Government of South Australia

State Records of South Australia

Digitisation of official records and management of source documents

Guideline

December 2009

Version **3.1**

Table of Contents

Introduction

Many agencies in South Australia are currently digitising official records by using scanning or imaging technologies. Typically the records created and captured by imaging are managed using a database; an Electronic Document and Records Management System (EDRMS) or a business system.

When implementing digitisation programs agencies need to ensure that they meet both business requirements and the legislative requirement to preserve official records of enduring evidential or informational value for future reference.

Scope of this guideline

This guideline can be applied by all agencies as defined in section 3 of the *State Records Act 199*7, including:

- state government departments and administrative units, including the police force
- local government authorities
- courts and tribunals
- incorporated or unincorporated bodies
- the Governor and Ministers of the Crown
- former agencies that ceased to exist before the commencement of the State Records Act.

This guideline deals with the digitisation of paper source documents and the subsequent management and disposal of these and their digitised counterparts. It does not currently relate to other forms of conversion or migration of official records 'born' electronically.

This guideline primarily addresses the application of digitisation technologies when integrated with either an EDRMS or business system. It aims to minimise the risks to government, both state and local, in terms of records of longer-term temporary or permanent value being lost or destroyed, without limiting the application of digitisation technologies for efficient office administration or other purposes.

This guideline and the complementary *General Disposal Schedule No 21* (GDS 21) **do not** authorise the destruction of any source documents that have been deemed to be of permanent value in accordance with an approved and current disposal schedule.

This guideline is issued as part of the Across-Government Adequate Records Management Framework. Compliance with this guideline will assist agencies in meeting Adequate Records Management requirements.

This guideline is issued under Section 7(g) of the State Records Act.

Other related electronic records initiatives

State Records is currently participating in the Australasian Digital Recordkeeping Initiative (ADRI) with other state, territory and national archival authorities to address broader digital recordkeeping issues and to develop nationally recognised standards. Consistent with this State Records aims to develop a Digital Recordkeeping Strategy and to establish a digital repository, which will enable State Records to receive, store, provide access to and preserve both digitised and 'born digital' records that are of permanent value.

On 14 July 2009, the Minister Assisting the Premier in Cabinet Business and Public Sector Management approved a framework of standards that mandate and support EDRMS procurement and implementation. State government agencies, in accordance with the State Records Act, are required to procure a compliant system in accordance with the requirements detailed within these standards. In addition, local government authorities are encouraged to purchase compliant solutions in order to achieve a number of business benefits and cost savings.

State Records has also developed two standards, including a functional specification, concerning the management of records held within agencies' business systems.

Related documents

The following related documents are available from State Records' website (www.archives.sa.gov.au):

- *Adequate Records Management Standard*
- *EDRMS Design Standard*
- *Document and Records Management Systems Standard*
- *South Australian Recordkeeping Metadata Standard (SARKMS)*
- *Management of Official Records within a Business System Standard*
- *Functional Specification for Records in a Business System Standard*
- *Contracting and Official Records Standard and Guideline*
- *Day Batching of Official Records Recordkeeping Information Sheet*
- *General Disposal Schedule No 15 (7th edition) for State Government Agencies in South Australia*
- *General Disposal Schedule No 20 (Version 4) for Local Government Records in South Australia and*
- *General Disposal Schedule No 21 (Version 3) for management and disposal of source documents and digitised versions after digitisation.*

Acknowledgments

State Records acknowledges the policy work regarding digitisation of the following organisations:

- Public Records Office of Victoria
- National Archives of Australia.

Variation to this guideline

State Records may update or alter this guideline from time to time as authorised by the Director of State Records, in consultation with the State Records Council. All South Australian agencies will be informed of any such alterations or updates.

Further reading

A bibliography of digitisation related material is located at Attachment 5.

