Government of South Australia

GPO Box 2343
ADELAIDE SA 5001
Tel (08) 8204 8773
Fax (08) 8204 8777 DX:467
srsaRecordsManagement@sa.gov.au
www.archives.sa.gov.au

State Records of South Australia

Functional Specification for Records in a Business System

Standard

October 2011

Version **1**

Table of Contents

Introduction

A business system is a term used to describe a combination of hardware, computer software, and planning which together allows a business to carry out specific jobs, manage aspects of the business, and maintain a level of quality and efficiency. A business system may be a single computer program, or may be several linked programs, which form the underlying infrastructure of the business (A Guide to Business Systems, www.businesssystem.co.uk). Examples of a business system include financial systems such as Basware, human resource systems such as CHRIS, and case management systems.

Agencies implement business systems to automate business activities and transactions. Increasingly, the only evidence or record that a business transaction occurred is generated and held within the respective business system. In many instances the system is not designed to adequately manage the official records that may result from those activities. Without evidence of these activities, agencies are exposed to risk and may be unable to meet legislative, accountability and business requirements or community expectations.

Official records come in many different formats, for example word processing, spreadsheets, email, compound document or web pages. A series of fields within a database can also make up an official record. While an agency may have an electronic document and records management system (EDRMS), it may not capture all of the agency's official records.

This document is designed to address the gap between the governments' obligations under the *State Records Act 1997* and the ability of agency business systems to manage official records.

This Specification details the South Australian Government defined recordkeeping requirements to be found in a business system. Complying with these requirements will ensure that the records within a business system can be captured and managed so as to guarantee their authenticity, reliability, usability and integrity.

This Specification provides a set of requirements for records management functionality within business systems software. It aims to:

- assist agencies to improve electronic records management practices
- reduce the duplication of effort and associated costs in identifying a minimum level of functionality for records in business systems, and
- establish greater standardisation of records management requirements for software vendors.

The intent of these specifications can be realised through interfacing or integrating the business system with an EDRMS or by building the functionality into the business system.

Purpose

The purpose of this document is to assist agencies ensure that records of business activities transacted through business systems are appropriately identified and managed. Specifically, it will assist agencies to:

- understand processes and requirements for capturing and managing records in business systems
- develop requirements for recordkeeping functionality to be included in a design specification when building, upgrading or purchasing a business system
- evaluate the recordkeeping capability of proposed customised or commercial off-the-shelf software, and
- review the functionality for recordkeeping or assess compliance of existing business systems.

The Specification outlines a number of key records management requirements, with recommended levels of obligation (must, should, may) that can be used as a starting point for further development. Agencies will still need to assess, amend and select their requirements based on business, technical and SA jurisdictional requirements.

This document does not include general system management or design requirements.

Requirements for the long-term preservation of electronic records are not explicitly covered. However, the inclusion of requirements for export supports preservation by allowing the export of records to a system that is capable of long-term preservation activities, or for the ongoing migration of records into new systems.

Use of the term ‘system’ in this document refers to a computer or IT system.

Audience

The primary audience for this document is staff responsible for designing, reviewing and/or implementing business systems within agencies. It also includes records managers who are involved in advising or assisting in such processes, and software vendors and developers who wish to incorporate records functionality within their products.

Scope

Under 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.

Other agencies, including local government authorities, are encouraged to apply this Standard.

Document context

The International Council on Archives (ICA) has developed a suite of guidelines and functional requirements as part of the Principles and Functional Requirements for Records in Electronic Office Environments project, including:

- *Module 1: Overview and Statement of Principles*
- *Module 2: Guidelines and Functional Requirements for Records in Electronic Office Environments*, and
- *Module 3: Guidelines and Functional Requirements for Records in Business Systems*.

This Specification, and its companion document *Management of Official Records in a Business System Standard*, were developed by State Records (SRSA) substantially based on Module 3.

It is recommended that this Specification be read in conjunction with the:

- *Adequate Records Management (ARM) Standard*
- *Management of Official Records within a Business System Standard*
- *Test cases for recordkeeping requirements in a business system* (in development)
- *South Australian Recordkeeping Metadata Standard* (SARKMS)
- *Glossary of Records Management terms*.

This standard aligns with the *Victorian Electronic Recordkeeping Standard Version 2* (VERS) in regard to the export and transfer of records to a digital archive.

Other documents relevant to the electronic recordkeeping environment include:

- *Document and Records Management Systems Standard*
- *EDRMS Design Standard*
- *EDRMS Functional Specification Standard*
- *EDRMS Procurement and Pre-Implementation Guideline*
- *Digitisation of Official Records and Management of Source Documents Guideline*

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

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.

