreasonable risks on the interests (including business, accountability and evidence needs) of the Government as a whole, other B/Ds and the relevant B/D.

5. In addition to the above, the relevant B/D should satisfy itself that it is able to ensure and demonstrate with clear evidence the required degree of authenticity, integrity, reliability and usability of the digitised records as complete substitute for the original records for meeting continuous legal, business, accountability and evidence needs.

Notes

(1) An officer not below the rank of **Senior Executive Officer** or equivalent should be assigned to complete Parts I to III of the checklist. He/she should read carefully the main body of the document "Disposal of Original Records (for Records that have been Digitised and Stored in a Digital Form)" before completing the checklist. He/she should tick the column "Not applicable" next to the relevant question and document the rationale if the issue to be assessed therein is irrelevant to the request.

(2) **The checklist should be endorsed by an officer not below the rank of Chief Executive Officer or equivalent**.

(3) The meaning of the key terms used in Parts I and II of the checklist are set out below -

(a) "**original records**" means the non-electronic records in their original form

and such records have been separately digitised and stored in a digital form;

(b) "**digitised records**" means the digitised versions of the original records mentioned in (a) above;

(c) "**system**" means the information system (other than an electronic recordkeeping system (ERKS)) used to manage and store the digitised records mentioned in (b) above; and

(d) "**electronic storage medium**" means the medium, e.g. an optical disk in which the digitised records mentioned in (b) above are stored for off-line and/or off-site storage.

(4) The responsible officer should copy the completed Parts I to III to the Departmental Records Manager (DRM) and Head of Information Technology Management Unit (ITMU) for information prior to seeking endorsement of the outcome of the risk analysis.

Part I : General Information

Name of bureau or department : _____

Purpose of Conducting the Risk Analysis

1. Please choose one of the following by ticking ("✓") the appropriate box -

   ☐ seek agreement for early destruction of original records for the first time and a records retention and disposal schedule need to be established/amended;

   ☐ review a records retention and disposal schedule authorising early destruction of original records after a lapse of **two years**; or

   ☐ review a records retention and disposal schedule authorising early destruction of original records as necessitated by major events set out in paragraph 18.1 of the main body of the document "Disposal of Original Records (for Records that have been Digitised and Stored in a Digital Form)".

Information on Original Records

2. Disposal Authority No. (if any) : _____

3. Records series title of the original records being proposed for destruction:

   _____

4. Disposal classes (for complex series only):

   _____

5. Subject matter of the records series:

   _____

Note

The information requested above can be found in the approved records retention and disposal schedule(s) (i.e. RMO2 - *Records Retention and Disposal Authority*) governing the disposal of the original records. If a draft records retention and disposal schedule(s) (i.e. RMO1 - *Records Inventory Form*) is being drawn up, please ensure that the information provided here tallies with those provided therein.

Part II (A) : Checklist

Note: Please tick "✓" as appropriate. All questions except for those marked with an asterisk (*) have been designed to the effect that answers to those questions where applicable are expected to be in the **affirmative** so as to demonstrate that the B/D concerned has adhered to the best practices in the specific areas. For those questions marked with an asterisk (i.e. Questions 1 - 10, 30 and 31), answers to them where applicable are expected to be in the **negative**.

	S/N	Issues	Results			Remark
			Yes	No	Not Applicable (Please provide reasons)	
	Legal and Regulatory Requirements and Related Issues [The following questions assess whether the original records should be retained to meet legal and regulatory requirements.]					
*	1.	Will the destruction of the original records contravene any legal and/or regulatory requirements?				If the answer to this question is "Yes", the B/D should list the relevant legal and/or regulatory requirements and retain the original records. If in doubt, the B/D should seek legal advice as appropriate.
*	2.	Will my B/D breach any legislation or regulatory requirements if the original records are				

