Information Management Advice 18 - Managing records in business systems - Checklist

Questions for vendors when selecting new business systems

Business systems hold dynamic information that supports your agency's business activities. Many of these systems also hold State records, but do not have sufficient inbuilt recordkeeping capability to manage those records over time. Records created and captured in these systems are more likely to become inaccessible or be inappropriately destroyed because they are not configured to adequately manage records for as long as they are required. TAHO recommends that recordkeeping functionality requirements be considered in plans to implement business systems. Systems will then be capable of meeting minimum requirements for preserving Permanent State records.

This checklist is designed to assist agencies by suggesting some questions to ask vendors during the procurement process.

NOTE: This checklist covers only those functions necessary to support long-term preservation of State records, and is intended to be a component of the functional specifications that the agency may prepare when commencing the vendor selection process.

Recordkeeping requirements must be deployed 'by design'

Agencies can proactively plan for recordkeeping requirements to be incorporated by design. It is important that recordkeeping requirements are considered when:

- Purchasing new systems
- Planning for system migration
- Planning to move to cloud services
- Business process outsourcing
- Developing new applications

The advantages of considering recordkeeping requirements include:

- Better management of high risk and high value business information
- Significantly lifts the recordkeeping burden from employees by automating the process of capturing records and business workflow
- Reduces purchase, configuration and ongoing maintenance costs by removing the need to maintain legacy data
- Improves the ability to retrieve records through better maintenance of context and better support of search
- Supports interoperability and improves long-term migration options.

- Ensures records are retained according to the requirements laid down in authorised Retention and Disposal Schedules.

When you ask vendors if the new system incorporates functional requirements for keeping records and metadata, it is important that vendors demonstrate that the system can meet these requirements.

Do not rely on vendor marketing material to provide this evidence.

Functional specifications that address recordkeeping requirements

The system must keep a version of each defined record, either in documentary form (e.g. a document or object) or as a collection of data (which is fixed and complete). The system must capture/create, accumulate and maintain over time the minimum required recordkeeping metadata.

Minimum Recordkeeping Requirements	**Questions for the vendor**	**Documentation/ Evidence**
System documentation	• What documentation is provided about business activities and actions supported by the system, system configurations, system metadata, workflows and permissions? • Does the system comply with any records or information management standards such as ISO15489: Records Management, IS31: Retention and Disposal of Records, IS34: Metadata or IS18: Information Security?	• Technical documentation • Manuals
System and device dependencies	• Does the system support interoperability or integration with other systems? • How is this enabled? • Is an API (application programming interface provided? • Is interaction with mobile devices a feature, and how is this implemented? • Is the system locally installed, outsourced and/or cloud-based? See *Guideline 17 Managing risks associated with Cloud Computing.*	• Technical documentation • Vendor demonstration • Talk to other sites where system is installed
System failure	• What processes enable system recovery without the loss of data or internal integrity after failures?	• Backup and recovery documentation • Vendor demonstrates versioning and rollback capability

Minimum Recordkeeping Requirements	**Questions for the vendor**	**Documentation/ Evidence**
Create Where the record is made up of more than one component, the system must be able to maintain relationships between all components.	• Can the system create and maintain links between records and to metadata and audit data? • Does the system store one instance of information but link to it from many places? • If the record consists of a series of transactions or sequential events are they linked by a unique ID (e.g. document set id)? • Does the system allow document version control (and revisions within versions)? • Is it possible to fix the records (e.g. by making them read-only?)	• Audit logs or system event logs • Vendor demonstration of data input process
Retrieve The system must be able to store and retrieve the defined records along with their associated metadata and including all components of the records in useable, human-readable form.	• Does the system allow for a classification schema, taxonomy or tagging to assist search and retrieval? • Does the system have the ability to limit data input to specified values, so that accuracy is maintained? • Does the system support full text search of OCR'd documents, or only search across captured metadata? • Can an Administrator configure/filter search values, and search results?	• Data validation techniques, • Pick lists and/or thesauri • The automatic capture of date and time information from the system