Variation to this standard

State Records may update this standard 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 contact

Agencies and authorities that require further information relating to this Standard should contact the Manager, Government Recordkeeping at:

State Records of South Australia
GPO Box 2343
ADELAIDE SA 5001
Phone: (08) 8204 8773
Fax: (08) 8204 8777
Email: srsaRecordsManagement@sa.gov.au

Functional Specification Requirements

Arrangement of this Functional Specification

The Functional Specification requirements are detailed in the table below. They are arranged in four sections according to key records management concepts and processes:

- Creating records in context
- Managing and maintaining business records
- Supporting import, export and interoperability, and
- Retaining and disposing of records as required.

The functional requirements focus on the outcomes required to ensure records are managed appropriately. They do not specify particular processes, as it is recognised that the techniques and strategies to achieve the outcomes will depend on the type of system being used.

Integration with other systems

As stated in the Introduction, an agency may choose to undertake the management of records externally to the business system. This can be achieved by either directly exporting the records or by integrating with an external records management system. In the requirements section, this is referred to as "*the business system either alone or in conjunction with other systems*".

Choices made about how the records will be managed will influence the extent to which the outlined requirements are selected or amended for inclusion with a business system. While the requirements are phrased in terms of the functionality that a business system 'must' or 'should' possess, depending on the model chosen, the requirement can be met purely within the business application in question, or through the use of additional tools, operating software or integration with, or export of the records/reports to, external records management systems.

Obligation levels

The obligation levels indicate the relative importance of each of the functional requirements. They are to be interpreted as follows:

- Must – requirements that use 'must' are a mandatory requirement for compliance with the specification.
- Should – requirements that use 'should' may be ignored if a valid reason exists, but the full implications of ignoring must be understood and carefully weighed before choosing a different course.
- May – requirements that use 'may' are optional.

Obligation levels must be understood in light of the preceding section on integration with other systems.

1. Creating records in context

The following list of functional requirements is concerned with ensuring:

A fixed record is created – it must be established at what point in the process a record is created, and any further processes that happen in the system must result in the creation of a new record or the augmentation of the existing record, rather than an alteration to it. This means that data that needs to be kept to record previous decisions or processes cannot be overwritten but new data can be added.

The electronic records created by a business system may comprise digital objects – such as digital documents (for example, word-processed documents or spreadsheets), websites, audio and video – or other specialised data formats, and/or data elements and related metadata.

Metadata for records is captured – records must be linked to the metadata that provides context of their creation and use. Most of this information can be automatically generated by the system.

Where relevant, aggregations of records can be managed and a records classification tool can be supported – typically a business system will not contain an internal classification scheme, and for systems that only relate to a limited number of transactions, this metadata may be found in the system documentation, rather than directly associated with every record within the system.

It is expected that agencies will capture metadata for records in line with an identified metadata standard, in accordance with organisational and/or jurisdictional requirements.

1.1 Creating a fixed record

	The business system must, either alone or in conjunction with other systems:
1	Ensure that records created or received by the BS can be captured and stored along with associated metadata, regardless of format and technical characteristics.
2	Support mechanisms for capturing records received by the system that are: • automated, or • a combination of automated and manual.
3	Support mechanisms to ensure that it can capture all records that it is likely to receive from external systems. For example, these may include: • common office packages • workflow applications • electronic messaging systems • e-commerce systems

	• web content management systems • imaging and graphic design systems • multimedia applications • corporate systems • security administration systems, and • other business information systems. Records may also comprise more than one component. 3.1 Where the BS captures a record made up of more than one component, it must maintain a relationship between all components and associated metadata so that they can be managed as a single record and retain the structural integrity of the record. 3.2 Where the BS creates or receives records generated by electronic messaging systems, it must be able to capture attachments and embedded objects together with electronic messages as either linked records or a single compound record. 3.3 Where the BS creates or receives records generated by electronic messaging systems, it must be able to undertake the bulk capture of electronic messages relating to the same transaction. 3.4 Where the BS creates or receives web-based records, such as a dynamic web page, it must be able to capture the record as either: • a single compound record • an aggregation of linked component records • a snapshot – 'frozen' in time • a collection of components that can be regenerated or reproduced on request, or • a combination of the above. 3.5 Where the BS creates or receives records generated by electronic messaging systems, it must be capable of capturing and identifying all incoming and outgoing electronic messages and attachments.
4	Ensure each record is uniquely identifiable within the system (or within the agency, if necessary) and store this identification as metadata with the record.
	The business system should, either alone or in conjunction with other systems:
5	Provide an application programming interface or similar to support integration with other systems, including an electronic records management system, so as to: • enable records created or received by the BS to be exported to an external system • enable, where required, an electronic records management system to establish