Further information and feedback

Agencies requiring further information relating to this guideline should contact the Manager, Records Management Services at:

State Records
GPO Box 2343
ADELAIDE SA 5001
Ph: +61 8 8204 8773
Fax: +61 8 8204 8777
E-mail: srsarecordsmanagement@sa.gov.au

Legislation

The primary South Australian legislation that has an impact on the application of scanning and imaging systems are:

- the *State Records Act 1997*, which prohibits the destruction of official records without authority. As the processes of scanning and imaging to produce digital versions effectively results in the creation of new records, the Act applies not only to the original source documents but also to the digitised records captured in the process of digitisation

- the *Electronic Transactions Act 2000*, which provides legal validity to transactions carried out electronically and permits the recording and retention of information and documents in electronic form

- the *Evidence Act 1929* (as amended), which describes the way in which documents and records may be admitted as evidence into a court. Common law provides for original documents to be accepted as "best evidence". Digital versions may be admitted into evidence if the original is lost or destroyed, but they may have less weight as evidence. Paragraph 59B relates to the admissibility of computer output, however, several conditions apply to the admissibility of computer evidence including material that has been digitised by scanning or imaging, and

- the *Freedom of Information Act 1991* provides a legally enforceable right to access documents of state government agencies, Local government authorities and state government universities subject to any exemption provisions that may apply. This Act defines a document to include anything in which information is stored or from which information may be reproduced. This includes scanned and digital versions of records held within an EDRMS or business system when the source document is no longer available.

Technological risks

Obsolescence

One of the most challenging issues for agencies in adopting digitisation is technological obsolescence. One of the requirements of the Electronic Transactions Act is that documents in electronic format must be reasonably expected to be "readily accessible" for subsequent use. Agencies need to also take regard of the period for which a record needs to be retained and remain accessible in accordance with the State Records Act and the Adequate Records Management Framework.

Agencies need to consider, not only the integrity of the record and its associated metadata in the long term, but also the availability of software and computer hardware required to ensure the record remains readily accessible.

The following questions should be asked when agencies consider adopting digitisation technology and the destruction, or otherwise, of the original source version of records:

- How long do the records need to be kept?
- Has the system been designed, or a migration plan put in place, so that it is possible to read the digitised records for as long as they need to be kept?
- Is the agency operating a compliant EDRMS or business system according to all applicable South Australian Government standards and guidelines?
- Has a strategy been developed to ensure records captured by the system and their associated metadata remain readable and accessible over time with evolving technologies?

Format

State Records recommends the requirements within *PROS 99/007 Specification 4: VERS Long Term Preservation Formats* when creating the digitised records.

State Records is not prescriptive in relation to image resolution or other attributes. It is for an agency to determine the appropriate resolution it considers to be applicable to each type of document and its associated retention period. For example, it may be deemed that financial records such as invoices do not need as high a resolution as that of personnel records dependent upon how long the records are needed to be kept. An agency's business need dictates this.

Compression and decompression

Some formats for storing and managing digital images result in degradation each time the image is opened and saved as a new image.

Compression comes in two forms: lossless and lossy. Lossy compression removes some of the original detail but can reduce the size of image files to a far greater extent than lossless compression.

With each subsequent manipulation, such as migration, files are at risk of becoming unreadable or losing their evidential value. Long term preservation of digital records will

require that the images are in an open and enduring format using lossless compression techniques.

Encryption

Records that are encrypted present special problems in ensuring that they can be accessed and read over time. While encryption is often used for the secure and safe transmittal of data and information, it should not be used as a security measure for electronic storage. Other security measures are available to deal with the security of electronic data.

State Records will not accept into custody digital records that are encrypted.

Quality control

Agencies need to ensure that procedures are in place to cover the process of scanning source documents. Issues such as poor quality resolution, incomplete or an obstructed image, incomplete or inaccurate metadata or spelling/grammar errors can arise when scanning individual or batches of records. The procedures should include:

- the preparation of documents to be imaged
- verification that the digitised images are authentic, complete and accessible prior to the destruction of the source document
- frequency that verification is to occur, i.e. each time a source document is scanned, periodic testing or random sampling.

Outsourcing the digitisation of source documents

Not all agencies procure document scanning software and hardware. Agencies engaging contracted service providers for the scanning of source documents need to ensure that:

- they are satisfied with the digitised version, i.e. that the version is authentic, complete and reliable
- the source documents are returned to the agency within an appropriate timeframe.