	S/N	Issues	Results			Remark
			Yes	No	Not Applicable (Please provide reasons)	
		not maintained in a specific form? [Note: Where the **Electronic Transactions Ordinance** (Cap. 553) (ETO) applies to the original records and the associated digitised records, B/Ds should pay particular attention to sections 5A, 6, 7 and 8 of ETO. Sections 7 and 8 of ETO set out the circumstances under which a legal requirement for "presentation or retention of information in its original form" is satisfied by presenting or retaining the information in electronic form. In case of doubt, B/Ds should consult OGCIO and DoJ as appropriate.]				
*	3.	Does my B/D rely on, or is likely to require (e.g. the likelihood of the original records being required for on-going or anticipated legal proceedings) the original records as evidence in a court of law?				If the answer to this question is "Yes", the B/D should retain the original records.
*	4.	Will the interests of the Government, other B/Ds and/or my B/D in any on-going or anticipated legal action be adversely affected by the destruction of the original records?				If the answer to this question is "Yes", the B/D should retain the original records until and unless the relevant risk is removed. If in doubt, the B/D should seek legal advice as appropriate.
*	5.	(a) Are the nature and legal effect of the original records (e.g. contracts, title deeds,				

	S/N	Issues	Results			Remark
			Yes	No	Not Applicable (Please provide reasons)	
		power of attorney, declarations, etc.) essential for legal or business purposes of the Government, other B/Ds and/or my B/D? (b) Will the original records be required or are likely to be required (e.g. it is likely to require the original records if they are the only ones that can substantiate the interests of the B/D) as evidence when disputes arise?				
*	6.	(a) Do the original records contain seals, watermarks or other features that cannot be reproduced adequately? (b) Are such features (if any) essential for legal or business purposes, policies and procedures? [Note: An original record can be useful in some circumstances, e.g. for detection of fraud. Signs of forgery detectable in the original record may not be carried over into a digitised record. B/Ds should identify key records that might be the subject of fraud and which contain signatures, seals, water marks or other features that authenticate the records.]				
*	7.	(a) Is there any **high risk** of the authenticity, integrity and reliability of the digitised records being subject to challenges in legal proceedings with possible adverse effects?				

	S/N	Issues	Results			Remark
			Yes	No	Not Applicable (Please provide reasons)	
		(b) Are the risk of challenges identified at (a) above assessed to be **unacceptable** to my B/D? [Note: This refers to an assessment of the possibility of litigation, having regard to both past pattern and the nature of the issues relating to the records.]				
	Business, Accountability and Evidence Issues [The following questions assess whether the original records should be retained to meet business, accountability and evidence requirements.]					
*	8.	Will the destruction of the original records contravene any government policy or directive?				If the answer to this question is "Yes", the B/D should list the relevant government policy or directive and retain the original records.
*	9.	Are there any business requirements to retain the original records in their original format? [Note: Graphical materials such as posters, leaflets, designs and brochures may need to be retained in their original format for display. Moreover, where the original record contains physical amendments or annotations that cannot be identified as such on the				

	S/N	Issues	Results			Remark
			Yes	No	Not Applicable (Please provide reasons)	
		digitised image, B/Ds should consider whether the original records should be retained.]				
*	10.	Are the original records still being retrieved and used for the conduct of business? [Note: B/D should also consider the frequency and circumstances of retrievals in judging whether the original records should be retained.]				If the original records are still retrieved by users in conduct of business, the B/D should consider whether the digitised records can be relied upon in lieu of the original records for all purposes.
	11.	Are users relying on the digitised records primarily in the normal conduct of business?				If the answer to this question is "No", the B/D should consider whether the digitised records can be relied upon in lieu of the original records for all purposes.
	Issues Relating to the Authenticity, Integrity, Reliability and Usability of Digitised Records [This part assesses whether the digitised records have the required degree of authenticity, integrity, reliability and usability to substitute for the original records. These four characteristics are critical to maximise the legal admissibility and weight of the digitised records as evidence if being challenged in a court of law. Digitised records are normally stored in an information system or in an electronic storage medium for off-line and/or off-site storage, e.g. an optical disk. Proper operation, management and maintenance of the system or the storage medium are vital to ensure and demonstrate the authenticity, integrity, reliability and usability of the digitised records stored therein. In this connection, IT security and records management (RM) policy, practices and				