	an interface with a BS so that it may apply appropriate records management controls on the records contained within the BS, and • provide a mechanism to enable the BS to import records directly from an external BS, as required to support the system's core business functions.
6	Allow users to capture and store all records received by the BS in their native format.
7	Allow no technical limit to the number of records that can be captured and retained by the BS unless there is a business requirement to do so.
	The business system may, either alone or in conjunction with other systems:
8	Allow the agency to specify the format or pattern of the unique identifier, either through configuration or through specified requirements.
9	Be required to convert a record during the course of the capture process from its original format, native to the generating system, to a format compatible with the BS. 9.1 Where the BS supports the conversion of records from their original formats as part of the capture process (relates to Requirement 43), it must ensure that the context, content and integrity of the original record format are retained and that relevant requirements for conversion are adhered to.
10	Support the naming of records, either: • by the manual entry of names by users, or • through an automatic naming process pre-defined by the business system administrator or through specified requirements. 10.1 Where the BS supports the naming of records, it should provide features to support the process of naming of records. For example: • an automated spell check, or • a warning if a user attempts to create a record using a name that already exists within the BS. 10.2 Where the BS supports the naming of records, it should be able to restrict the ability to amend the name of a record to a business system administrator or other authorised user.
11	Provide mechanisms to ensure that a record received by the system can be captured and viewed, even if the generating application is not supported by the operating environment of the agency.
1.2 Record metadata	
	The business system must, either alone or in conjunction with other systems:

12	Support the range of metadata elements required to support the agency's business.
13	Be able to automatically capture metadata acquired directly from a generating application, an operating system or by the BS itself.
14	Capture all metadata specified during system configuration, and retain it with the record as a robust inextricably linked relationship at all times.
15	Restrict the ability to amend record metadata, so that: • only selected metadata elements can be edited by any user during creation • selected metadata elements can only be edited by an authorised user during creation, and • selected metadata elements can be edited by an authorised user. The restrictions may be specified in requirements, or through configuration by a business system administrator.
16	Support the ability for a business system administrator or other authorised user to amend or override metadata inherited by records and, where applicable, aggregations of records.
17	Be able to maintain and identify selected metadata over time, regardless of whether the related record has been transferred, deleted or destroyed.
	The business system should, either alone or in conjunction with other systems:
18	Allow customer-defined metadata fields for the entry of descriptive information about the records or, where applicable, aggregations of records.
19	Retain a history in the metadata profile of the reclassification of a record, or where applicable an aggregation of records, including the original location of an aggregation of records noting the usual audit trail requirements for systems.
20	Allow the business system administrator to configure pre-defined business rules for the assignment of metadata on capture of a record, or where applicable, an aggregation of records of a particular record type. This may provide a substitute mechanism for assigning metadata at the time of creation. 20.1 Where the BS supports the use of pre-defined business rules to assign metadata on capture, the establishment and amendment of such rules must be restricted to the business system administrator. 20.2 Where the BS supports the use of pre-defined business rules to assign metadata on capture, it should enable records, and where applicable aggregations of records, to be assigned metadata retrospectively, following a change to the pre-defined business rules.

1.3 Managing of aggregations of records	
	The business system may, either alone or in conjunction with other systems:
21	Support the creation and/or receipt of aggregations of records, whereby associated records may be linked together through record metadata so that records management processes may be applied to all records within the aggregation (the nature of an aggregation will vary depending on the type and function of business system). Where the BS supports the aggregation of records, it must: 21.1 Be able to generate a unique identifier within the system (or within the agency if necessary) for each aggregation of records defined by the system. 21.2 Be able to automatically record the time and date of creation of an aggregation of records, within the metadata profile for the aggregation of records. 21.3 Allow a business system administrator to configure the naming mechanisms for aggregations of records. 21.4 Allow the re-assignment of records from one aggregation of records to another by a business system administrator or other authorised user where there is a business requirement to do so. 21.5 Ensure that records attached to an aggregation of records remain correctly allocated following reclassification of that aggregation of records, so that all structural links remain in place.
1.4 Records classification	
	The business system may, either alone or in conjunction with other systems:
22	Allow records, and where applicable aggregations of records, to be classified in accordance with the agency's business requirements. While the business system software is unlikely to support the full definition of a classification scheme, it may contain relevant categories derived from the agency's records classification scheme.