Agencies need to have a formal agreement/contractual arrangement in place with the third party provider that guarantees rights and responsibilities (for the agency and provider) are clearly articulated and agreed upon. Refer to the *Contracting and Official Records Standard and Guideline* for further information.

Certification of an EDRMS or business system

Prior to an agency being able to destroy temporary source documents in accordance with GDS 21, an agency's EDRMS or business system needs to comply with requirements set out in one of three certifications for digitised records.

The first certification (Attachment 1) refers to the digitised records managed in a compliant EDRMS. These systems have been assessed as compliant having been evaluated and tested against the South Australian EDRMS suite of standards to ensure that the records are inviolate, the capture of adequate metadata and the risks associated with system obsolescence are mitigated.

The second certification (Attachment 2) is for an agency's compliant business system (either stand alone or integrated/interfaced with an EDRMS) that has been assessed as being compliant with the South Australian business systems standards.

The third certification (Attachment 3) is for a non-compliant EDRMS or business system (either stand alone or integrated/interfaced with an EDRMS); these systems are not compliant with the State Records framework of standards, having either not been assessed against the established requirements or having been assessed as non-compliant. However, it is recognised that these systems may support the digitisation of records (functionally) and meet the conditions stipulated within Attachment 3.

Records managed in any of the systems identified above need to be disposed of according to GDS 21.

An executive level officer (CE, CEO or CIO) is required to certify that the system for digitising and managing records meets certain conditions, including, but not limited to:

- the system is compliant with and captures the mandatory elements of the *South Australian Recordkeeping Metadata Standard (SARKMS)* and that the mandatory metadata is maintained as a permanent record

- the system has appropriate audit trails in place, as defined in the State Records *Document & Records Management System Standard*

- the system has been designed and implemented to ensure that a digitised record represents a true and accurate rendition of the source document and is fit for the purpose for which it was created. Particularly, that procedures and business rules are in place to ensure the digitised record is classified by an appropriate business function-based thesaurus that facilitates the inheritance of disposal classification, security and access rights, efficient searchability and retrieval *(Note: a function-based thesaurus only applies to a business system when it is integrated/interfaced with an EDRMS, however stand alone systems must still be able to facilitate the inheritance of disposal classification, security and access rights, efficient searchability and retrieval) (Note: the documents/records must be captured within a file/folder/container and/or all related documents/records linked/cross-referenced in order to ensure the evidence, integrity and context of a record that includes multiple documents/parts is apparent, maintained and able to be reproduced for access purposes (whether business or public) as needed over time)*

- the system has been designed with adequate physical and other security safeguards to ensure the records remain inviolate and can only be changed in an authorised fashion

- audit records are maintained as recordkeeping metadata

- the system has been designed to ensure that adequate versions of the originals are being made, ie that the digitised records are fit for the purpose for which they were created

- the system is operated and maintained by people who are trained and competent in its application and use to ensure the digitised records are adequately managed over time

- the records captured in the system are stored in an open and enduring data format, e.g. PDF, JPG or TIFF or the agency has a migration strategy in place to ensure that official records are not placed at risk of loss through technological obsolescence

- the digitised records are authorised as true and accurate renditions of the source documents by a person in the agency with appropriate authority.

Please refer to the relevant certification to determine the compliance requirements and conditions applicable to the agency's system.

Such certification needs to be provided to State Records by agencies, in writing, using the form at either Attachment 1, 2 or 3 of this Guideline. Certification by an executive level officer demonstrates that senior management within an agency are aware of, and take responsibility for, the records management programs and practices in their organisation. Agencies should consider the conditions established within the three certifications and ensure they can be met before implementing systems for digitising records. Agencies are required to also have held discussions with State Records prior to receiving an agency's certification, to ensure that digitisation programs are compliant.

This commitment also includes the ongoing maintenance of the system according to technological advancement. This will enable the agency to destroy any temporary value source documents at the time of digitisation and once an agency's business need expires.

Systems that meet the requirements established under State Records framework of EDRMS standards or the business systems standard will be compliant with the technical requirements for certification. Agencies should complete Attachment 1 or 2 once State Records has confirmed the agency's system is compliant in terms of governance and application of recordkeeping principles. Systems that do not meet State Records standards as detailed above will need to meet requirements established within Attachment 3.