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
procedures; scanning procedures and processes; system operation and management, user training, etc. are relevant issues to be assessed.]					
RM and IT Security Policy, Practices and Procedures [The following questions assess whether the relevant B/D has established a clear direction and demonstrated support for, and commitment to, the proper management of records through the formulation, promulgation and maintenance of departmental IT security and RM policy, practices and procedures.]					
12.	(a) Have departmental RM policy, practices and procedures established and implemented in my B/D to cover the original records and the associated digitised records? (b) Have the departmental RM policy, practices and procedures been adequately documented, published and communicated to all appropriate staff members? (c) Have the departmental RM policy, practices and procedures been reviewed, updated and revised regularly and as and when required, e.g. when significant changes occur to the business, legal and/or regulatory environment?				
13.	(a) Have the roles and responsibilities of staff members in managing records, including the original records and the associated digitised records, been clearly set out and communicated to relevant staff members? (b) Have the roles and responsibilities mentioned in (a) above been reviewed and				

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
	revised regularly and as and when required?				
14.	Are there sufficient measures in place to monitor staff compliance with the departmental RM policy, practices and procedures to manage records, including the original records and the associated digitised records?				
15.	Has segregation of roles and responsibilities in RM been implemented in my B/D?				
16.	(a) Has departmental IT security policy been established and implemented covering the original records where applicable and the associated digitised records? (b) Have the departmental IT security policy, practices and procedures been adequately documented, published and communicated to all appropriate staff members? (c) Have the departmental IT security policy, practices and procedures been reviewed, updated and revised regularly and as and when required, e.g. when significant changes occur to the business, legal and/or regulatory environment?				
17.	(a) Have the roles and responsibilities of staff members in managing IT systems and electronic storage media, including the original records where applicable and the associated digitised records, been clearly set out and communicated to relevant staff members? (b) Have the roles and responsibilities mentioned in (a) above been reviewed and				

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
	revised regularly and as and when required?				
18.	Are there sufficient measures in place to monitor staff compliance with the departmental IT security policy, practices and procedures to manage records, including the original records where applicable and the associated digitised records stored in systems or electronic storage media?				
19.	Has segregation of roles and responsibilities in managing systems and electronic storage media been implemented in my B/D?				
Management and Operation of the Information System and/or the Electronic Storage Medium for the Digitised Records					
(A)	General Issues [The following questions assess whether there are sufficient documented procedures to govern the proper use, operation, management and maintenance of the system and the electronic storage medium for the digitised records.]				
20.	Has sufficient documentation been established and made available covering the following aspects of the system and/or the electronic storage medium to manage and store records including the digitised records? ▪ roles and responsibilities; ▪ system manual which is normally applicable to a system only (a description of the key hardware and software components of the system);				

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
	▪ maintenance and monitoring; ▪ procedural manuals which are normally applicable to a system only (a manual detailing the procedures to be followed relating to the system); and ▪ preventive and corrective actions to deal with nonconformity and system malfunctioning.				
21.	In connection with Question 20, has responsibility for overseeing the preparation, management and updating of documentation been clearly assigned?				
22.	In connection with Question 20, has the documentation been reviewed and updated regularly and as and when required with a view to improving the suitability, adequacy and effectiveness of the management and operation of the information system and/or the electronic storage medium?				
23.	Is my B/D able to assert with confidence and evidence the authenticity, integrity, reliability and usability of the digitised records to substitute for the original records having regard to the established departmental policies, practices and procedures in IT security and RM, the operation and management of the system and/or the electronic storage medium and the competency of staff managing the digitised records?				
(B)	System Security [The following questions assess whether the access control and security measures in place are able to demonstrate that the digitised records are				