Minimum Recordkeeping Requirements	**Questions for the vendor**	**Documentation/ Evidence**
Access The system must incorporate safeguards based on defined access rules and user identification to limit who can view or access records and associated metadata. The alteration, deletion or addition of metadata elements is controlled by administrative users only.	• Can the system restrict or permit access to the records by specified individual users, assigned roles or groups? • Is the system able to provide appropriate permissions to access records in particular ways (e.g. viewing, printing, editing, copying, and transmitting?) • Does the system log unusual connections; security audit failures; failed logon attempts; attempts to log on to default accounts; activity during nonworking hours; file, directory, and share permission changes; and elevated or changed user permissions? • Does the system enable security classifications to be applied to and changed as and when required by the system administrator/s?	• Documentation refers to user account or identity management modules • Vendor demonstration of system security model
Point of capture metadata To be assigned to individual records and/or to aggregation (grouping) of records: • Unique identifier • Title or name • Date of creation • Who/what created the record (person/ system event)	• Does the system assign unique identifiers? • Does the system capture the time/date the record was registered? • Can naming conventions, classification schemes or encoding schemes be applied at capture? • Can the system enable reports or data entry profile forms to be customised if this metadata is not automatically applied?	• Time stamps • Audit logs or system event logs • User account or identity management modules • Reporting capability

Minimum Recordkeeping Requirements	**Questions for the vendor**	**Documentation/ Evidence**
Process and Disposal metadata The business system allows for the application of disposal actions and triggers to be applied to records. For example, changed access rules, modification to records, and transfer of records. • The date of the action • Identification of who/what undertook the action • What action was undertaken • The authority governing the disposal of the records	• Does the system enable security classifications to be applied to records at creation and subsequently changed as and when required by the system administrator/s? • Can destruction/deletion of records be achieved and does the system identify that a record was destroyed (deleted) from the system? • Does the system identify permanent value records and enable appropriate protection to ensure their long term viability? • Are change events logged in an audit log? • Can the system apply and allow for review of disposal actions, changed access rules and triggers to records? • Does the system allow for 'flagging' of records as Vital Records or subject to 'legal hold' and remove them from active disposal programs?	• Audit logs or system event logs • System vendor demonstrating that system extracts change events and entries in the audit log and presents these in a report • Capacity to produce reports for compilation of agency Register of Records destroyed
Reports and export process Is the system able to export the defined digital records and their associated metadata to another system or to an external medium? The process should not degrade record relationships, data quality or metadata.	• What file or content types are supported by the system? • Can naming conventions, classification schemes or encoding schemes be applied to achieve standardisation, for reporting, and for easier access to records in the system? • Can reports and exports be produced in .pdf or .xml formats?	• System vendor demonstrating accurate conversion of content for all the types of source formats handled by the system

Summary of functional requirements for recordkeeping

The business system must be able to:

1. Keep a fixed and complete version of each defined record, in documentary form or as a collection of data.
2. Capture/create, accumulate and maintain over time the minimum required recordkeeping metadata.
3. Manage the record in the business system such that it is possible to:
   a. Demonstrate that the record is accurate
   b. Demonstrate that a record has not been modified without authorisation
   c. Maintain the history of the record with associated metadata events
   d. Copy the records to new storage media (also known as refreshing)
   e. Reliably retain the record (through system failures and disasters)
4. Export the records and associated metadata to another system
5. Export the records and associated metadata in a long-term preservation format (See *Guideline 19 Digital preservation formats*) for transfer to TAHO
6. Ensures records are retained according to the requirements laid down in authorised Retention and Disposal Schedules.

Further Advice

For more detailed advice, please contact:

Government Information Strategy Unit
Tasmanian Archive and Heritage Office
91 Murray Street
HOBART TASMANIA 7000
Telephone: 03 6165 5581
Email: gisu@education.tas.gov.au

Acknowledgements

State Records NSW: Making decisions about how long to keep digital information (April 2014)

Information Security Classification

This document has been security classified using the Tasmanian Government Information Security classification standard as PUBLIC and will be managed according to the requirements of the Tasmanian Government Information Security Policy.

Document Development History

Build Status

Version	Date	Author	Reason	Sections
1.0	28-05-2014	Samara McIlroy	Initial release	All

Amendments in this Release

Section Title	Section Number	Amendment Summary
		This is the first release of this document.

Issued: July 2014

Ross Latham
State Archivist