Government of South Australia

State Records
of South Australia

EDRMS Functional Specification

Standard

August 2009

Version **3**

Table of Contents

Introduction

This Specification details the South Australian Government defined recordkeeping and business functional compliance requirements for proposed Electronic Document and Records Systems (EDRMS). Compliance with this Specification is **mandatory** for meeting the *Document and Records Management Systems Standard 2009*.

This document <u>needs</u> to be read in conjunction with the:

- *EDRMS Design Standard* (2009)

- *Document and Records Management Systems Standard* (2009)

- *South Australian Recordkeeping Metadata Standard* (SARKMS) (2009)

- *EDRMS Procurement and Pre-Implementation Guideline* (2009)

- *Digitisation of Official Records and Management of Source Documents Guideline* (2005)

- *Glossary of Records Management terms*.

These documents are available from the website of State Records of South Australia (SRSA) **http://www.archives.sa.gov.au.**

It is expected that any proposed EDRMS will have inherent functionality or seamlessly integrated components that will support the ability to deliver content management and process management outcomes as well as the mandatory document and records management requirements.

Respondents should also ensure they provide sufficient evidence to substantiate their proposed solution's functional compliance (e.g. screen dumps when performing a particular function, detailed explanations of how the function works, etc). It should be noted that assessment of compliance with this Functional Specification is not subjective and that all requirements are mandatory and must be adequately addressed. Equally, functionality that does not appear as a legitimate functional element will be deemed non-compliant (e.g. it is not sufficient to determine records disposal through reporting functionality, disposal criteria having been established at the point of document/file creation should enable automated viewing of records for disposal by the administrator).

Respondents should note that this EDRMS Functional Specification is an updated version to the copy (Version 2.0) previously published to the website of State Records of South Australia.

Scope

This Standard is issued in accordance with sections 7(h) and 14 of the *State Records Act 1997*. As stated in section 14(2) of the *State Records Act 1997*, this standard is binding for administrative units of the public service and agencies or instrumentalities of the Crown.

Although other agencies, including local government authorities, are not bound by State Records' standards, they are strongly encouraged to apply this Standard to ensure adequate records management practices.

This Standard takes effect from 1 August 2009. From that date any procurement of an EDRMS must adhere to this Standard.

S.A. Government Standards

It is recommended that EDRMS suppliers unfamiliar with the South Australian Government's records management regulatory environment download the following documents from State Records' website:

- *State Records Act 1997*

- *Adequate Records Management (ARM) Standard* (2002)

- *Adequate Records Management - Improvement Matrix and Evidence Toolkit* (2007)

- *Across Government Records Management Strategy* (2004)

- *EDRMS Procurement and Pre-implementation Guideline* (2009)

Further government IT standards relevant to the operating environment for SA Government can be found at:

http://www.cio.sa.gov.au/policies-and-standards/technology/index_html.

Total Solution Requirements

It is a **mandatory** requirement that an EDRMS solution:

1. Is released in the Australian market (the version being bid) and is fully functional in at least one organisation (other than own) located in Australia.
2. Is currently supported in the Australian market by the Supplier.
3. Provides a complete solution, not a partial solution.
4. Is compliant with all specifications (1 to 5) of the *Victorian Electronic Recordkeeping Standard* (VERS) Version 2.
5. Meets all (100%) of the functional requirements as an "off the shelf" solution without significant customisation.

Functional Specification Requirements

Arrangement of this Functional Specification

The **mandatory** Functional Specification requirements are detailed in the table/s below.

- Each section begins with the heading of the Document and Records Management System Standard Principle e.g. *Risk Management, Reporting*, etc.

- Following each principle an element of that principle is identified in the table, e.g. *Capture and management of records*

- Under each element in the table, the business function is stated and the functional requirements are identified.

Where required, reference is made to other documents in the Notes & Comments section of the table.

1. General Solution Requirements

Standard Element: **Capture and Management of Records**	Notes & Comments
1.1 The solution is user friendly, modular, integrated, has a graphical user interface, is accessible from remote locations and is interoperable with other desktop office systems and business applications.	Refer to government IT standards.

1.1.1   The solution is user friendly incorporating the following elements:
• The solution interface is presented consistently across all windows, menus, commands and functions.
• The solution is logical to operate and simple to learn taking into account the differing needs and abilities of potential users.
• The solution's functions are intuitive and as easy to use as possible by enabling:
   - functions to be performed with as few mouse clicks or keystrokes as possible and
   - the completion of routine functions from one screen
• The solution ensures that minimal movement between screens is required to perform system operations.
• The solution makes consistent use of function keys, hot-keys and short-cut keys across all modules and components.
	Refer also to section 7.4 for solution Help requirements.

1.1.2 The solution provides a web browser interface across all modules and components/functions with the exception of the Administration module and functions, which allows users to operate independently from remote locations. The web browser interface must meet the *South Australian Government Web Site Standards and Protocols*.	
1.1.3 The solution interfaces or integrates (as required) with standard office applications, including email and business applications.	Refer to government IT standards.
1.1.4 The solution is modular – that is, agencies need only purchase and pay for functionality that is required.	

2. Risk Management Requirements

Standard Element: **Capture and Management of Records**	**Notes & Comments**
2.1 Rely upon records as an accurate record of the activity/activities that they document. 2.1.1 The solution ensures records may be relied upon as an accurate record of the activities that they document.	The solution must meet all Risk Management functional compliance requirements to fulfil this statement.
2.2 Capture and register physical and digital documents and records, regardless of format and technical characteristics from within the source software package or the system software. 2.2.1 The solution captures physical and digital documents and records, regardless of format and technical characteristics, from: • within the EDRMS solution software; and • within the source software This includes the capture of web content, documents and assets published on the Intranet/Internet. 2.2.2 The solution allows users to capture, register and store all digital documents and records in their native format. 2.2.3 The solution captures physical and digital documents and records upon saving or receipt. 2.2.4 The solution captures physical records that have been digitised using OCR and imaging technologies. 2.2.5 The solution enables the user to capture e-mail and all it's attachments as a single record or as separate records whilst maintaining a link between the email and the attachments. 2.2.6 The solution captures a dynamic document, such as a dynamic web page, as a snapshot 'frozen' in time as well as one or more of the following: • a single compound record, or • an aggregation of linked component records, or • a collection of assets that can be regenerated upon request or • a combination of the above. 2.2.7 The solution must make a clear and obvious distinction between digital documents and registered digital records. 2.2.8 The solution provides options for registering all unregistered digital documents in a particular folder or folders as formal records, in a single process. 2.2.9 The solution enables digital documents to be registered as records prior to disposal. 2.2.10 The solution allows users to transfer smoothly between the document management environment and the records management environment to register a digital document as a digital record.	Refer to government IT standards. Source software may include, but is not limited to: • standard office applications • workflow applications • email systems • e-commerce and web transactions • imaging and graphic design systems • barcode support systems; • library management systems; • corporate systems; • business information systems; • security administration systems; • multimedia applications

Standard Element: **Capture and Management of Records**	**Notes & Comments**

2.3   Manage physical and digital documents and records, using records management principles and practices, regardless of format and technical characteristics.
 	