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
	adequately protected against unauthorised access, alteration and deletion.]				
24.	Has the system been designed with adequate physical and other security safeguards to ensure that the records remain inviolate and can only be changed in an authorised manner?				
25.	Have adequate and effective access control and security measures been implemented for the system and/or the electronic storage medium to protect records against unauthorised access, alteration and deletion?				
26.	In connection with Question 25, have the access control and the security measures been adequately documented and reviewed regularly and where appropriate so that enhancement is made if found necessary?				
27.	Has the relevant security requirements in respect of storage, processing and transmission of classified records, including digitised records prescribed in the Security Regulations been complied with? [Note: This requirement is applicable to classified records, e.g. CONFIDENTIAL records stored in a system or in an electronic storage media.]				
28.	Has segregation of roles and responsibilities been implemented to address the risk of either accidental or malicious changes to and deletion of the digitised records?				

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
29.	(a) Has a security risk assessment been undertaken on the system on a regular basis in accordance with the government and departmental security policy, and the results been properly documented? (b) Has the system passed the recent security risk assessment? (c) Have recommendations on security measures identified by the results of the recent security risk assessment been implemented?				According to Baseline IT Security Policy [S17] issued by OGCIO, security risk assessments for information systems shall be performed at least once every two years and before production, and prior to major enhancements and changes associated with these systems.
* 30.	Are there any reported cases of missing records or incomplete records since the deployment of the system and use of the electronic storage media to store the digitised records?				The B/D should also consider the frequency of the cases, the likelihood of future recurrence and the adverse impacts.
* 31.	Are there any reported cases of unauthorised alteration and deletion of records since the deployment of the system and use of the electronic storage media to store the digitised records?				The B/D should also consider the frequency of the cases, the likelihood of future recurrence and the adverse impacts.
32.	(a) In connection with Questions 30 and 31, have security measures been reviewed following the reported cases?				

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
	(b) Have security measures been stepped up after the review (item (a) above) and is there a reasonable basis to believe that the enhanced measures are effective?				
33.	Have procedures been established for dealing with actual or suspected security breaches?				
34.	Are audit trails generated automatically? If not, are there appropriate manual procedures?				
35.	Are audit trail data (i.e. information stored in the audit trails) unalterable?				
36.	Do the audit trails of the system cover the following – ▪ the system operation and management, e.g. disposal of digitised records; and ▪ any change, including addition, alteration or deletion of the stored records, including the digitised records and the metadata of the records; and details of changes.				
37.	Are the audit trails of the digitised records kept for at least the same period as the digitised records to which they relate?				If the answer is "No", please state how long the audit trails are kept.
38.	Are relevant authorised personnel able to access audit trail data as appropriate?				
39.	Are there appropriate and sufficient procedures to ensure that audit trail data are –				

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
	▪ authentic; ▪ understandable (the audit trail data provides meaningful and adequate information for officers to interpret the data); and ▪ available as required.				
(C)	Scanning Procedures and Processes [The following questions assess whether the technology chosen, procedures and process of scanning are able to ensure and demonstrate that – ▪ all necessary information of the original records is scanned and captured as accurately as possible; ▪ the captured image has **not** been changed since its creation, or where change is permitted, the precise nature of such changes is documented (e.g. conversion from colour to greyscale); ▪ contextual information about the original record (i.e. metadata) is captured in order to reinforce the evidential value of the associated digitised record; ▪ the digitised records were created in a trustworthy environment (i.e. the scanning facility, including the scanner and scanning software operated correctly at all relevant times); ▪ there exists no room for tampering with the scanned images before their capture by the system as digitised records; ▪ the technical standards (e.g. file formats, resolution and compression) of scanning are able to ensure the legibility and usability of the digitised records; and ▪ the procedures and processes, including quality assurance of the digitised records are in place so that if required, they can be subsequently				