Notification of destruction of source and digitised records

It is the responsibility of each agency to notify State Records that records in its custody are due to be destroyed, before destruction takes place in accordance with an authorised disposal schedule.

For source documents, this is a once-off communication via a policy statement indicating the agency's business requirements regarding the retention and disposal of temporary source documents and its capability for managing the digitised versions as the corporate record.

For example, what is the set period of time that the agency retains the temporary source document before disposal occurs? What procedures are in place to ensure that the digitised record is authentic, complete and accessible? This communication to State Records must also include the procedures and business rules that are in place within the agency as referred to in Attachments 1, 2 and 3.

State Records suggests that agencies obtain legal advice prior to developing their policy statement to ensure the destruction of specific record types is not detrimental to the interests of the agency or its clients.

An agency's policy statement must accompany one of the above certifications prior to the destruction of any temporary source documents.

For digitised records, agencies are required to use the form *Notification of Intention to Destroy Records*, available from the State Records website (www.archives.sa.gov.au).

For further information, please refer to GDS 21 which is available from the State Records website.

Technical standards for an EDRMS or business system

State Records requires agencies to comply with the following standards when implementing EDRM systems:

- *Adequate Records Management Standard, issued by State Records (2002)*
- *Document and Records Management Systems Standard, issued by State Records (2009)*
- *South Australian Recordkeeping Metadata Standard (SARKMS), issued by State Records (2009), and*
- *The Victorian Electronic Records Strategy (VERS), issued by the Public Records Office of Victoria.*

EDRMS solutions that were procured from the now defunct Across-Government Panel comply with the above standards as long as they have been configured and customised in a way that complies with these standards.

In addition, State Records encourages agencies to become familiar with Chapter 2 of the following handbook issued by Standards Australia:

- *HB 171-2003 Guideline for the management of IT Evidence (available from Standards Australia)*

State Records also requires agencies to comply with the following standards when implementing line of business systems:

- the functionality requirements established under the *South Australian Management of Official Records within a Business System Standard*
- the functionality requirements established under the *South Australian Functional Specification for Records in a Business System Standard*
- the mandatory recordkeeping metadata elements which are captured and maintained as a permanent record in accordance with *South Australian Recordkeeping Metadata Standard* (SARKMS).

Due to the rapid evolution and variety of industry standards, State Records does not endorse any technical standards for systems used for digitising official records. However, a checklist of items to assist agencies when considering implementation of digitisation systems is at Attachment 4.

Management of digitised official records

The digitised versions of records captured into an EDRMS or business system will take on or inherit the disposal criteria attributed to the original source documents, as outlined in the appropriate General Disposal Schedule (GDS) or agency specific Records Disposal Schedule (RDS).

Digitised records identified for either temporary or permanent retention, will need to be managed appropriately. This means that the digitised version has:

- been captured and maintained in an certified EDRMS or business system that meets the requirements in Attachments 1, 2 or 3
- been captured or maintained in an open and enduring format or has a migration strategy in place and
- all associated mandatory recordkeeping metadata captured and retained permanently.

Management of metadata

The management of recordkeeping metadata associated with records captured into a recordkeeping system is particularly important as it provides the context, content and structure of records. Without recordkeeping metadata, records will lose much of their evidential value and context.

State Records has issued the *South Australian Recordkeeping Metadata Standard (SARKMS),* which is available from the State Records website (www.archives.sa.gov.au). It outlines the mandatory metadata elements required to ensure records will maintain their evidential value over time, and will enable compliance with the *Adequate Records Management Standard,* also available in electronic format from the State Records website.

Recordkeeping metadata needs to be retained even if a record has been removed since it provides the essential evidence of the existence of records. For this reason, the mandatory recordkeeping metadata needs to be retained permanently in an open and enduring format.

General Disposal Schedule No 15 (7th Edition) contains an entry on the disposal and retention of recordkeeping metadata.

Authority for disposal of source documents that have been digitised

State Records Council has approved GDS 21 to authorise the accelerated destruction of source documents, subject to special conditions being met. This is on the basis that the digitised version and its associated metadata will be retained in accordance with an approved disposal schedule as if it were the original.

