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

Management of Official Records in a Business System

Standard

October 2011

Version **1**

Table of Contents

© 2011 Government of South Australia

This Standard may be copied for use by South Australian Government Agencies and Local Government Authorities and for reasonable study or research purposes. No part of this Standard may be reproduced or distributed for profit or gain or for any other purpose without the written permission of the Manager [Director] of State Records of South Australia.

Introduction

A business system is a term used to describe a combination of hardware, computer software, and planning which together allows an agency 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 (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 of a process or business transaction is generated and held within the respective business system. In many instances the system is not designed to adequately manage the official records which 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 documents 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 official records of the agency.

Purpose

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 document also ensures that when selecting, procuring and implementing a business system or upgrading an existing system that it complies with South Australian Government requirements.

A compliant business system is one that has been implemented according to this Standard, the *Functional Specification for Records in a Business System Standard*, and the *South Australian Recordkeeping Metadata Standard (SARKMS).*

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.

Agency business systems should be interfaced or integrated with an EDRMS. If not, the functionality outlined in this Standard must be built into the business system.

This Standard must be applied when implementing or upgrading a business system. There is no requirement to modify existing systems or versions of systems.

Objectives

This Standard will assist agencies ensure:

- official records are appropriately identified and managed;
- the ongoing management of the records' authenticity, reliability, usability and integrity through the capture of sufficient metadata;
- evidence of business transactions is preserved as metadata;
- records can be preserved in an open and enduring format; and
- audit trail and reporting capabilities are accessible.

Adoption of this Standard will also benefit agencies through:

- establishing greater standardisation of records management capture and control;
- supporting transparency, informed and quality decision-making, and planning;
- providing an information resource that can be used to demonstrate and account for an agency's activities;
- enabling consistency, continuity and efficiency in service delivery;
- identifying processes and requirements for managing records in business systems; and
- assessing compliance of existing business systems against government obligations.

Related documents

This Standard is supported by the *Functional Specification for Records in a Business System Standard*. Both this Standard and the Functional Specification are based on *Principles and Functional Requirements for Records in Electronic Office Environments - Module 3: Guidelines and Functional Requirements for Records in Business Systems* (2008) published by the International Council on Archives (ICA), http://www.ica.org.

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

- *Functional Specification for Records in a Business System*
- *South Australian Recordkeeping Metadata Standard* (SARKMS)
- *Across Government Records Management Strategy*
- *Adequate Records Management (ARM) Standard*

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.

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

Policy statement

Agencies are responsible for the capture and management of official records stored within a business system. Not all information contained in a business system will be required to be managed as an official record. Prior to reviewing, designing, building or procuring business systems software, it is therefore necessary to determine the agency's needs in regard to managing official records.

Official records must be maintained in good order and condition and managed as evidence of a business activity; ensuring their authenticity, reliability, integrity, accessibility, confidentiality and usability. Maintenance of this evidence, as records, is necessary for operational viability and accountability of the agency.

In business systems this involves identifying the information (eg documents/fields/metadata) that will form the official record. The following four steps will assist in determining information that is to be managed as an official record.

Step 1 Analyse the work process - This involves identifying the legislative and business requirements, including community and stakeholders expectations, for evidence of the business transaction that is taking place within the business system. It also includes identifying the information, including additional metadata that forms that evidence. Both these elements combined make the 'record'.

Step 2 Identify linkages and dependencies - This involves identifying system information (location, size, file formats, security, audit trails etc); policy and procedural documentation to back-up processes that were undertaken in accordance with agency standards; linkages to other systems; and the retention period for the records.

Step 3 Devise strategies to 'fix' a record in time - This will differ depending upon whether the business system is integrated with an EDRMS or through the business systems' records management functionality. Strategies may be:

- if within an EDRMS set the object as 'read only' and apply metadata such as event history,
- if within the business system, design controls to prevent overwriting or deletion of specific data or creating a distinct digital object of the selected metadata elements that is fixed and unalterable.

Step 4 Implementation – Implementation activities are specific to the strategy selected in Step 3 and beyond the scope of this document. However, an important aspect of this step is to ensure user roles, functions and permissions to access are defined, agreed to and documented.

Principles

This Standard outlines five key principles and related compliance requirements for the implementation and configuration of recordkeeping functionality in a business system.

- *Principle 1: Risk Management* – The system must enable agencies to effectively manage the risks associated with poor management of records.
- *Principle 2: Reporting* – The system must be able to interrogate and report upon the data it contains.
- *Principle 3: Metadata* – The system shall employ metadata standards to ensure accurate identification and aid preservation of the records.
- *Principle 4: Accessibility* – The system shall enable agencies to access and subsequently disclose information to meet their business needs in ways that protect information that is personal, confidential and critical.
- *Principle 5: System integrity* – The system must contain the appropriate functionality to ensure the protection of data.