2.3.1   The solution is compliant with Records Management Standard AS ISO 15489.
 	
2.3.2   The solution manages physical and digital documents and records regardless of format and technical characteristics.
 	
2.3.3   The solution accepts and processes information that contains dates in current, previous and future centuries, at a minimum:
   • century recognition;
   • calculation and logic that allows for same century and multi-century formulas and date values; and
   • leap year calculations.
 	
2.3.4   The solution manages and preserves physical and digital documents and records, regardless of format and technical characteristics so that when retrieved they can be reproduced, viewed, and manipulated in the same manner as the original.
 	
2.3.5   The solution enables the System Administrator or accredited RM practitioner to create and maintain a relationship link between the physical and digital record in a mixed folder consisting of both physical and digital documents.
 	
2.3.6   The solution prevents any unauthorised modifications to the content of a version of a registered physical or digital record.
 	
2.3.7   At the time of capture the solution attaches the physical or digital record to an aggregated hierarchical structure within which physical and digital records can be stored either physically or virtually (refer to requirement 2.15 for details), as specified in VERS Standard Version 2. The record takes on the disposition of the storage unit.
 	
2.3.8   The solution prevents the unauthorised destruction or deletion of registered physical and digital records and associated metadata at all times.
 	
2.3.9   The solution allows only the System Administrator to authorise and confirm the destruction of records approved for destruction before the operation is executed.
 	
2.3.10   The solution destroys or deletes records (and preserves the metadata) that are stored in its repository and have been approved for destruction in a manner such that the records cannot be reconstructed.
 	
2.3.11   The solution has a viewable registry entry including associated metadata for each registered record.
	Evidence of compliance will be that the solution meets all other functional compliance requirements within this document.
	
	Formats may include, but not be limited to:
	• Word-processing documents
	• Spreadsheets
	• E-mail and attachments
	• Voice Mail
	• Digitally recorded images
	• Drawings
	• Databases
	• Objects (eg audio, video)
	• GIS (Geographical Information Systems)
	• Maps
	• Plans
	• Web content, documents and assets
	• OCR documents
	• Images - tif, jpg, gif, etc.

Standard Element: **Capture and Management of Records**	Notes & Comments
2.4 *Manage digital records in a consistent, open and enduring format as VEOs utilising Extensible Markup Language (.xml) and Portable Document Format (.pdf) as specified in VERS Version 2.* 2.4.1 The solution maintains and stores digital records in their native format for as long as required. 2.4.2 The solution stores permanent inactive digital records in an open and enduring format as VEOs, as specified in VERS.	Native formats may include: • DOC • SVF • XLS • PDF • PPT • GIF • HTML • JPG • XML • MPG • DWG • DPF • TIF • DXF • IMG • FIL • TXT • INP • DWF • MDB • MOD • PC etc.
2.5 *Identify and manage all vital records.* 2.5.1 The solution allows users to flag records identified as vital. 2.5.2 The solution identifies when vital records are due for review and update.	

Standard Element: **Storage**	Notes & Comments
2.6 *Store data distributed across a number of databases and/or servers in a number of physical locations.* 2.6.1 The solution stores and retrieves physical and digital document and record data within integrated and distributed repositories and storage environments.	Refer to government IT standards.
2.7 *Store physical and digital documents and records appropriately and efficiently.* 2.7.1 The solution stores physical and digital document and record data in variable length fields, storing only the data that is entered with no empty spaces. 2.7.2 The solution prevents or resolves any conflicts caused by changes to storage repositories and locations. 2.7.3 The solution allows only the System Administrator to move or delete physical and digital documents and records outside of the disposal process. 2.7.4 The solution stores metadata in an easily searchable format, not just in audit logs. 2.7.5 The solution enables the System Administrator to generate a report on the size and remaining capacity of its digital record stores and repositories.	

Standard Element: **Tracking and Version Control**	**Notes & Comments**
2.8 Track the location of physical records and the assignment of digital documents and records as specified in VERS Version 2. 2.8.1 The solution tracks and provides an audit log of the location of physical and digital records. 2.8.2 The solution tracks a physical or digital document or record's location by providing check-in and checkout facilities that record the checkout location of the document or record and the dates of checkout and check-in. 2.8.3 The solution tracks all copies made of digital records, recording the movement of all copies in the audit log. 2.8.4 The solution provides an audit log that tracks access to physical and digital records. 2.8.5 The solution automatically tracks records and the storage units they are contained in as they progress through their life cycle. 2.8.6 The solution will track the history of a physical or digital record at each level of the hierarchical structure within which physical and digital records can be stored either physically or virtually (refer to requirement 2.15 for details on hierarchical structure). This history should include the following information: • current location; • previous locations; and • associated dates. 2.8.7 The solution provides ordering and reserve facilities, allowing a user to request a physical or digital record checked-out to another location (user). This action transmits a message to the location (user) or escalates to the System Administrator for action.	Location may be a physical location or an assignment to a workgroup or user
2.9 Maintain version control for all physical records and digital documents and records. 2.9.1 The solution captures and maintains each version of a physical record and digital document and record. 2.9.2 The solution provides options for registering some or all versions of a digital document as digital records. 2.9.3 The solution identifies the latest version as well as all other versions of a physical and digital document and record. 2.9.4 The solution increments versions of physical and digital documents and records at the time of capture. 2.9.5 The solution must be able to copy a digital record to make a new digital document or record, ensuring the original digital record remains intact. 2.9.6 The solution ensures that when a document or record is annotated, marked up or modified in any manner, a new version of that document or record is created.	