GDS 21 **cannot** be used to authorise disposal of source documents or digitised renditions that are not covered by a current and approved GDS or RDS.

In addition, GDS 21 does not authorise the destruction of permanent paper-based source documents. Permanent paper-based source documents need to be transferred to State

Records when no longer required by an agency for current administrative purposes and in any case once 15 years old.

Retention of permanent source documents

Permanent records are records that have been identified as permanent under an approved disposal schedule. If the source documents are considered to be permanent records, then the process of digitisation does not allow their destruction.

Advice from the Crown Solicitor's Office indicates that the provisions of the Electronic Transactions Act, which allow for recording and retention of information and documents in electronic form, cannot be used to justify the destruction of paper (or other physical format) records determined to be of permanent value in accordance with the State Records Act.

Destruction of temporary source documents and risk

A significant risk of digitisation is that temporary source documents may be destroyed after they have been digitised without proper consideration of the business needs of the agency.

It is often the case that an electronic version of a record will not be given high value as evidence in a court of law, because organisations will not be able to prove that the record has remained inviolate.

The following questions should be considered when assessing the risk of destroying original temporary source documents after digitisation:

- Does the agency rely on, or is it likely to require the records as evidence in a court of law? If so, how often?
- Are there any special requirements to retain the temporary source documents such as:
  - legislative requirements
  - business need
  - customer expectation that the records can be accessed in the original format
  - a corporate seal, watermark or security feature that cannot be replicated during the scanning process?
- Is the system maintained in a way that will enable access and ready retrieval by a Freedom of Information Officer?
- Has the system been designed with adequate physical and other security safeguards to ensure the records remain inviolate and can only be changed by a person with appropriate authority?
- Does the system have audit trails in place?
- Are audit records retained as recordkeeping metadata?
- Does the system capture all mandatory metadata elements required to ensure compliance with the SARKMS?

- Has the digitisation system been designed to ensure that adequate[1] versions of the paper source documents are being made? Is the resolution sufficient that the digitised version is an acceptable facsimile of the source in all respects?
- Is the system operated and maintained by people who are trained and competent in its use to ensure the digitised records are adequately managed over time?
- Are the digitised records authorised as true and accurate renditions of the source documents by a person in the agency with appropriate authority?

Agencies are referred to Standard Australia's *AS/NZS 4360-1996 Risk Management* and *HB 143-1999 Guidelines for managing risk in the Australian and New Zealand public sector* (available from Standards Australia) that provides useful tools for assessing risks associated with implementing new technologies and systems.

Only agencies that have completed and had approved one of the system certification forms, Attachments 1-3 of this guideline, can destroy hardcopy temporary records that have been digitised within a certified system.

Audit Regime

To ensure compliance with the Adequate Records Management Framework, State Records of South Australia has included the assessment of agencies business processes surrounding the accuracy and authenticity of scanned documents captured within an EDRMS or business system as part of its wider adequate records management audit of agency programs and practices.

---

[1] i.e. fit for the purpose for which the records were created.

Attachment 1: Certification of a compliant EDRMS that stores digitised official records

The system described below is used to capture and store official agency records by application of scanning / imaging technology. Subject to the certification below, only **temporary source documents** may be disposed of in accordance with General Disposal Schedule No 21 (GDS 21).

This certification should be renewed each time there is a major upgrade of the system i.e. from version 6 to 7, but not from 6.1 to 6.2.

Agency Name: _____ Agency GA No: _____

Name of EDRMS: _____Version: _____

Description of Official Records Captured (attach further pages if required):
_____
_____

Disposal Schedule(s) for Records Captured by the System:
_____

Certification

I hereby certify that the EDRMS used to capture the official records described above is compliant with:

- the mandatory recordkeeping metadata elements which are captured and maintained as a permanent record in accordance with *South Australian Recordkeeping Metadata Standard* (SARKMS)
- the Victorian Electronic Records Strategy (VERS)
- the functionality requirements established under the South Australian EDRMS Functional Specification Standard.