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
	demonstrated in a court of law.]				
40.	Have the scanning procedures and processes been planned, selected, implemented and documented? [Note: Digitisation approach, e.g. in-house or outsourced digitisation, hardware and software and strategies for integrating the digitised records into work processes, etc. should be taken into account.]				
41.	Have technical standards of scanning, including those set out below, been planned, selected, 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 deskewing to correct poor document alignment (rotation); ▪ colour management; and				

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
	▪ 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 (Clause 6.2.5 of ISO/TR 13028:2010(E)).]				
42.	Is the performance of the equipment and software used for scanning of original records in a manner or quality acceptable for 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.]				
43.	In connection with Question 41, is there adequate technical support in relation to the technical standards to enable ongoing maintenance of the scanning facility and migration capability when necessary?				
44.	Have the scanning procedures and processes been reviewed and revised regularly and as and when required?				
45.	Have the technical standards been reviewed and revised regularly and as and when				

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
	required?				
46.	Are annotations (e.g. stamps, redaction or addition of notes) to digitised images managed as overlays and the actual images are not changed?				
47.	Are there appropriate and auditable scanning procedures and processes in place to ensure that all the necessary information of the original records have been scanned and captured as accurately as possible?				
48.	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 system or stored in the electronic storage medium?				
49.	Are the results of quality assurance processes documented?				
50.	Have the quality control procedures and measures been reviewed and revised regularly and as and when required?				
51.	Can the system demonstrate that any changes, e.g. conversion from colour to greyscale made to the digitised records once they are stored in the system or in the electronic storage media, are authorised?				
52.	Has any use of enhancement techniques on the digitised record been well documented?				

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
	[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, enable 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.]				
53.	(a) Have the digitised records been assigned links (e.g. through the use of metadata) to the original records? (b) Have links been assigned between associated documents (e.g. a document and a self-adhesive note attached) of the digitised record so that the digitised record is regarded as a single item to faithfully represent the original record?				
54.	Have the digitised records been assigned sufficient and accurate metadata set out below to support on-going business processes and management of the records - ▪ metadata about the record, the business being transacted and the agents associated with the business; and ▪ metadata specific to the particular image and the scanning process such as date and time of scanning.				
55.	Are appropriate and adequate procedures in place to ensure that metadata relating to				

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
	the digitised records are accurate and consistent?				
56.	Are errors and defects in the digitised records corrected?				
57.	Have rescanning procedures been established and adopted to correct any errors identified?				
58.	Has rescanning been properly documented?				
(D)	Disposal of Records [The following questions assess whether disposal of records, including destruction are conducted in a systematic and auditable manner in the system and whether similar measures have been in place to ensure that digitised records stored in an electronic medium are disposed of properly with due authorisation.]				
59.	Are the original records covered by any approved retention and disposal schedule(s)? [Note: Records retention and disposal schedules for programme records should be approved by the Government Records Service (GRS) while those of administrative records are governed by the *Government Administrative Records Disposal Schedules* (GARDS) issued by GRS.]				If the answer to this question is "No", the B/D should draw up a retention and disposal schedule(s) for GRS' approval.
60.	Are there procedures to ensure that appropriate authorisation is obtained before implementation of disposal of records in my B/D?				
61.	Is disposal of records in the system or in the electronic storage media authorised,				

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
	documented (e.g. stored in the audit trails of the system) and audited?				
62.	Are classified electronic records, e.g. CONFIDENTIAL digitised records, disposed of in compliance with the requirements set out in the IT Security Guideline (G3)? [Note: This requirement is only applicable to classified records stored in a system or in an electronic storage media.]				
63.	Will the digitised records acting in place of the original records be retained according to the approved retention and disposal schedules?				
64.	Is disposal of original records documented in the metadata of the associated digital records and is accessible and produced on request?				
(E)	Records Storage [The following questions assess whether the digitised records are stored in a safe, secured and proper environment and are able to remain authentic, complete and accessible for as long as required.]				
65.	Is the hardware, e.g. servers of the system, stored in a safe and secure environment in accordance with the government and departmental IT security policy, guidelines and practices?				
66.	Has the storage technology (including hardware and software) been installed and operated in accordance with manufacturer's recommendations?				