Standard Element: **Tracking and Version Control**	**Notes & Comments**
2.9.7 The solution allows the user to create versions of digital documents, without automatically creating a new digital record. 2.9.8 The solution supports versioning of web content, documents and assets at the item and aggregate levels.	
2.10 Capture and maintain a complete record of all events performed within the system as an audit trail. 2.10.1 The solution automatically captures and maintains a complete record of all events performed within the system as an audit trail, including: • creation of a new user or group • registration of all records • movement and location of a record • access to a record • changes to access and security affecting a record, folder or user • relocation of records to another folder, identifying both origin and destination • relocation of a folder to a different part of the record plan, identifying both origin and destination • changes made to metadata associated with folders or records • all disposal review decisions made by a System Administrator • reapplication of a disposal authority to an entity, identifying both previous and subsequent authorities • placing or removing of a disposal freeze on a record or folder • a separate log of all deletion or destruction actions carried out by any user • reclassification of a record or folder • changes to the classification scheme/s The solution records: • the action carried out • the object of the action • the user undertaking the action and • the date and time of the event 2.10.2 The solution ensures that actions undertaken by a System Administrator are captured in the audit trail, including configuration and reconfiguration of the audit trail itself. 2.10.3 The solution records the details of all activities performed on digital records, at the item and aggregate levels and all associated metadata. 2.10.4 The solution ensures that the System Administrator can backup and remove audit files from the system on a regular basis by capturing the current audit file as a record and initiating a new version of the audit file. This action is to be performed as a single process. These records are to be retained in accordance with *General Disposal Schedule 15 and 20*.	The solution must meet all audit trail functional compliance requirements to meet this statement.

Standard Element: **Tracking and Version Control**	**Notes & Comments**
2.11 *Track physical and digital documents and records through changes of custody e.g. through organisational change or outsourcing.* 2.11.1 The solution tracks physical and digital documents and records through various changes in custody (e.g. through organisational change or outsourcing).	

Standard Element: **Disposal**	Notes & Comments
2.12 Ensure all physical and digital records are disposed of in accordance with the provisions of the State Records Act or other legislation that authorises such disposal.	The solution must meet all Disposal functional compliance requirements to meet this statement.
2.12.1 The solution allows all physical and digital records to be disposed of in accordance with the provisions of the *State Records Act 1997* or other legislation that authorises such disposal.	
2.12.2 The solution must support the definition and application of the following disposal actions: • review • export • transfer • destruction	Transfer consists of confirmed export followed by destruction, once the success of the transfer process has been confirmed.
2.12.3 The solution allows the System Administrator to identify eligible records for disposal and preserve metadata for: • interim transfer • archiving • destruction	
2.12.4 The solution exports and transfers only registered digital records, not unregistered digital documents.	
2.12.5 The solution automatically destroys digital items when the digital records to which those items relate are destroyed subsequent to a successful transfer process.	
2.12.6 The solution retains appropriate transfer metadata as specified by VERS Version 2 when records are transferred.	
2.12.7 The solution records all disposal actions in an audit trail.	
2.12.8 The solution restricts the operation of the disposal process to the System Administrator or accredited RM practitioner.	
2.12.9 The solution enables the System Administrator or accredited RM practitioner to generate reports on a regular basis of all disposal actions on folders due for destruction in a specified period of time.	
2.12.10 The solution is able to import and export General Disposal Schedules or other operational Records Disposal Schedules approved for a specific agency in a tabular format.	
2.13 Dispose of records in accordance with current General Disposal Schedules (or other operational Records Disposal Schedules approved for a specific agency).	
2.13.1 The solution provides for the use of multiple disposal schedules, details of which can be imported from a tabular format, entered manually on an ad-hoc basis as well as exported as required.	
2.13.2 The solution provides for a disposal schedule to automatically be attached as a default to the classification scheme, record type and record	

Standard Element: **Disposal**	Notes & Comments
class.	
2.13.3 The solution allows disposal classes to be applied to physical and digital records at the item, folder and aggregate levels.	
2.13.4 The solution automatically assigns a unique identifier to each disposal class and, where applicable, must allow the disposal class to be associated with the appropriate disposal schedule.	
2.13.5 The solution stores the archive and destruction date in a way that allows for all records to be automatically or globally updated if the disposal schedule changes.	
2.13.6 The solution automatically calculates when disposal of records are due in real time, based on the disposal schedule.	
2.13.7 The solution automatically updates the disposal date of all records if the disposal schedule changes.	
2.13.8 The solution automatically seeks confirmation from a System Administrator or accredited RM practitioner before implementing any disposal action.	
2.14 Apply a disposal or retention sentence at creation of the document and the record type (via the classification), which can be modified on an ad hoc or global basis by the System Administrator or accredited RM practitioner.	
2.14.1 The solution applies a disposal schedule at capture of a record based on its classification, record type or record class.	
2.14.2 The solution provides for the retention period to be described by common word(s) and not a cryptic code.	
2.14.3 The solution allows the System Administrator or accredited RM practitioner to modify the disposal or retention criteria on an ad hoc or global basis including the ability to track alterations of entries, recording date of modification and name/initials of the person making the entry.	
2.14.4 The solution allows the System Administrator or accredited RM practitioner to alter retentions of records during any phase of their life cycle if the retention changes from their original designations.	
2.14.5 The solution sorts, views, saves and prints the next disposition action and due dates of records identified by the accredited RM practitioner.	
2.14.6 The solution allows the System Administrator or accredited RM practitioner to search within the disposal schedule.	
2.15 Implement an aggregated hierarchical structure within which physical and digital records can be stored either physically or virtually to ensure accurate disposal (Refer to SARKMS, VERS Version 2 and the EDRMS Design Standard).	
2.15.1 The records and metadata of permanent records to be transferred to State Records conform to State Records' specific criteria and formats (refer to the EDRMS Design Standard).	

Standard Element: **Disposal**	Notes & Comments

2.15.2   The solution aggregates <u>physical</u> records in a hierarchical structure within which the records can be stored physically. The aggregation occurs in the following order:
 	
    •   multiple Records stored within a Folder
    •   multiple Folders stored within a Storage Unit, that is a box
    •   multiple Storage Units within a Consignment
    •   multiple Consignments within a Government Record Series (GRS)
 	
    There will be multiple Government Record Series (GRS) within an agency.
 	