I also hereby certify that the EDRMS has been configured and/or customised in a manner that is compliant with the following conditions:

- the system has been designed and implemented to ensure that a digitised record represents a true and accurate rendition of the source document and is fit for the purpose for which it was created. Particularly, that procedures and business rules are in place to ensure the digitised record is classified by an appropriate business function-based thesaurus within that facilitates the inheritance of disposal classification, security and access rights, efficient searchability and retrieval *(Note: the digitised version must be captured within a file/folder/container and all related documents/records linked/cross-referenced in order to ensure the evidence, integrity and context of a record that includes multiple documents/parts is apparent, maintained and able to be reproduced for access purposes (whether business or public)as needed over time)*
- the system has been designed with adequate physical and other security safeguards to ensure the records remain inviolate and can only be changed in an authorised manner

- the audit records remain in place for at least as long as the record

- the system is operated and maintained by people who are trained and competent in its application to ensure the digitised records are adequately managed over time

- this agency has a migration strategy in place to ensure that official records are not placed at risk of loss through technological obsolescence or alternatively that the records captured by the system are stored in an open and enduring data format, e.g. PDF, JPG or TIFF.

Signed:_____   Date: ………../ ………../ ……………
      (Chief Executive / Information Officer)

Witness:_____   Date: ………../………../…….……...
      (Name)

NOTE: A copy of this certificate must be sent to State Records and a copy retained for agency reference.

Attachment 2: Certification of a compliant business system that stores digitised official records

The system described below is used to capture and store official agency records by application of scanning / imaging technology. Subject to the certification below, only **temporary source documents** may be disposed of in accordance with General Disposal Schedule No 21 (GDS 21).

This certification should be renewed each time there is a major upgrade of the system i.e. from version 6 to 7, but <u>not</u> from 6.1 to 6.2.

Agency Name: _____Agency GA No: _____

Name of system: _____Version: _____

Description of Official Records Captured (attach further pages if required):
_____
_____

Disposal Schedule(s) for Records Captured by the System:

_____

Certification

I hereby certify that the business system used to capture the official records described above is compliant with:

- the functionality requirements established under the *South Australian Management of Official Records within a Business System Standard*

- the functionality requirements established under the *South Australian Functional Specification for Records in a Business System Standard*

- the mandatory recordkeeping metadata elements which are captured and maintained as a permanent record in accordance with *South Australian Recordkeeping Metadata Standard* (SARKMS).

I also hereby certify that the business system above (either stand alone or integrated/interfaced with an EDRMS) has been configured and/or customised in a manner that is compliant with the following conditions:

- the system has been designed and implemented to ensure that a digitised record represents a true and accurate rendition of the source document and is fit for the purpose for which it was created. Particularly, that procedures and business rules are in place to ensure the digitised record is classified by an appropriate business function-based thesaurus that facilitates the inheritance of disposal classification, security and access rights, efficient searchability and retrieval *(Note: a function-based thesaurus only applies to a business system when it is integrated/interfaced with an EDRMS, however stand alone systems must still be able to facilitate the inheritance of disposal classification, security and access rights, efficient searchability and retrieval) (Note:*

the documents/records must be captured within a file/folder/container or all related documents/records linked/cross-referenced in order to ensure the evidence, integrity and context of a record that includes multiple documents/parts is apparent, maintained and able to be reproduced for access purposes (whether business or public) as needed over time)

- the system has been designed with adequate physical and other security safeguards to ensure the records remain inviolate and can only be changed in an authorised manner

- the audit records remain in place for at least as long as the record

- the system is operated and maintained by people who are trained and competent in its application to ensure the digitised records are adequately managed over time

- this agency has a migration strategy in place to ensure that official records are not placed at risk of loss through technological obsolescence or alternatively that the records captured by the system are stored in an open and enduring data format, e.g. PDF, JPG or TIFF.

Signed:_____   Date: ………../ …………/ ……………
      (Chief Executive / Information Officer)

Witness:_____   Date: ………../…………../……..……....
      (Name)

NOTE: A copy of this certificate must be sent to State Records and a copy retained for agency reference.

Attachment 3: Certification of a non-compliant EDRMS or business system that stores digitised official records

The system described below is used to capture and store official agency records by application of scanning / imaging technology. Subject to the certification below, only **temporary source documents** may be disposed of in accordance with General Disposal Schedule No 21 (GDS 21).