2. Managing and maintaining business records

Once records have been created, they must be managed and maintained for as long as required. Records must be managed to ensure they have

- Authenticity
- Reliability
- Integrity
- Usability

Normal system controls over access and security support the maintenance of these characteristics, and therefore should be appropriately implemented. As this functionality is common to business systems, these have not been included in the functional requirements below.

The following functional requirements are concerned with ensuring:

- Metadata for records can be configured.
- Records can be reassigned or reclassified and if required, duplicated and extracted – as circumstances change, there must be mechanisms in the business system that allow the reassignment or reclassification of records. Also, agencies may wish to copy the contents of an existing record in order to facilitate the creation of a new and separate record, or to create a copy of a record that has come from the material removed or permanently masked.
- Reports can be produced on/about records in the business system, as well as the management of those records.
- Records can be effectively managed when they have been subject to encryption and digital signatures. However, the ongoing maintenance of these records needs to be given consideration.

  Encryption is the process of transforming information using an algorithm (or cipher) to make it unreadable to anyone except those who possess a key, and can decrypt the information to make it readable again. Encryption protects the confidentiality of information.

  A *digital signature* is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that a known sender created the message, and that it was not altered in transit.

  While encryption and digital signatures have a valuable role to play in ensuring the authenticity and integrity of records in transmission, they also present risks to the ongoing useability of the record, as decryption keys and public keys for digital signatures may expire while the record is still required. For this reason, records should not be stored in encrypted form.

  Metadata can record the encryption and decryption processes and attest to the successful decryption of records.

  If such security measures are used as a means of protecting the authenticity and integrity of records, a key management plan must be in place.

	The business system must, either alone or in conjunction with other systems:
23	Prevent the destruction or deletion of records, including aggregations, and associated metadata at all times, except as specified in Section 4.1: Compliance with disposal schedules.
2.1 Metadata configuration	
	The business system must, either alone or in conjunction with other systems:
24	Be able to draw together all elements of metadata to create a metadata profile for a record and, where applicable an aggregation of records.
25	Allow a business system administrator to define the source of data for each metadata element during BS configuration. This will include ability to specify which metadata elements are to be manually entered and maintained. Allow metadata values to be obtained from look-up tables or from calls to the operating system, application platform or other software applications, as required.
26	Support mechanisms for validating the contents of metadata elements, such as: • format of the element contents • range of values • validation against a pre-defined list of values, and • valid classification scheme references (where supported).
27	Be able to manage a metadata profile over time – maintaining links to the record and adding process metadata about business records activities. Where the BS is unable to independently manage a metadata profile over time, and the records are maintained within the system, the BS must be able to either: • Export the metadata profile to an external system, such as an electronic records management system, capable of managing the profile in accordance with the requirements for adequate recordkeeping functionality, and allowing it to be linked to the records contained within the original BS. In this case, it is also mandatory that the external BS support the import of metadata from the original BS. • Permit an interface with an external system, such as an electronic records management system, so that the external system can manage the metadata profile maintained within the original BS. The external system must be capable of supporting the ongoing management of the metadata profile in accordance with the requirements for adequate recordkeeping functionality outlined in this specification. Where the BS is unable to independently manage a metadata profile over time, and the records are maintained externally to the BS, the BS must be able to export the

	metadata with the records to a centralised digital object store, such as an electronic records management system, for ongoing management.
	The business system should, either alone or in conjunction with other systems:
28	Be able to manage a metadata profile in its entirety, so as to facilitate risk management and audit processes.
2.2	**Record reassignment, reclassification, duplication and extraction**
	The business system should, either alone or in conjunction with other systems:
29	Support the movement of records, where appropriate, by providing mechanisms for the reassignment or reclassification of records within the BS (including reassignment of records from one aggregation of records to another, where the aggregation of records is supported) by an authorised user.
30	Support mechanisms to enable the duplication of records, either within the BS or created outside of the BS. Where duplicates are created outside the BS, their existence may be noted in the record metadata profile of the original record. 30.1 Where the BS is able to copy the contents of an existing record in order to create a new and separate record, it must ensure that the original record remains intact and unaltered. 30.2 Where the BS supports the duplication of records, it should provide a controlled copy facility. 30.3 The BS should facilitate the tracking of copies made of an identified record, recording information on access to copies in the audit log. The audit log may keep details of copies created outside the BS, as well as copies created within the BS.
	The business system should, either alone or in conjunction with other systems:
31	Allow the creation of an extract from a record, whereby sensitive information is removed or hidden from view in the extract, while the originating record remains intact. 31.1 Where the BS supports extraction, it must note the creation of an extract in the metadata of the originating record, including date, time, creator and reason for creation of the extract. Whether the extract itself needs to be maintained as a record depends on the analysis of business processes. 31.2 Where the BS supports extraction, it must be able to copy metadata attributes from the originating record to an extract – allowing selected elements to be amended as necessary. For example, an extract may have a different security category from the originating record.