2.15.3   The solution aggregates <u>digital</u> records in a hierarchical structure within which the records can be stored virtually. The aggregation occurs in the following order:
 	
    •   multiple Records stored within a Folder (activity)
    •   multiple Folders stored within a Storage Unit, that is a Function
    •   multiple Storage Units (functions) within a Consignment
    •   multiple Consignments within a Government Record Series (GRS)
 	
    There will be multiple Government Record Series (GRS) within an agency.
 	
2.15.4   The solution enables the System Administrator or accredited RM practitioner to establish and maintain relationship links between the physical storage unit/s and the virtual Function/s in a mixed Consignment.
 	
2.15.5   The solution creates and maintains relationships between series including:
 	
    •   previous series
    •   subsequent series and
    • related series	

Standard Element: **Functional Continuum**	Notes & Comments
2.16 Jointly use records between related agencies, where relevant (such as after restructuring, amalgamation, resource re-allocation or business process re-engineering). 2.16.1 The solution allows records to be used jointly between related agencies, in situations such as restructuring, amalgamation, resource re-allocation and business process re-engineering, by enabling records to be rendered and viewed in an open and enduring format as VEOs as specified in *VERS Version 2*. 2.16.2 The solution supports the long-term management of encapsulated objects as VEOs as specified in *VERS Version 2*. 2.16.3 The solution has the ability to define, integrate and automate across organisational business rules and processes.	The solution must also meet all Migration, Metadata and Conversion functional compliance requirements to meet this statement.

Standard Element: **Migration**	Notes & Comments
2.17 Ensure that when implementing a new system, migration of data between the new and existing systems occurs, including metadata for inactive records and from inactive databases. 2.17.1 The solution migrates data between the old and the new systems, including metadata for inactive records: • Data is to be accepted from other document and records systems • Data migration is to include metadata from inactive databases and • The solution is to be capable of importing and exporting data including associated metadata in an open and enduring format as specified in *VERS Version 2* for the purpose of migration. 2.17.2 The solution generates a report detailing any failure during a migration process from the system, identifying objects that have generated processing errors or were not successfully migrated. 2.17.3 The solution is able to migrate digital records, folders and other record plan entities (where supported), and associated metadata in accordance with the requirements for export and import (Refer also to section 4.4)	

Standard Element: **Conversion**	Notes & Comments
2.18 Ensure that appropriate conversion and test processes are used so that data migrated to a new system is not corrupted or altered in such a manner that it may affect the evidentiary integrity or completeness of the record during the process. 2.18.1 The solution has conversion tools and test processes to ensure that no data is lost or corrupted during system upgrades, migration or conversion. 2.18.2 The solution is able to perform a bulk conversion of digital records, and associated metadata to an open and enduring format as specified in *VERS Version 2*. 2.18.3 The solution supports long-term archival data preservation formats, as specified in *VERS Version 2*, including: • the ability to store and manage digital records in archival data preservation formats, and • the ability to convert digital records to archival data preservation formats during capture or export.	

3. Reporting

Standard Element: **Business Process Management**	Notes & Comments
3.1 Ensure that access, control and security requirements are being met by the system by employing reporting tools within the system 3.1.1 The solution uses a tool that allows for the interrogation of and reporting on the data that multiple databases contain (please name both internal and third party tools proposed and supported). 3.1.2 The solution uses reporting tools to satisfy access, tracking and control requirements via an in-built and/or external report writer or common desktop software. Results should be extractable in a variety of formats. 3.1.3 The solution provides a reporting capability to produce management, statistical and ad hoc reports on system activity. 3.1.4 The solution uses tools for interrogation and reporting of breaches in security. 3.1.5 The solution can produce reports on: • the level of access a user has; • the records each user has accessed; and • the operations that were performed on those records and associated metadata.	
3.2 Use reporting and analysis tools for the management of retention and disposal policies. 3.2.1 The solution reports on all disposal activity undertaken by the system. 3.2.2 The solution reports on when disposal of records is due.	Refer also to requirement 2.10

Standard Element: **Business Process Management**	Notes & Comments
3.2.3 The solution reports on the volume and types of objects that are overdue for disposal.	
3.2.4 The EDRMS generates a report listing: • all disposal classes currently defined in the system; • all physical and digital records, folders or other record plan entities (where supported) to which a particular disposal class is currently applied; • all digital objects for which a particular disposal action will occur, over a given period of time; and • all objects due for disposal within a given period of time, providing quantitative information on the volume and type of records.	
3.2.5 The solution notifies the System Administrator or accredited RM practitioner that a physical or digital record within a workflow process is due for disposal.	
3.2.6 The solution generates a report detailing the outcome of a destruction process, detailing all physical and digital records successfully destroyed and identifying those records that were **not** successfully destroyed.	
3.3 Manage and monitor the progress of activities (that is 'workflow') associated with document content (in the context of business process management).	
3.3.1 The solution enables the System Administrator to design business process workflow definitions by identifying the set of activities/tasks that must be completed end-to-end (across workgroup, unit or agency) to fulfil a business process.	
3.3.2 The solution provides tools to model, simulate, deploy and operate end-to-end sequential and parallel business processes.	
3.3.3 The solution provides an environment within which business rules can be defined, integrated, deployed and managed across business processes.	
3.3.4 The solution enables the System Administrator to design, assemble, deploy and manage serial and parallel business process workflows based on the defined workflow definitions and business rules.	
3.3.5 The solution must not limit the number of business process workflows that can be defined.	
3.3.6 The solution supports the ability to integrate business process workflows with existing business applications (e.g. Masterpiece, CHRIS, etc) at 'integration points' in the process flow.	
3.3.7 The solution supports conditional process workflows, where the direction of a workflow is determined by user input or system data.	
3.3.8 The solution stores process definitions in a separate repository to the business process workflows.	
3.3.9 The solution monitors the progress of activities/tasks through the	

Standard Element: **Business Process Management**	Notes & Comments
workflow (workflow management).	
3.3.10 The solution provides process diagnostic tools that enable the System Administrator to identify and resolve business process workflow issues and to continually improve business process workflows.	
3.3.11 The solution progressively captures process workflow metadata for physical and digital records, as specified in SARKMS and VERS Version 2 Specification 2.	
3.3.12 The solution notifies the action officer responsible for a workflow process, via email that a particular activity/task within a defined process is overdue.	
3.3.13 The solution notifies the responsible manager/supervisor of a process via email that a particular activity/task within a defined process is overdue with the name of the person responsible for that task.	
3.3.14 The solution enables the System Administrator to reassign responsibility for a workflow activity/task.	
3.3.15 The solution provides comprehensive reporting facilities to allow the monitoring of the amount of traffic, performance, and exceptions of workflow activities/tasks and processes.	
3.3.16 The solution records all changes to defined process workflows in the audit trail.	
3.3.17 The solution applies user access privileges and information security classification to physical and digital documents and records that are within process workflows.	