Agency business systems should be interfaced or integrated with an EDRMS. If not, the functionality outlined in this Standard must be built into the business system.

Principle 1: Risk Management

The system must enable agencies to effectively manage the risks associated with poor management of records.

Scope

Risk management is the process of anticipating what can go wrong and why, and identifying possible solutions. A business system can control risk by managing corporate information in a systematic manner. Processes where information may be lost, damaged or misinterpreted should be identified and managed within the context of the business system. Records that are considered vital to the agency must be given particular attention.

Although a business system can control risk, it may itself represent a risk when things go wrong with the system. For example, the system may fail at events such as:

- capture
- storage, tracking and access
- disposal and destruction
- migration between systems.

Minimum compliance requirements

Creation of records

An agency shall:

- create records when there is a business or legislative need, or a community expectation for them to be accountable for decisions made and actions taken
- provide resources for the maintenance of a business system, including migration between systems, and the migration of metadata from inactive databases.

Capture and management of records

A business system shall enable agencies to:

- capture and register a document, from the system software or external systems, where applicable
- rely upon records as accurate evidence of the activity/activities that they document
- manage official records, using records management principles and practices
- identify and manage all vital records.

Storage

A business system shall enable agencies to:

- store official records in their native format.

Disposal

A business system shall enable agencies to:

- record all disposal actions (including date and other details) in a metadata profile or audit log
- ensure all records are disposed of in accordance with the provisions of the *State Records Act 1997* or other legislation which authorises such disposal
- dispose of records in accordance with current General Disposal Schedules or an agency's current Records Disposal Schedule, enacted either manually or automatically
- restrict the operation of the disposal process to the business system administrator or authorised user.

Migration

A business system shall enable agencies to:

- ensure that, when implementing a new system, complete migration of data between the old and new systems occurs, including metadata for inactive records and from inactive databases, when appropriate
- full and adequate import/export functionality is available, when appropriate.

Conversion

A business system shall enable agencies to:

- 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.

Encryption

When a business system supports encryption, it shall enable agencies to:

- support the capture of metadata for electronic records created or received in encrypted form
- ensure that an encrypted record can only be accessed by those users with the appropriate authorisation or security clearance to do so
- support the implementation of a cryptographic key management plan
- be able to convert and store encrypted electronic records in unencrypted form
- allow encryption to be removed when a record is captured or identified, unless required to maintain security of the record.

Digital Signatures

When a business system supports digital signatures, it shall enable agencies to:

- ensure that use of digital signatures can be captured and identified along with associated authentication metadata
- store with the record:
    - the digital signature associated with that record
    - the digital certificate authenticating the signature
    - any other confirmation details
- apply a digital signature to an electronic record, or aggregation of electronic records, during a transmission or export process;
- allow the management of the key, to the digital signature, in order that it does not expire, or in cases of expiration, successful decryption of official records occurs.

Authentication

When a business system supports authentication, it shall enable agencies to:

- store metadata about the process of authentication
- allow authentication metadata to be stored either with the record to which it relates, or closely linked to the record.

Principle 2: Reporting

The system must be able to interrogate and report upon the data it contains.

Scope

A business system should be able to provide reporting tools for the production of statistical, descriptive and audit reports. As well as standard reports, the system should also be able to provide flexible enquiry facilities and user defined ad hoc reports.

Reports must be able to satisfy a range of legal, operational, evidential and audit requirements. The production of reports must not compromise any of the other system principles, particularly those relating to security of data.

Minimum compliance requirements

Reporting as a tool

A business system shall enable agencies to:

- report on any failure during an export of records from the business system
- use reporting and analysis tools for the management of retention and disposal policies, .

Report generation

A business system shall enable agencies to generate a number of reports for:

- the actions carried out on an official record
- all disposal classes, disposal actions, records overdue for disposal, and records subject to a disposal freeze
- listing the details of any migration process to ensure the integrity of records

Principle 3: Metadata

The system shall employ metadata standards to ensure accurate identification and aid preservation of the records.

Scope

Metadata refers to labelling, cataloguing and describing information in such a way to allow the information within the business system to be properly searched and processed.

In order for information to have the capability of being captured as a record, it is necessary to add additional metadata to give context of the business operations and environment in which it was created.

The *South Australian Recordkeeping Metadata Standard (SARKMS)* provides the minimum metadata that must be captured and with minimal user input. When user input is required it should be provided from drop-down menu lists, usually with a logical default value. Metadata compliant templates of all major desktop applications should be made available to users to eliminate duplicated effort.

Business systems that are upgraded should include functionality that facilitates the capture of metadata according to SARKMS. Business systems often identify mandatory metadata elements when describing people, organisational business units, workgroups, activities and functions.