	31.3 Where the BS supports extraction, it may maintain linkage between an extract and the record from which it was taken. Such a link should preserve the relationship between the extract and the record without compromising the access and security controls applicable to the record.
32	Provide solutions for expunging sensitive information by producing redacted copies of records.
2.3 Reporting on records	
	The business system must, either alone or in conjunction with other systems:
33	Be able to report the actions carried out on records, and where applicable aggregations of records, during a specified period of time.
34	Be able to produce statistical information about records, and where applicable aggregations of records, captured and maintained by the BS, such as the number and location of records by application type and version.
	The business system should, either alone or in conjunction with other systems:
35	Be able to produce a report listing the details of any migration process to ensure the integrity of records. As migration may be an infrequent occurrence, the reporting may involve manual intervention.
2.4 Online security processes	
	The business system must, either alone or in conjunction with other systems:
36	Automatically record the details of all online security processes (for example, in an audit trail).
37	Support date and time stamping for all records subject to online security processes.
	Encryption
	The business system may, either alone or in conjunction with other systems:
38	Support encryption of electronic records. Where the BS supports the encryption of electronic records, it must, either alone or in conjunction with other systems: 38.1 Support the capture of metadata for electronic records created or received in encrypted form in accordance with relevant standards, including: • the serial number or unique identifier of a digital certificate • type of algorithm and level of encryption, and • date and time stamps relating to encryption and/or decryption processes.

	38.2 Ensure that an encrypted record can only be accessed by those users associated with the relevant cryptographic key, in addition to other access controls allocated to the record. 38.3 Where the BS supports the capture, identification and/or transmission of encrypted electronic records and associated metadata, it must support the implementation of a key management plan. 38.4 Where the BS supports the capture, identification and/or transmission of encrypted electronic records and associated metadata, it must be able to maintain cryptographic keys for the life of the electronic record, or records, with which they are associated. 38.5 Where the BS supports the capture, identification and/or transmission of encrypted electronic records and associated metadata, it must support the separate, secure storage of encrypted records and their associated decryption keys. Where the BS supports the encryption of electronic records, it should, either alone or in conjunction with other systems: 38.6 Be able to store encrypted electronic records in unencrypted form. 38.7 Allow encryption to be removed when a record is captured or identified, unless the encryption is required to maintain the security of the record while within the BS.
	Digital signatures
	The business system should:
39	Where the BS is able to store digital certificates for encrypted records and digitally signed records, it should warn a business system administrator of any certificates approaching expiry.
	The business system may, either alone or in conjunction with other systems:
40	Be capable of ensuring that any electronic records created or received by the BS that employ the use of digital signature technology can be captured and identified by the BS along with associated authentication metadata. Where the BS supports the use of digital signatures, it must, either alone or in conjunction with other systems: 40.1 Support the use of metadata for electronic records transmitted or captured bearing digital signatures, in accordance with relevant metadata standards. At a minimum this metadata must note the fact that a digital signature was authenticated.

	40.2 Be able to check the validity of a digital signature at the time of capturing an electronic record. 40.3 Be able to store with the electronic record: • the digital signature associated with that record • the digital certificate authenticating the signature • any other confirmation details in such a way that they can be retrieved with the record, but without compromising the integrity of a private key. 40.4 Allow a business system administrator to configure the extent to which authentication metadata is routinely stored with the electronic record. For example: • retain the fact of successful authentication only • retain metadata about the authentication process, and • retain all authentication metadata, including signatures. 40.5 Be able to demonstrate the continued integrity of a digitally signed record, whether or not authorised changes have been made to the metadata of the record. Where the BS supports the use of digital signatures, it should, either alone or in conjunction with other systems: 40.6 Be able to support incorporation of, or interfacing with, digital signature technologies so that authentication metadata can be automatically captured by the system. Where the BS supports the use of digital signatures, it may, either alone or in conjunction with other systems: 40.7 Be able to apply a digital signature to: • an electronic record, or • an aggregation of electronic records during a transmission or export process in a manner that supports external authentication.
	Authentication
	The business system may, either alone or in conjunction with other systems:
41	Be able to support authentication through interface with public key infrastructure-based security technologies.