Standard Element: **Report Generation**	Notes & Comments
3.4 Ensure generation of a number of reports, from multiple databases as required, for: • *disposal, for example: the number of folders eligible for destruction, a list of all folders and parts that do not have a disposal action allocated, etc;* • *general statistical purposes, for example: reports on number of folders created or number of folders retrieved and viewed;* • *data and user administration (including activity of Administrator);* • *activity within the classification structure; and* • *other aspects of records in the system.* 3.4.1 The solution provides standard management reports **w**ithin a specified date range for activity relating to, as a minimum: • retention and disposal activity • process workflow • users or groups of users • classification • archival management • destruction; • file and document storage units • access • security • general statistics • data and user administration (including activity of Administrator) and • vital records (when last reviewed and updated).	
3.5 Generate, save, modify, sort and re-use report formats. 3.5.1 The solution allows reports to be generated, saved, modified and re-used in the future. 3.5.2 The solution allows generated reports to be easily saved, printed or exported from the system.	
3.6 Report on user-defined search results.	The solution must meet the functional compliance requirements in 2.10, 3.4 and 3.7 to meet this statement.

Standard Element: **Audit Reports**	Notes & Comments
3.7 Access audit trails and audit reports for all transactions (including system administration). 3.7.1 The solution produces audit reports for all events and transactions (including system administration). 3.7.2 The solution produces ad hoc audit reports by drawing on relevant data from the audit trail.	
3.8 Define and customise information required for an audit trail and report. 3.8.1 The solution allows the System Administrator to define or customise data for reporting and audit requirements.	

4. Metadata

Standard Element: **Capture**	Notes & Comments
4.1 Complies with the South Australian Recordkeeping Metadata Standard (SARKMS), the EDRMS Design Standard and VERS Version 2 Specification 2. 4.1.1 The Solution complies with the *South Australian Recordkeeping Metadata Standard,* the EDRMS Design Standard and VERS Version 2 Specification 2.	
4.2 Use a unique identifier for each record. 4.2.1 The solution automatically assigns a unique system identifier for each physical and digital document and record as it is registered, and stores this identifier as metadata with the record. 4.2.2 The solution automatically assigns a unique system identifier for all other entities (e.g. folders, storage units, disposal schedules, consignments, etc). 4.2.3 The solution allows the System Administrator to define the format of additional unique identifiers (not those that are system generated) used by the agency to identify entities such as documents, records, folders, storage units, disposal schedules, etc, at capture. 4.2.4 The solution enables the System Administrator or an accredited RM practitioner to assign default metadata values based on record type, classification and record class.	
4.3 Capture metadata (as specified in the South Australian Recordkeeping Metadata Standard (SARKMS), the EDRMS Design Standard and VERS Version 2 Specification 2) in relation to all documents, regardless of format and technical characteristics, for: • content including the title, subject, description, language and coverage • registration including the records identifier, date and location of the document	

Standard Element: **Capture**	Notes & Comments
- structural elements including type, aggregation level and format of the document and its preservation history - contextual elements such as the document's agent, relation and function - history including management history and use history and - terms and conditions including access rights and disposal actions.	
4.3.1 The solution automatically captures digital documents and records metadata acquired directly from an authoring application, an operating system, or generated by the EDRMS itself for the metadata elements.	
4.3.2 The solution captures physical or digital document and record metadata entered manually by a user during registration for the metadata elements.	
4.3.3 The solution enables the capture of digital document and record metadata at the time of creation and registration.	
4.3.4 The solution supports the mapping of digital document metadata to digital record metadata.	
4.3.5 The solution allows automatically captured metadata to be edited prior to registration of the record.	
4.3.6 The solution ensures that mandatory metadata fields are populated before storing the record.	
4.3.7 The solution creates, saves, displays and prints the complete document and record metadata.	
4.3.8 The solution stores or links the record metadata to the record so that it can be displayed when needed and transferred to another location with the record when required.	
4.3.9 The solution stores metadata over time, regardless of whether the related record has been archived, deleted, destroyed or transferred.	
4.3.10 The solution automatically records the closing date of a folder and utilises this metadata to support other records management functions, such as disposal.	

Standard Element: **Maintenance**	Notes & Comments
4.4 Import and export document and file profile information, thesaurus and disposal schedules between system databases, and between applications as VEOs as specified in VERS Version 2. 4.4.1 The solution is able to export all physical and digital records and associated metadata it has captured, regardless of format or the presence of the generating application. 4.4.2 The solution enables the System Administrator to export records, folders, aggregated storage units or other record plan entities, and all associated metadata to: • another EDRMS within the Department/Portfolio • an EDRMS in a different agency or • State Records for the long-term preservation of permanent physical and digital records. 4.4.3 The solution ensures that any export action includes: • all records and associated storage units that qualify for export under a disposal class • all metadata associated with exported records, associated storage units and other record plan entities and • all audit trail data associated with exported records. 4.4.4 The solution is able to generate a report detailing any failure during an export of records from the system, identifying objects that have generated processing errors or were not successfully exported. 4.4.5 The solution imports records and associated metadata including record and file profile information, classification schemes and disposal schedules and classes. 4.4.6 The solution enables the System Administrator to perform a bulk import of records with associated metadata that is presented in accordance with the *EDRMS Design Standard* mapping this to the receiving structures. 4.4.7 The solution is able to import digital records as VEOs.	
4.5 Develop document and record profiles and specifications at a System Administrator level. 4.5.1 The solution enables the System Administrator to develop document profiles and specifications. 4.5.2 The solution captures and maintains metadata relating to any records classification scheme/s it supports, in accordance with the EDRMS Design Standard. 4.5.3 The solution enables the System Administrator to determine, configure and potentially customise the interface (content, layout etc.); please indicate which method is to be used.	The solution must meet all Security, functional compliance requirements to meet this statement
4.6 Effect global changes to specific fields, at a System Administrator level. 4.6.1 The solution allows the System Administrator to define optional	