This certification should be renewed each time there is a major upgrade of the system i.e. from version 6 to 7, but <u>not</u> from 6.1 to 6.2.

Agency Name: _____Agency GA No: _____

Name of system: _____ Version: _____

Description of Official Records Captured (attach further pages if required):
_____
_____

Disposal Schedule(s) for Records Captured by the System:

_____

Certification

I hereby certify that the EDRMS or business system (either stand alone or integrated/interfaced with an EDRMS) used to capture the official records described above is compliant with the following conditions:

- the system, although not compliant, has been designed and implemented to ensure that a digitised record represents a true and accurate rendition of the source document and is fit for the purpose for which it was created. Particularly, that procedures and business rules are in place to ensure the digitised record is classified by an appropriate business function-based thesaurus that facilitates the inheritance of disposal classification, security and access rights, efficient searchability and retrieval *(Note: a function-based thesaurus only applies to a business system when it is integrated/interfaced with an EDRMS, however stand alone systems must still be able to facilitate the inheritance of disposal classification, security and access rights, efficient searchability and retrieval) (Note: the documents/records must be captured within a file/folder/container or all related documents/records linked/cross-referenced in order to ensure the evidence, integrity and context of a record that includes multiple documents/parts is apparent, maintained and able to be reproduced for access purposes (whether business or public)as needed over time)*

- the system has been designed with adequate physical and other security safeguards to ensure the records remain inviolate and can only be changed in an authorised manner

- the system has been tested and proven over a number of years that the digitised records are able to be accessed, retrieved and legible

- the system has appropriate audit trails in place as defined in the State Records *Document & Records Management System Standard*

- the audit records remain in place for at least as long as the record

- mandatory recordkeeping metadata elements are captured and maintained as a permanent record in accordance with *South Australian Recordkeeping Metadata Standard* (SARKMS)

- the system is operated and maintained by people who are trained and competent in its application to ensure the digitised records are adequately managed over time

- this agency has a migration strategy in place to ensure that official records are not placed at risk of loss through technological obsolescence or alternatively that the records captured by the system are stored in an open and enduring data format, e.g. PDF, JPG or TIFF.

Signed:_____   Date: ………../ ………../ ……………
      (Chief Executive / Information Officer)

Witness:_____   Date: ………./………..../……….………..
      (Name)

NOTE: A copy of this certificate must be sent to State Records and a copy retained for agency reference.

Attachment 4: Checklist for digitisation systems

Information gathering/collection

- Interview representatives from all operational areas which are affected by introduction of the digitisation system
- Interview representatives of key stakeholder groups
- Gather statistical information about current work practices and processes
- Benchmark with similar organisations
- Identify legislative and regulatory environment in which the agency operates, *State Records Act 1997, Freedom of Information Act 1991, s*pecific agency legislation
- Identify Records Management Standards and guidelines which need to be considered, e.g. AS ISO 15489, *Adequate Records Management Standard*, *South Australian Recordkeeping Metadata Standard (SARKMS)*, etc
- Identify risks including technical, legal and other risks.

Scope definition

- develop overview of project
- identify broad business drivers
- identify options available to meet business drivers
- identify document scanning and workflow software
- develop business process management/workflow
- identify objectives/scope of project, e.g.
  - number of documents/records to be processed => scanner speed
  - number of documents to be stored on system
  - metadata storage => refer SARKMS
  - Digitised Image Resolution standard required to ensure documents are adequate for the purpose required
  - Digitised Image Format standards
  - number of users/workstations
- develop risk assessments to assess the need for ongoing access to source documents
- develop policies and procedures regarding the verification quality control and periodic equipment testing of hardcopy imaging processes
- identify related corporate projects, e.g. web development / e-business
- develop brief methodology description
- estimate costs for completing project – broken down into phases
- identify problems and strategies to overcome them
- identify measurable outcomes expected from project.

Strategic support

- research/identify process for obtaining approval for project
- link the project to the organisation's business
- identify a project sponsor or "champion"
- appoint/select a project manager
- establish a steering group to take responsibility for the project
- identify key players and ensure they are supportive of the project.