	Where the BS supports authentication interface with public key infrastructure-based security technologies, it must: 41.1 Be able to store metadata about the process of authentication, including: • the serial number or unique identifier of the digital certificate • the registration and certification authority responsible for authentication, and • the date and time of authentication. 41.2 Where the BS supports authentication, it must allow authentication metadata to be stored either: • with the record to which it relates, or • separately but closely linked to the record.
42	Provide a flexible architecture in order to accommodate new online security technologies as they are released.

3. Supporting import, export and interoperability

Import to and export from the business system, and interoperability with other systems are frequently required functionalities. Records may need to be imported from other systems, exported to different systems, such as an EDRMS, or exported to other agencies in the event of government restructure or other changes.

Records may need to be retained for longer than the lifespan of the business system, creating a need to export records into new business systems. Transfer to a digital archive should also be considered.

Note: State Records designs for a Digital Archive align with the specifications detailed in the Victorian Electronic Recordkeeping Standard (VERS) Version 2.

3.1 Import

	The business system should, either alone or in conjunction with other systems:
43	Be able to undertake a bulk import of records exported from another business system or previous version of the BS (may include an EDRMS) capturing: • records in their existing format, where appropriate, maintaining their content and structure • records and their associated metadata, so as to maintain the relationships between them and map the metadata to the receiving structure, and • maintaining the relationships between records and associated metadata, and where applicable aggregations of records.
44	Be able to import any audit trail information that may be directly associated with records, and where applicable aggregations of records, captured and maintained by the BS and guarantee the integrity of the imported information.
	The business system may, either alone or in conjunction with other systems:
45	Be able to perform an indirect import of records with no associated metadata, or metadata that is presented in a non-standard format, mapping this to the receiving structures.

3.2 Export

	The business system must, either alone or in conjunction with other systems:
46	Be able to export records and associated metadata, and where applicable aggregations of records, to: • another system within the agency, or • a system in a different organisation.

47	Ensure that any export action is able to include: • all records, and where applicable aggregations of records • all metadata associated with exported records and, where applicable aggregations of records, and • all audit trail data associated with exported records.
48	Be able to export records, and where applicable aggregations of records, such that: • the content, context and integrity of records, and where applicable aggregations of records, are not degraded • associations are retained between exported records and their associated metadata, and • relationships are maintained between exported components of a record, between exported records, and where applicable aggregations of records, so that their structural links can be re-built in the receiving system.
49	Be able to export all the types of records it can capture, regardless of format or the presence of the generating application.
50	Allow objects to be exported more than once. While a business decision may be made to delete information in the BS after export, the purpose of this requirement is to ensure that the BS itself does not limit the export process.
51	Ensure that any export action is documented in metadata associated with the record.
	The business system may, either alone or in conjunction with other systems:
52	Be able to export records that have been converted into open standard formats.
3.3 Transferring to State Records	
	The business system must, either alone or in conjunction with other systems:
53	Be able to export records and associated metadata, and where applicable aggregations of records, to an archival institution or program for the long-term preservation of records appraised as having archival value. Be capable of exporting records to State Records in a consistent, open and enduring format as VEOs (VERS Encapsulated Objects) utilising Extensible Markup Language (.xml) and Portable Document Format (.pdf) as specified in VERS Version 2. The metadata encapsulated within the VEO will be expected to adhere to various standards that State Records will release from time to time. "Schema" used to define various items of metadata must adhere either to recognised international or Australian standards or those that have been registered for use within South Australia. Requirements of VEOs will be refined from time to time as State Records

	issues standards and requirements.
54	Support the definition and application of the transfer disposal action.
55	Allow authorised users to add any metadata elements required for the archival management of records selected for archival transfer.

4. Retaining and disposing of records as required

The following list of functional requirements is concerned with ensuring:

Compliance with disposal schedules – existence of a disposal schedule that covers the records in the business system is assumed, determining how long the records should be kept for legal obligations, business needs and community expectations.

Disposal is effectively applied – provision must be made for facilitating retention and disposal either in the system, or through the integration with external software components. Keeping everything for the entire lifespan of the system can be expensive and impair the operations of the system. There may be some circumstances where a cost-benefit analysis and risk analysis conclude that it is preferable to retain records for the lifespan of the system. However, this only may postpone decision-making about the appropriate retention of records until the time of decommissioning.