Standard Element: **Maintenance**	Notes & Comments
metadata fields as mandatory.	
4.6.2 The solution allows the System Administrator to effect global changes to specific metadata fields.	
4.6.3 The solution allows the System Administrator to define new metadata fields.	
4.6.4 The solution allows the System Administrator to define metadata validation rules.	
4.6.5 The solution enables the System Administrator to restrict the ability to amend record metadata, so that: • selected metadata elements can be edited by <u>any</u> user during registration • selected metadata elements can only be edited by an <u>authorised</u> user during registration and • selected metadata can be edited by an <u>authorised</u> user <u>after</u> registration.	
4.7 Ensure long-term preservation of data through comprehensive migration practices.	
4.7.1 The solution stores metadata over time, regardless of whether the related record has been archived, deleted or destroyed.	
4.7.2 The solution manages digital records as specified in *VERS Version 2* to ensure their integrity and support long-term preservation.	
4.7.3 The solution developer must have a program in place to ensure that digital records remain accessible and retain their integrity after a system upgrade.	

Standard Element: **Accuracy**	**Notes & Comments**
4.8 Ensure accuracy during data capture and entry. 4.8.1 The solution uses an integrated spell checker and has the ability for authority lists to be invoked during text entry in all profile (metadata) input fields (except numerical or code fields). 4.8.2 The solution allows the System Administrator to customise the spell checker. 4.8.3 The solution enables the System Administrator to manage and maintain pop-up or pull-down menus and pick lists to assist the entry of metadata. Menus and pick lists: • are easily accessible to the user • are able to be modified by the System Administrator • upon amendment will update the data previously assigned to records 4.8.4 The solution enables the System Administrator to define and maintain system templates (data entry forms) that automatically populate commonly used data into record metadata fields.	

5. Accessibility

Standard Element: **Appropriate Access**	Notes & Comments
5.1 Ensure that all physical and digital documents and records, regardless of format and technical characteristics, are accessible by authorised users in accordance with information security classification and user access profile.	The solution must meet all Access, Security and Risk Management functional compliance requirements to meet this statement.
5.1.1 The solution allows access to physical and digital documents and records, regardless of format and technical characteristics from any single point of access in accordance with the information security classification assigned to the document or record and user access profile assigned to the user.	
5.1.2 The solution retrieves and displays digitised records.	
5.1.3 The solution allows simultaneous viewing of digital documents and records by all authorised users in accordance with information security classification and user access profiles.	
5.1.4 The solution withholds all or part of a search result, according to user access privileges and information security classification.	
5.2 Ensure that access to physical and digital documents and records is subject to South Australian Government archives, freedom of information, security, privacy and confidentiality legislation and requirements. This includes the Information Privacy Principles as well as agency specific legislation as well as the ability to support business rules that manage personal, confidential, NAP and corporate documents and records. For example access to personal information, commercial-in-confidence information, or other sensitive information that must not be misused, intentionally or unintentionally, either within the agency or when shared with external organisations, groups or individuals.	The solution must meet all Access, Security and Risk Management functional compliance requirements to meet this statement.
5.2.1 The solution distinguishes between documents and records that are openly available and those that are restricted.	A user group may consist of a single user. A person may belong to more than one user group.
5.2.2 The solution captures metadata that supports privacy, freedom of information, archives and agency specific legislation including: • information about the release of physical and digital records • information which may be/is used to retrieve details from another system • disclosability and exemption indicators and • access determinations as specified in SARKMS	
5.2.3 The solution restricts access to physical and digital documents and records, folders, associated storage units and other entities in the record plan to members of a user group/s who have been allocated an equivalent or higher security category within their user group/s in accordance with the user access profiles.	
5.2.4 The solution captures, registers and maintains digital documents and records that are encrypted, or bear digital signatures or digital watermarks.	
5.2.5 The solution captures, registers and maintains an encrypted digital document or record directly from an application capable of encryption.	

Standard Element: **Appropriate Access**	Notes & Comments

5.2.6   The solution stores digital documents and records in either an encrypted or unencrypted form.
 	
5.2.7   The solution automatically or manually captures metadata elements, at the time of registration, as specified in the *EDRMS Design Standard* for digital documents and records:
    • that have been encrypted
    • bear digital signatures
    • bear digital watermarks
 	
5.2.8 The solution must be able to remove access restrictions from a permanent, inactive record when the record is transferred to another agency or archives.	

5.3 Provide access to records, under the Freedom of Information legislation, through appropriate storage and security. 5.3.1 The solution must allow access to records, under the Freedom of Information legislation, through appropriate classification, storage and security. 5.3.2 The solution enables an accredited RM practitioner to amend the information security classification of a physical or digital document or record to "open" when released under the auspices of Freedom of Information legislation.	The solution must meet all Access, Security and Risk Management functional compliance requirements to meet this statement.
5.4 Easily access digital records in their native format environment. 5.4.1 The solution enables digital documents and records to be accessed in their native format for as long as required and practicable. 5.4.2 The solution enables permanent inactive records to be accessible in an open and enduring format as VEOs as specified in VERS Version 2.	

Standard Element: **Classification**	Notes & Comments

5.5   Ensure that all records are arranged in a logical and controlled manner and that a system of arrangement is in place (i.e. the Keyword AAA thesaurus, or another thesaurus as the agency requires).
 	
5.5.1   The solution allows the System Administrator or an accredited RM practitioner to implement one or more classification scheme/s (e.g. the Keyword AAA thesaurus, or other classification schemes) in order to organise physical and digital records in a logical and controlled manner.
 	
5.5.2   The solution enables physical and digital documents and records, to be classified with the agency's classification scheme/s at the time of creation or registration.
 	
5.5.3   The solution allocates a unique identifier to each term defined with a records classification scheme.
 	
5.5.4   The solution uses hierarchical relationships in a classification scheme, including:
    • Broad Terms
    • Preferred, non-preferred and forbidden terms
    • Related terms
    • Scope notes and
    • Narrower terms
 	
5.5.5   The solution enforces the use of a records classification scheme for naming new objects.
 	
5.5.6   The solution enables the System Administrator to configure the naming mechanisms for entities within the record plan.
 	
5.5.7   The solution permits only the System Administrator or an accredited RM practitioner to define and maintain the records classification scheme/s.
 	