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
67.	Are facilities and procedures, e.g. data verification, available to ensure the integrity of records, including digitised records stored in the system when records are transferred to and from storage?				
68.	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?				
69.	Where records are compressed during the storage process, do the compression methods used evaluated and documented to have no effect on the authenticity and integrity of the stored records, including digitised records in the system or the electronic storage media?				
70.	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?				
71.	Are electronic storage devices of the system subject to regular integrity checking, e.g. to use a checksum to check for data file changes during storage?				
72.	Where records are migrated to new storage media, are there proper and sufficient procedures in place to ensure that – ▪ all appropriate records and the associated information in the system (e.g.				

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
	metadata) have been migrated to the new storage technology; and ▪ the records themselves and the associated information in the system (e.g. metadata) have either not been changed or the changes are known, audited and meet the government and departmental requirements?				
73.	Have the records and the associated information in the system (e.g. metadata) been stored and maintained in a file format that is predicted to allow access over the relevant retention period?				
74.	Where file format conversion is required, are there proper and sufficient procedures in place to demonstrate that all appropriate digitised records have been converted to the new file format(s)?				
75.	Are there facilities, e.g. using a write-once-read-many optical disk to store digitised records, and proper procedures in place to ensure that the digitised records are unalterable in all storage media?				
76.	Have migration and/or preservation strategies and processes been defined and documented for the digitised records stored in the system and/or the electronic storage media to ensure their authenticity, integrity, reliability and usability for as long as they are required?				
(F)	System Maintenance and Monitoring				

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
	[The following questions assess whether the system is operated and maintained properly so as to ensure the authenticity, integrity, reliability and usability of records, including the digitised records stored therein.]				
77.	Is all system maintenance performed by qualified personnel?				
78.	Is preventive maintenance of the system carried out regularly?				
79.	Are preventive maintenance procedures documented?				
80.	Is a system maintenance log kept, which details completed preventive and corrective maintenance, system downtime and action taken?				
81.	Where system access controls can be bypassed during maintenance of hardware and/or software, is personnel performing such processes be strictly controlled, monitored and audited?				
82.	Are measures in place to ensure that records including the digitised records will remain retrievable in the event of system change, computer upgrades or change of software or hardware vendors?				
83.	Is the system administered by people who are trained and competent in its application to ensure that the digitised records are adequately managed over time?				
84.	Have all system failures been documented?				
(G)	System Back-up and Recovery				

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
	[The following questions assess whether the authenticity and integrity of records stored in the system are adequately protected from loss or corruption in case of system failure.]				
85.	(a) Are there procedures for the back-up and verification of records including digitised records and associated information in the system (including audit trails and metadata)? (b) Are the procedures mentioned in (a) above adequately documented?				
86.	(a) Are there procedures (e.g. verification testing) to check that the integrity of records, including digitised 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?				
87.	(a) Are backup media stored in a safe, secure and environmentally suitable location? (b) Are backup media transferred to their storage location in a secure and managed manner?				
88.	Are backup media tested at regular intervals to ensure readability?				
(H)	Business Continuity Planning [The following questions assess whether a business continuity plan is in place to ensure the maintenance of the integrity of records, during and after an				

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
	incident or a disaster.]				
89.	Is a business continuity plan 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?				
90.	(a) Has the business continuity plan been tested? (b) Have the results of the tests been properly documented?				
Use of Third Party Services, e.g. scanning of paper records [Note: If a B/D outsources a service relating to the capturing (including conversion of the original paper records into digitised records), management and maintenance of digitised records, e.g. conducting scanning of the paper records and quality assurance procedures, to a service provider, the following issues have to be assessed to ascertain whether the B/D is able to demonstrate compliance with the government and departmental IT and RM policies, practices and procedures by the way of outsourcing.]					
91.	(a) Has the contract/arrangement with the service provider clearly set out the IT and RM requirements and responsibilities for the service provider to comply with? (b) Has the service provider's performance and compliance with those requirements and responsibilities mentioned in (a) above been regularly monitored and reviewed?				
92.	Are there sufficient measures and control in place to ensure that the service provider				