Records ready for disposal can be reviewed – prior to taking any disposal action, authorised users must be able to review the disposal action and be able to amend it/apply a different action.

Records are appropriately destroyed – it should not be possible for records to be deleted except in accordance with an authorised disposal schedule, and then only after approval to do so has been received by State Records.

Metadata of the destroyed records is retained – evidence of the disposal actions must be maintained either through metadata within the business system or through integration with another system.

Reporting can be undertaken on the disposal activity.

4.1 Compliance with disposal schedules

	The business system must, either alone or in conjunction with other systems:
56	Support the controlled disposal of records legally authorised for disposal. Provision must be made for facilitating retention and disposal either in the BS, or through the integration with external software components. There may be some circumstances where a cost-benefit analysis and risk analysis conclude that it is preferable to retain records for the lifespan of the BS.
57	Allow the definition of at least one disposal class for each classification of records the BS manages. This can be applied to records and associated metadata and, where applicable aggregations of records, achieved either through in-built functionality of the BS software or via an automatic (e.g. an EDRMS or other software application)

	or manual external mechanism. Records should only be disposed of in accordance with business rules defined within the agency's approved record disposal schedules or the general disposal schedule (including GDS21). If the BS manages multiple classes of records there must be at least one set of business rules for each class of record to allow for disposal of both electronic and physical records.
58	Allow disposal classes to be systematically (manually or automatically) applied to any and all records and associated metadata, and where applicable aggregations of records. The methods employed may include: • the incorporation of disposal functionality within the BS software • the integration of external software applications with the BS • manual mapping and application of disposal schedules to the records of the BS by the business system administrator or other authorised user, or • any combination of the above.
59	Ensure that the definition of each disposal class consists of: • a trigger to initiate the retention period • a retention period to establish how long the record must be maintained, and • an action, to prescribe the fate of the record. Support a range of disposal triggers based on active metadata (generated by the BS or supplied by external system mechanisms integrated with the BS). For example: • date of record creation • date of last retrieval of a record • opening or closing date of an aggregation of records (where applicable), or • date of last review of a record, and where applicable an aggregation of records.
60	Automatically track the initiation and progress of retention periods, in order to determine disposal dates for records and associated metadata, and where applicable aggregations of records. Be able to identify any conflict of disposal actions and either: • automatically apply the correct disposal action according to precedence defined by the agency (usually the longer period is applied), or • notify the business system administrator or other authorised user and request remedial action.
61	Support the definition and application of the following disposal actions: • review • export • transfer (consisting of export followed by destruction, once the success of the

	transfer process is confirmed) • transfer to State Records (see section 3.3), and • destruction.
62	Enable flexibility to allow the BS administrator to assign non-standard retention periods and disposal actions (e.g. in the case of Freedom of Information (FOI), court cases, review). Support external disposal triggers based on notification of a defined event either manually entered into the system by a user or automatically acquired via an external system integrated with the disposal mechanism. Allow a disposal freeze to be placed on a record and associated metadata, and where applicable an aggregation of records, in order to prevent any disposal action from taking place for the duration of the freeze (e.g. in the case of FOI, court cases, review).
63	Prevent the deletion or destruction of any record subject to a disposal freeze. Under other circumstances, deletion or destruction may be carried out by a business system administrator or authorised user.
64	Restrict the ability to remove a disposal freeze to a business system administrator or other authorised user.
65	Restrict the ability to amend the business rules governing disposal to the business system administrator or other authorised user. Restrict the ability to apply and reapply disposal classes to the business system administrator or other authorised user.
66	Support a disposal process consisting of: • identification of records and associated metadata, and where applicable aggregations of records, for which the retention period has elapsed • reapplication of a disposal class if required • notification to a business system administrator or other authorised user (e.g. of disposal action due), and • execution of the relevant disposal actions after confirmation by a business system administrator or other authorised user. These actions may be applied automatically or manually as determined by the disposal mechanism employed by the BS.
67	Be able to maintain a history of all changes to disposal classes, including date of change and reason for change.
68	Ensure that amendments to a disposal class take immediate effect on all records and associated metadata, and where applicable aggregations of records, to which that