5.5.8   The solution permits only the System Administrator or an accredited RM practitioner to move and reclassify a folder or group of folders, and their attached records.
 	
5.5.9   The solution allows the manual or automatic update of all folder and record metadata attributes that are determined by classification, following reclassification of a folder.
 	
5.5.10 The solution permits only the System Administrator or an accredited RM practitioner to add or modify metadata relating to records classification scheme/s.	

5.6 Define record classification up to four hierarchical descriptor levels. 5.6.1 The solution defines record classification up to four hierarchical descriptor levels. *5.6.2 The solution allows the addition of folders to the lowest levels of a defined records classification scheme in order to organise aggregations of physical and digital records.*	

Standard Element: **Classification**	Notes & Comments
5.6.3 The solution enables lower levels in a defined records classification scheme hierarchy to inherit classification and another related metadata from higher levels, at the time of creation or registration.	
5.7 Browse the thesaurus over a graphical user interface for selection of terms for classification and retrieval. 5.7.1 The solution allows users to browse the classification schemes. 5.7.2 The solution allows users to select terms from the classification scheme for classification and retrieval.	
5.8 Link classification terms to disposal criteria (see Principle 1: Risk Management in the EDRMS Design Standard), allowing for global or individual modification of links. 5.8.1 The solution links classification terms to disposal criteria, allowing for global or individual modification of links.	
5.9 Upgrade and import the existing thesaurus, providing the option for a retrospective change to relevant documents and record types, while maintaining the historical trail of terminology; please name any third party products used for importing. 5.9.1 The solution allows the System Administrator or an accredited RM practitioner to make global amendments to the definition of a records classification scheme in a single process. 5.9.2 The solution enables the existing records classification schemes to be upgraded, providing the option for a retrospective change to relevant records and record types.	
5.10 Report or list records as a group related by business activity, for transfer, in the case of a functional re-allocation either within an agency, or between agencies. 5.10.1 In the case of a functional re-allocation either within an agency, or between agencies, the solution can identify records as a group related by business activity, for transfer. 5.10.2 The solution generates reports listing: • all folders classified within the records classifications scheme; and • all folders classified in a section of the records classification scheme, • structured according to the hierarchy of the record plan or other classification scheme.	

Standard Element: **Searching and Retrieval**	Notes & Comments
5.11 Find records immediately, or with the minimum extra effort, upon demand subject to access privileges.	
5.11.1 The solution provides automatic indexing of all physical and digital document and record data and related metadata upon capture and updating to create and upgrade a full-text index for accurate retrieval.	
5.11.2 When a search is completed the solution displays a list of documents and records meeting the retrieval criteria, or notifies the user if there are no records meeting the retrieval criteria.	
5.11.3 When a search is completed the solution identifies the latest version of the record, but all versions of the record are available for the user to select and view.	
5.11.4 The solution prints the list of documents and records returned by a search query.	
5.11.5 The solution displays the content of all the types of digital documents and records, which it is able to capture, in a manner that presents all components of the digital record together as a unit, subject to security classification and user access privileges.	
5.11.6 The solution displays the content of all the types of digital records it can capture, in a manner that renders their original visual presentation and layout, without needing to load the generating application.	
5.11.7 The solution displays all available metadata associated with a physical or digital document or record and associated storage units upon request.	
5.12 Search and access records without being limited by geographical/server architectural constraints. For example, a specified search should be able to be performed across system databases, across all fields, from a single point of access.	The solution also must meet all Storage and Access functional compliance requirements to fulfil this statement
5.12.1 The solution provides full search functionality (e.g. access and searching), which is not limited by the location of the user.	
5.12.2 The solution provides search facilities to meet the needs of a range of users, from casual to sophisticated.	
5.12.3 The solution provides a help function to give guidance on searching and searching hints, regarding each of the functions under the 'Searching and retrieval' section.	
5.12.4 The solution enables the System Administrator to configure default search options for end users.	
5.13 Link, group and relate documents to other documents or records created or used as part of the same business activity, either specified by the system or user derived (including aggregations such as document to file to box to consignment to records series).	
5.13.1 The solution links, groups and relates records, regardless of format and technical characteristics, to other records created or used as part of the same business activity, either specified by the system or user defined.	

Standard Element: **Searching and Retrieval**	**Notes & Comments**
5.14 *Support technology to generate, read, print and identify barcodes for tracking record movements e.g. files, boxes, etc (please name third party tools proposed and supported).* 5.14.1 The solution supports the production and use of barcodes and barcode technology to track and locate physical records. 5.14.2 The solution enables an accredited RM practitioner to stock-take/audit physical records using barcode technology. 5.14.3 The supplier provides integrated barcode hardware and software with the solution.	

5.15 *Retrieve information by searching the database using at least the following parameters:*
   • Full text;
   • Combined text and field;
   • Keyword;
   • File/document;
   • Metadata field;
   • Date document created/captured;
   • Author of document;
   • Barcode;
   • Location; and
   • Classification scheme.
 	
5.15.1   The solution retrieves information by searching across multiple databases, across all fields, from a single point of access, using the following minimum search functions:
   • Full text
   • Record format
   • Last action
   • Disposal action
   • Disposition (status) of record, i.e. active, inactive, destroyed, archived, transferred
   • Combined text and field
   • Keyword
   • Storage unit and record title and number
   • Dates e.g. records created, captured, destroyed, etc
   • Author of record
   • Barcode
   • Location
   • Classification scheme
   • Unique identifier and
   • Metadata element.	

5.16 *Support a mix of metadata and content searches using controlled lists and combining search terms to conduct simple keyword and complex searches,*	

Standard Element: **Searching and Retrieval**	Notes & Comments
using search terms such as Boolean terms, logical operators, broader and narrower terms, and proximity searches, as required. 5.16.1 The solution allows the user to perform a range of searches, including complex searches to locate a specific record using any combination of the record or metadata elements. 5.16.2 Search terms can be combined in a <u>Boolean search</u> and provide a mechanism, to control order of precedence. The search terms must include, but not be limited to AND, OR, NOT, greater than (>), less than (<), equal to (=), not equal to (<>), and must include a designated "wild card".	
5.17 Refine search criteria and results at a user level, based on operational needs. 5.17.1 The solution allows users to refine or customise search criteria and results. 5.17.2 The solution allows the System Administrator to configure or define the search results window and captions. 5.17.3 The solution allows users to further customise the search results window and captions.	
5.18 Save search parameters. 5.18.1 The solution allows users to save and re-use search parameters. 5.18.2 The solution allows the System Administrator to define and save standard searches.	