S/N	Issues	Results			Remark
		Yes	No	Not Applicable (Please provide reasons)	
	complies with the committed service requirements?				
Staff Training [The following questions assess the competence of staff members who are responsible for managing the digitised records and/or operating/managing the system and/or the electronic storage media in which the digitised records are stored.]					
93.	Is proper and sufficient RM and IT training, including IT security provided to staff responsible for managing and operating the system in accordance with the government and departmental IT policies, practices and procedures?				
94.	Is proper and sufficient training provided to staff responsible for managing the records stored in the system and/or the electronic storage media in accordance with the government and departmental RM policies, practices and procedures?				
95.	Has the staff training programme been reviewed and revised regularly and as and when required?				
Other Issues Specific to the B/D [Note: The B/D should consider whether there are issues specific to their business environment and add the identified issues.]					
96.					

Part II (B) : Reference

[Please list out the following for reference by the endorsement officer -

- the business-specific legal and regulatory requirements, government policy and directive relevant to your B/D, etc. that have been considered in the context of completing the checklist in Part II (A) above;
- any other legal and regulatory requirements and/or government regulations/directive, etc. that warrant the attention of the endorsement officer when completing Part IV below; and
- views and comments made by other stakeholders, e.g. DRM and Head of ITMU on the issues set out in the risk analysis.]

Part III : Outcome of the Risk Analysis and Recommendation

[Please document the outcome of the risk analysis based on the answers given to Part II (A) and (B) (e.g. the authenticity, integrity and reliability of the digitised records are likely subject to challenges because of inadequate security measures are in place to safeguard the system ABC), the recommendation (e.g. security measures should be enhanced to mitigate the risks identified) and the justification for making such recommendation, etc.]

Name of officer who completed Parts I to III: _____

Post Title: _____

Rank[#]: _____

Date: _____

[#] The risk analysis should be completed by an officer not below the rank of Senior Executive Officer or equivalent.

Part IV : Endorsement

[Please state your views on whether the original records should be destroyed. Please also provide information/views to supplement those set out in Parts II and III above, if any.]

Name of officer: _____

Post Title _____

Rank[#]: _____

Date: _____

[#] Outcome of the risk analysis should be endorsed by an officer not below the rank of Chief Executive Officer or equivalent.

Annex 4

To: Government Records Service Director
(Attention: Records Management and Administration Office,
Email: ADMIN_RCINFO/GRS/HKSARG or admin_rcinfo@grs.gov.hk)

Destruction of Original Records which have been Digitised and Managed in an Electronic Recordkeeping System (Administrative Records)

(Please read the explanatory notes below before completing this form.)

Bureau / Department (B/D)	
Branch / Division / Section / Office	
Classification of Records	Unclassified / Classified* Administrative Records *(* Delete as appropriate. Please note that "Classified records" refer to records with security classifications "Restricted", "Confidential", "Secret" or "Top Secret".)*

I should be grateful for your agreement to destroy the following original records -

Item No.	Subject Matter (subject/records group in General Administrative Records Disposal Schedules (GARDS))	Quantity of Records (No. of files & linear metres)	In Compliance with Items in GARDS	Disposal Remarks in GARDS
1				
2				
3				
4				
	Total:	files (lm)		

2. I confirm that -

(a) all of the records listed above have been digitised and managed in my B/D's electronic recordkeeping system, and those associated digitised records are to be kept in the electronic recordkeeping system no shorter than the retention period as listed above;

(b) the records listed above are proposed to be destroyed before expiry of the retention period specified in GARDS. The risks of early destruction of the records listed above have been assessed and are considered acceptable;

(c) all legislation and relevant government regulations/circulars governing the retention and disposal of the records listed above have been complied with; and

(d) the disposal of records listed above has been considered and endorsed by an officer not below the rank of Senior Executive Officer or equivalent according to paragraph 17 of General Circular No. 2/2009.