Marketing & communication

- give the project a name
- produce a project update, newsletter or website to ensure stakeholders are informed of progress
- provide presentations to key stakeholder groups
- develop rewards/incentives for participation.

Analysis

- review/identify adequacy of current records in terms of their value as evidence
- identify where records should be created that are not currently created
- review adequacy of existing metadata capture
- identify mandatory metadata elements required as referred in SARKMS
- identify retention requirements through
  - General Disposal Schedules (GDS) and
  - Agency Specific Records Disposal Schedules (RDS)
- identify control tools
- analyse current business workflows
- determine types and extent of user/operator training required.

System design

- develop functional/technical specification as referred to in *Document & Records Management Systems Standard* and associated suite of EDRMS documents
- identify how software and hardware will be selected and procured
- identify system configuration
- develop testing plans
- identify the resolution required to ensure digitised records are readable
- identify electronic document storage requirements, e.g. how much digital storage capacity/disc space will be required to store digitised images and the associated metadata
- develop imaging policies and procedures
- develop training and education programs for staff using the system
- develop change management strategies
- develop migration strategies

- develop a rollout program.

Implementation

- appoint / select staff if required
- devise rollout of tools including software
- train key people
- establish ongoing support e.g. IT help
- convert / migrate records as necessary
- formally close existing / legacy systems
- review progress against project plan.

Post implementation review

- review the business case objectives and requirements
- review performance measures
- review each component of the project
- report outcomes of the review to key stakeholders and users.

Attachment 5: Bibliography

- Hazen, D., Horrell, J., Merrill-Oldham, J. 1998. *Selecting Research Collections for Digitization. Council on Library and Information Resources*, available online at www.clir.org/pubs/reports/hazen/pub74.html

- National Archives of Australia. *Digital Recordkeeping Guidelines for Creating, Managing and Preserving Digital Records*. May 2004. Available online at www.naa.gov.au/

- National Archives of Australia. *General Disposal Authority for source records that have been copied, converted or migrated.* February 2003. Available online at www.naa.gov.au/

- Public Record Office Victoria. Scanning or Imaging of Records: Advice to Victorian Agencies. June 2001.

- Public Record Office Victoria. *System Requirements for Archiving Electronic Records*. PROS 99/007 Specification 1.

- Queensland State Archives. Guideline for the Digitisation of Paper Records. April 2006.

- Rothenberg, J. 1998. *Avoiding Technological Quicksand: Finding a Viable Technical Foundation for Digital Preservation*. Council on Library and Information Resources. Available online at www.clir.org/pubs/reports/rothenberg/contents.html

- Smith, A. February 1999. *Why Digitize?* Council on Library and Information Resources. Available online at www.clir.org/pubs/reports/pub80-smith/pub80.html

- Standards Australia. Australian Standard AS/NZS 4360 –1999 – Risk Management

- Standards Australia. Australian Standard HB 171 – 2003 – "Guidelines for the management of IT evidence"

- State Archives of Western Australia. Records Management Standards for Document Imaging Systems. March 1994.

- State Records Authority of New South Wales. *Digital Imaging and recordkeeping*. Recordkeeping in Brief 11. Available online at www.records.nsw.gov.au/publicsector/rk/rib/rib11.htm

- State Records of South Australia. *EDRMS Design Standard*. August 2009.

- State Records of South Australia. Management of E-mail as Official Records: Policy, Guidelines and Technical Considerations. May 2007.

- State Records of South Australia. *Adequate Records Management Standard*. March 2002.

- State Records of South Australia. *Adequate Records Management: Improvement Matrix*. March 2002.

- State Records of South Australia: *South Australian Recordkeeping Metadata Standard* (SARKMS). August 2009.

- Wilkinson, Ross and Andrew Waugh. 2000. 'Preserving System Independent Electronic Records: Theory and Practice', Informaa, 16(1): 15-19.

Glossary

SRSA has developed a comprehensive glossary based upon a number of sources. Where a definition exists within current legislation, such as the *State Records Act 1997*, it will take primacy. If no definition is available within legislation, the primary source is Australian Standard AS ISO 15489 Records Management.

The glossary is available on the SRSA website, www.archives.sa.gov.au.