6. System Integrity

Standard Element: **Security**	Notes & Comments
6.1 Apply security classification to the user, the record and the record type at creation, which can be modified on an ad hoc or global basis by the System Administrator, if required. 6.1.1 The solution enables the System Administrator to define, manage and modify user access privileges and information security classification that may be applied to users, physical and digital records and other entities in the record plan. 6.1.2 The solution enables user access privileges and information security classification (as specified in SARKMS and VERS Version 2) to be assigned to users, physical and digital documents and records and other entities in the record plan. 6.1.3 The solution requires the allocation of a single information security classification as a minimum to a physical or digital record, folders, associated storage units and other entities in the record plan, with the default being the lowest category that is 'open'.	The solution must also meet all Access, Security and Risk Management functional compliance requirements to meet this statement.

Standard Element: **Security**	Notes & Comments
6.1.4 The solution ensures that physical and digital records, folders, associated storage units and other entities in the record plan automatically inherit user access profiles and information security classification from higher levels of the record plan under which they are created.	
6.1.5 The solution allows the System Administrator to enter user details e.g. Name, location, e-mail address, etc, for the establishment of user profiles and user access privileges.	
6.1.6 The solution allows the System Administrator to create and maintain user profiles of specific user access privileges for each authorised user.	
6.1.7 The solution allows the System Administrator to define different groups of users with different user access privileges.	
6.1.8 The solution provides a hierarchical relationship between the user and their multiple user groups.	
6.1.9 The solution allows the System Administrator to relate document and record information security classification to user access privileges to ensure security is maintained at all times.	
6.1.10 The solution allows only the System Administrator to change a record's profile, (e.g. Information security classification, storage unit, etc.).	
6.1.11 The solution tracks changes to user profiles.	
6.2 *Relate document and record information security classification and system function to user authorisation to ensure appropriate document security is maintained at all times.*	
6.2.1 The solution allows the System Administrator to relate system functions to user profiles to ensure security is maintained at all times.	
6.2.2 The solution ensures that all users are allocated one (or more) roles, and allows access only to system functions permitted by the role/s.	
6.2.3 The solution allows only the System Administrator to authorise access capabilities to any combination of system functions by users and user groups.	
6.2.4 The solution requires the System Administrator to allocate user access privileges to a user profile, with the default being the 'view' category.	
6.3 *Ensure that the risk of access to the system from outside the agency is minimised through using appropriate system security processes.*	
6.3.1 The solution shall prevent unauthorised access to the repository and system from inside and outside the agency.	
6.3.2 The solution, in conjunction with its operating environment, uses authentication measures that allow only authorised users to access the system. As a minimum the software will implement the following authentication measures:	

Standard Element: **Security**	Notes & Comments

• User ID
    • Password and
    • Group ID
 	
6.3.3   The solution allows the System Administrator to deactivate and reinstate user profiles.
 	
6.3.4   The solution retains the integrity of the users' history when the profile is deactivated.
 	
6.3.5 The solution allows integrated login profiles with existing desktop login.	

6.4 Meet legal requirements by maintaining data integrity through the system security. 6.4.1 The solution allows information security classification to be applied to a physical or digital document or record at capture and registration. 6.4.2 The solution allows the System Administrator to modify the information security classification on an ad-hoc or global basis.	
6.5 Ensure that security breaches are recorded in an audit trail. 6.5.1 The solution records all system, user and information security attempts and breaches in an audit trail.	
6.6 Ensure that records can be recovered from failed and interrupted processes without loss of data or integrity in order to be used and accessed in a timely manner. 6.6.1 The solution recovers records from failed and interrupted processes in order to be used and accessed in a timely manner without loss of data or integrity.	
6.7 Maintain system integrity by a System Administrator being able to access currently logged on users, determine their usage statistics, and log users out of the system when required (please define whether this is achieved at the network or application level). 6.7.1 The solution allows the System Administrator to display currently logged on users. 6.7.2 The solution allows the System Administrator to log users out of the system. 6.7.3 The solution allows the System Administrator to produce user usage statistics, as defined by the Administrator. For example, details of records captured, accessed, modified, deactivated, etc.	
6.8 Perform full and incremental back-ups. 6.8.1 The solution allows the System Administrator to perform full and incremental back-ups and recoveries.	

Standard Element: **Reliability**	Notes & Comments
6.9 Enable full and incremental recovery of data stores and indices, synchronisation for remote data stores, and optimisation of data stores and indices, where relevant (please state how this occurs and how recovery of both content and metadata would be achieved).	
6.9.1 The solution enforces data integrity, referential integrity and relational integrity at all times.	
6.9.2 The solution synchronises multiple databases and remote data stores, and optimises data stores and indices.	
6.9.3 The solution allows the System Administrator to restore the entire EDRMS from back-ups, maintaining full data integrity to ensure business continuity.	
6.9.4 The solution allows the System Administrator to restore the entire EDRMS from the most recent back up to the point of system failure.	
6.9.5 The solution enables the System Administrator to perform an integrity check of any data updates that were unable to be recovered or rebuilt.	
6.9.6 The solution reports on any data that was unable to be recovered or rebuilt after a data restore is performed.	
6.10 Perform System Administration functions concurrently with other live transactions.	
6.10.1 The solution allows the System Administrator's functions to be performed concurrently with other live transactions.	
6.11 Tools and/or support for migrating data across new versions and releases, if required.	The solution also must meet all Migration functional compliance requirements to fulfil this statement.
6.11.1 The solution or vendor has tools and support for migrating data across new versions and releases.	
6.11.2 The solution or vendor must provide the capability to access information from superseded repositories and databases in the same system. This capability should support at least one full version of backward capability and is necessary for the migration of data stored in a previous version of the system to the current version.	

7. Support

Standard Element: **Maintenance**	Notes & Comments
7.1 Quality control and reporting mechanisms.	
7.1.1 The solution provides meaningful, plain English error messages, which include a description of error and the required action.	

Standard Element: **Support**	Notes & Comments
7.2 Basic Help/F1 functionality. 7.2.1 The solution provides a plain English, context-sensitive on-line help facility for all users via a standard format interface, such as a web browser.	

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.