	class has been applied. Where the BS supports the use of pre-defined business rules, it must enable the manual update or retrospective inheritance of disposal classes when a new disposal class is applied following a change to the pre-defined business rules.
	The business system should, either alone or in conjunction with other systems:
69	Be able to import a set of disposal classes so that the business administrator does not need to manually configure them. Be able to export a set of disposal classes so that they may be transferred to an external system e.g. an EDRMS.
70	Be able to manage a many-to-one relationship where multiple disposal classes may be linked to a record, and where applicable an aggregation of records. At a minimum, the BS administrator, or other authorised user, must be able to manually determine and map the appropriate disposal class with the highest applicable retention period.
	The business system may, either alone or in conjunction with other systems:
71	Support the definition of disposal classes from multiple disposal schedules, where more than one schedule needs to be applied.
4.2 Disposal application	
	The business system must, either alone or in conjunction with other systems:
72	Record all disposal actions (including date and other details) in a metadata profile.
73	Restrict the operation of the disposal process to a business system administrator or other authorised user.
74	Ensure that a retention period is calculated in real time and cannot be artificially advanced. Be able to detect any metadata changes that affect the retention period and calculate a new disposal date according to the disposal class, if not automatically, at least manually.
	The business system should, either alone or in conjunction with other systems:
75	Be able to notify the business system administrator on a regular basis of all disposal actions due to occur in a specified period of time.
	The business system may, either alone or in conjunction with other systems:
76	Support an interface with a workflow engine to facilitate the disposal process.
4.3 Review	
	The business system must, either alone or in conjunction with other systems:

77	Provide a means by which the content of a record, and where applicable an aggregation of records, identified for disposal can be made available to an authorised reviewer prior to the application of a disposal action.
78	When a review disposal action is triggered, allow the business system administrator to reapply a disposal class that could: • mark records, and where applicable aggregations of records, for further retention and later review, or • mark records, and where applicable aggregations of records, for further retention and later disposal action.
	The business system may, either alone or in conjunction with other systems:
79	Where a record, and where applicable an aggregation of records, is being reviewed, make the disposal class details available to the reviewer either by searching or navigation.
80	Automatically record the date of last review as active metadata, and allow the reviewer to add the reasons for the review decision as descriptive metadata.
4.4 Destruction	
	The business system must, either alone or in conjunction with other systems:
81	Ensure that authorised destruction results in the complete obliteration or inaccessibility of all records (including all components of each record, but not any metadata that is required to be retained), and that they cannot be restored through operating system features or specialist data recovery techniques. Backups should not be retained for longer than needed for business continuity purposes.
82	Seek confirmation of destruction from a business system administrator or other authorised user as part of the disposal process (as with all disposal actions). Prevent the destruction of records until confirmation is received, and allow the process to be cancelled if confirmation is not received.
83	Distinguish between an ad hoc delete function and the destruction function within the disposal process, so that each can be allocated individually to authorised users.
	The business system should, either alone or in conjunction with other systems:
84	Have the ability to ensure that when a record is authorised for destruction, all alternative renditions of that record are also destroyed.
4.5 Disposal metadata	
	The business system must, either alone or in conjunction with other systems:
85	Support the progressive addition of metadata to records, and where applicable

	aggregations of records, to enable disposal of records in accordance with the agency's business requirements.
	The business system should, either alone or in conjunction with other systems:
86	Be able to maintain a history of the disposal classes that have been applied to a particular record, in the metadata of that record.
87	Allow the BS to be configured to define disposal metadata to be retained after record disposal.
88	Allow a business system administrator to specify the mandatory metadata to be retained for records, and where applicable aggregations of records, that have been transferred, destroyed or moved offline.
	The business system should, either alone or in conjunction with other systems:
89	Support the entry of management metadata for disposal classes and disposal schedules, including: • a scheduled review date • date and details of revision, and • date and details when superseded.
4.6 Tracking, reporting and reviewing of disposal activity	
	The business system must, either alone or in conjunction with other systems:
90	Be able to produce reports on all disposal activity undertaken by the BS, including disposal activity undertaken by external disposal mechanisms integrated or interfaced with the BS.
91	Be able to produce reports, listing: • all disposal classes currently defined in the BS • all records and associated metadata, and where applicable aggregations of records, to which a particular disposal class is currently applied • all records for which a particular disposal action will occur over a given period of time • all records due for disposal within a given period of time (providing quantitative information on the volume and type of records) • all records that are overdue for disposal at a given point in time (providing quantitative information on the volume and type of records), and • all records subject to a disposal freeze e.g. records subject to a pending or ongoing Freedom of Information or legal discovery process.
92	Be able to produce a report detailing: • any failure during an export of records from the BS, identifying those records

	which have generated processing errors or were not successfully exported, and • the outcome of a destruction process, detailing all records successfully destroyed and identifying those records which were **not** successfully destroyed.
93	Be able to report on review decisions.

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.