Submitted by (Contact Officer)	(name)
	(rank/post)
	(tel. no.)
	(Lotus Notes e-mail)
Endorsement Officer (an officer not below the rank of Senior Executive Officer or equivalent [Note 1])	(name)
	(rank/post)
	(tel. no.)
	(Lotus Notes e-mail)
	(date of endorsement)
Supplementary remarks, if any	

Explanatory Notes

1. "An officer not below the rank of Senior Executive Officer or equivalent" is defined in the present context as an officer the maximum pay point of whose rank is not lower than MPS Point 44 or equivalent.

2. After completing this form, please attach this document in the email and send it to the Government Records Service Director (Attn: Records Management and Administration Office) by e-mail [ADMIN_RCINFO/GRS/HKSARG (Lotus Notes) or admin_rcinfo@grs.gov.hk (internet)]. Submission by paper or fax will normally not be considered.

3. If the email to Government Records Service Director is not sent by the Endorsement Officer, please copy to the Endorsement Officer for information. When the disposal request is approved, Government Records Service will inform the Endorsement Officer and copy to the Contact Officer.

Annex 5

To: Government Records Service Director
(Attention: Records Management and Administration Office,
Email: ADMIN_RCINFO/GRS/HKSARG or admin_rcinfo@grs.gov.hk)

Destruction of Original Records which have been Digitised and Managed in an Electronic Recordkeeping System (Programme Records)

(Please read the explanatory notes below before completing this form.)

Bureau / Department (B/D)	
Branch / Division / Section / Office	
Classification of Records	Unclassified / Classified* Programme Records *(* Delete as appropriate. Please note that "Classified records" refer to records with security classifications "Restricted", "Confidential", "Secret" or "Top Secret".)*
Our Ref.	

I should be grateful for your agreement to destroy the following original records -

Item No.	**Disposal Authority No. (DA No.) & Agency Records Series No. (ARS No.)**	**Records Series Title**	**Quantity of Records (No. of files & linear metres)**	**Disposal Class No. (if any)**	**Retention Period and Disposal Action in DA**
1					
2					
3					
4					
		Total:	files (lm)		

2. I confirm that -

(a) all of the records listed above have been digitised and managed in my B/D's electronic recordkeeping system, and those associated digitised records are to be kept in the electronic recordkeeping system no shorter than the retention period as listed above;

(b) the records listed above are proposed to be destroyed before expiry of the retention period specified in the disposal schedules. The risks of early destruction of the records listed above have been assessed and are considered acceptable;

(c) all legislation and relevant government regulations/circulars governing the retention and disposal of the records listed above have been complied with; and

(d) the disposal of records listed above has been considered and endorsed by an officer not below the rank of Senior Executive Officer or equivalent according to paragraph 17 of General Circular No. 2/2009.

Submitted by (Contact Officer)	(name)
	(rank/post)
	(tel. no.)
	(Lotus Notes e-mail)
Endorsement Officer (an officer not below the rank of Senior Executive Officer or equivalent [Note 1])	(name)
	(rank/post)
	(tel. no.)
	(Lotus Notes e-mail)
	(date of endorsement)
Supplementary remarks, if any	

Explanatory Notes

1. "An officer not below the rank of Senior Executive Officer or equivalent" is defined in the present context as an officer the maximum pay point of whose rank is not lower than MPS Point 44 or equivalent.

2. After completing this form, please attach this document in the email and send it to the Government Records Service Director (Attn: Records Management and Administration Office) by e-mail [ADMIN_RCINFO/GRS/HKSARG (Lotus Notes) or admin_rcinfo@grs.gov.hk (internet)]. Submission by paper or fax will normally not be considered.

3. If the email to Government Records Service Director is not sent by the Endorsement Officer, please copy to the Endorsement Officer for information. When the disposal request is approved, Government Records Service will inform the Endorsement Officer and copy to the Contact Officer.