By adopting SARKMS as a minimum, an agency will be able to identify, authenticate, describe and manage official records in a systematic way to meet its business and archival requirements. Metadata can also assist in:

- controlling authorised use
- facilitating discovery and retrieval
- documenting and preserving content, context and structure of records
- administering conditions of access and disposal.

In today's electronic environment, metadata is a tool that can help to assure the meaning, manageability and longevity of records that are created and maintained in electronic systems.

Minimum compliance requirements

Capture

A business system shall enable agencies to:

- comply with, as a minimum, the *South Australian Recordkeeping Metadata Standard* (SARKMS)
- use a unique identifier for each record
- capture metadata in relation to all records for:

- content including the title, subject, description, language and coverage (if applicable for the types of record in that system)
- registration of the record, including the records identifier, date and location
- structural elements including type, aggregation level (where applicable) and format of the document and its preservation history
- contextual elements of the record, such as the agent, relation and function
- history, including management history and use history
- terms and conditions including access rights and disposal actions.

Maintenance

A business system shall enable agencies to:

- import and export records between system databases, and between applications
- support the controlled disposal of records
- develop record profiles/templates and specifications at an administrator level (if applicable in that system)
- effect global changes to specific fields, at an administrator level
- ensure long-term preservation of data through comprehensive migration practices.

Accuracy

A business system shall enable agencies to:

- ensure accuracy during data entry using various mechanisms. For example:
  - automated entry from previous entries or manual entry as required
  - suppression of leading zeros
  - use of a customisable spell-checker applicable to all relevant fields.

Principle 4: Accessibility

The system shall enable agencies to access and subsequently disclose information to meet their business needs in ways that protect information that is personal, confidential and critical.

Scope

This principle refers to the control of, and access to, the agency's records.

Access

The official records of an agency may be accessed a number of times during their existence and this may occur for various reasons, such as the current administrative needs of the agency, research by the agency into the background of previous decisions and historical and other research. Information within the record may require control over its disclosure due to a number of issues, including:

- security
- personal privacy
- inter-governmental and intra-governmental access
- commercial confidentiality
- intellectual property
- legal liability
- freedom of information.

Agencies will want to ensure that information of a confidential nature is not accessible to all users while allowing access by appropriate people. Both the indiscriminate release of information and the refusal to release information may infringe on the rights of individuals and the business needs of the government, and cause severe liabilities for the agency.

Relationships between electronic records and records held in other formats must be clearly identified.

Retrieval

A business system must enable official records to be found upon demand. An agency's ability to find its official records within a specific time and with the required accuracy will have a significant impact on the transaction of its business. An agency that is able to find relevant records when needed will be able to make more efficient use of their human resources, and reduce costs.

The agency should be able to retrieve information from the system by searching the database, using a range of parameters.

Minimum compliance requirements

Appropriate access

A business system shall enable agencies to:

- ensure that all records are easily accessible by those authorised
- ensure that access to records is subject to South Australian Government security, privacy and confidentiality requirements, including the Information Privacy Principles
- provide access to records using appropriate storage and security.

Classification

A business system shall enable agencies to:

- define records, and where applicable aggregation of records, to be classified in accordance with a classification scheme, when appropriate
- support linkage between a record's classification and other processes such as capture, access and security, disposal, search and retrieval, and reporting.

Searching and retrieval

A business system shall enable agencies to:

- find records entered into the system upon demand
- link, group and relate documents to other documents created or used as part of the same business activity, either specified by the system or by the user
- retrieve information using search parameters defined by the business requirements
- refine search criteria and results at a user level, based on operational needs.

Principle 5: System Integrity

The system must contain the appropriate functionality to ensure the protection of data.

Scope

This principle refers mainly to the IT issues around access to, and integrity of, data within the system. Through the system's technical integrity, access to software functionality, as well as access to records held within the system can be limited to specific needs. For instance:

- system administrators should be able to access functionality in the system that an end-user cannot
- records of a confidential nature should only be available to those users who have the appropriate authorisation
- system integrity should prevent or minimise the risk of:
    - corruption or inaccessibility of the data
    - unauthorised access to the system.

Minimum compliance requirements

Security

A business system shall enable agencies to:

- apply security classification to the user, the record and the record type at creation
- relate record classification and system function to user authorisation so that appropriate document security is maintained at all times
- minimise the risk of access to the system from outside the agency by using appropriate system security processes
- meet legal requirements by maintaining data integrity through the system security
- automatically record the details of all online security processes through an audit trail.

Reliability

A business system shall enable agencies to:

- ensure that records can be recovered from failed and interrupted processes without loss of data or integrity
- perform full and incremental back-ups.

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.