TAHO
Tasmanian Archive + Heritage Office

Information Management Advice 17: Recordkeeping by Design - Requirements for Managing State Records in New Business Systems

Planning for the management of information as an asset in business systems is far easier if it is done by design as part of the planning and system specification process. Retrofitting recordkeeping requirements into existing business systems is difficult, sometimes not technically possible, and usually expensive.

Records and information management requirements need to be proactive, strategic, considered, or designed as a core component of systems, services and processes and not addressed as some legacy or retrospective consideration. Systems are episodes in the life of a record, and the requirements for managing these records throughout their useful life need to be considered and incorporated into system design.

Audience

This advice is for Project Managers, Line of Business Managers, Business System Owners, Business Analysts, Vendors, Records Managers, and officers involved in the design and implementation of line of business systems.

Recordkeeping by Design Approach

"Recordkeeping by design" is an approach to recordkeeping that enables it to be built into the design and architecture of information systems, business processes and network infrastructure. Taking a "recordkeeping by design" approach aims to ensure that recordkeeping is considered before, at the start of, and throughout the development and implementation of business systems that create and manage records. This approach involves a level of intentionality regarding records management, which indicates a genuine desire to actively manage records well.

A "by design" approach to records management enables IT professionals and those responsible for delivering services to the user community to approach records management as a design feature of agency process and activities, rather than a compliance burden to be endured or to which lip-service is given. It shifts the records management focus to risk prevention rather than compliance, using an innovative approach that is anchored in genuine recognition of the importance of records and information.

By focusing on the design and operation of information systems throughout their lifecycle, a 'by design' approach supports efforts to address information risk. Better recordkeeping functionality means that costly records management retrofitting will not be required, generating significant cost savings. A 'by design' approach forces leaders and project managers to direct their attention to the policy and operational objectives information projects are intended to achieve, in a way that recognises records management requirements.

Taking a 'by design' approach to records management constitutes a basis for cultural change in the way Tasmanian government plans, develops and implements information projects.

Take a proactive preventative approach

"Recordkeeping by design" is characterised by a proactive rather than a reactive approach, that does not wait for recordkeeping risks to materialise and require remediation or resolving recordkeeping issues once they have occurred, rather it aims to prevent them from occurring. "Recordkeeping by design" focuses on identifying the requirements initially, and subsequently building them into the design of systems as with other business requirements the system is intended to support.

Gather Information

Firstly, gather agency sources to assist you to identify recordkeeping requirements, and the value of the records the business system will create and manage.

Table 1: Documentation that will assist you to identify recordkeeping requirements, and the value of records the system will manage.

Documentation	***Relevant content***	***Source***
Appraisal Statement for State records required as State Archives	The Appraisal Statement assists agencies to identify and appraise State records to be preserved as State Archives. It describes in summary the types of records TAHO will preserve as Archives into the future. While appraisal is relevant to all State records, this Appraisal Statement focuses on the values guiding the appraisal and identification of permanent State records.	TAHO Website
Agency Legislative Mapping Document	Legislative mapping is a key step in researching and documenting the recordkeeping requirements of legislation that is relevant to your Agency. Legislative mapping assists in identifying all explicit and implicit recordkeeping requirements that are prescribed in legislation, and ensures that these requirements are covered in a Retention and Disposal Schedule. Legislative mapping is also useful to determine what functions and activities your agency is responsible for, and what State records the business should be creating. **Note**: A legislative map only includes legislation specific to your agency. The recordkeeping requirement of legislation applicable to all agencies, such as the *Archives Act 1983* or the *Personal Information Protection Act 2004*, are covered by the General Retention and Disposal Schedule for Common Administrative Records.	Records Manager/ Legal Officer

Documentation	***Relevant content***	***Source***
Agency Information Asset Register	The agency Information Asset Register should contain details of each asset, its retention and disposal class, information security classification, vital records status, and should indicate if the assets contain highly sensitive or confidential information. It may even indicate its risk status.	Information Security Officer/ Records Manager
General Retention and Disposal Schedule	A Retention and Disposal Schedule is a formal instrument that identifies records, defines how long they can be kept, and whether they should be destroyed or retained as State records. TAHO uses Retention and Disposal Schedules to permit disposal of records under the Archives Act 1983. To facilitate the disposal of common administrative records and common records relating to core functions, TAHO has approved a number of general Retention and Disposal Schedules. Additionally, several of these general schedules are specific to a particular sector of government.	TAHO Website
Agency Retention and Disposal Schedule	If you do not have disposal authorisation for your core records (those that document business unique to your agency) you also need to develop a functional Retention and Disposal Schedule to ensure that these records are disposed of in accordance with legal requirements. If it is not possible to do this prior to the system design process, you can review TAHO Appraisal Principles for State records. This indicate which characteristics of records determine if they are a State record of permanent value. Contact TAHO as we can appraise the function the business system is supporting to determine the disposal requirements of your system.	TAHO Website Agency intranet
Vital Records Register	Vital records include records needed to: • operate the agency during a disaster • re-establish the agency's functions after a disaster, and • establish and protect the rights and interests of the agency and its employees, customers and stakeholders. In effect, they are records that are essential to the agency. Without them the agency cannot establish, conduct or continue business effectively.	Agency Records Manager
Agency Risk Register	The level of management for each business system will depend on an assessment of the potential risk to the agency should the information and records become inaccessible, unreliable or deleted. Where the risk is high, the records contained within the system will need to be	Agency Risk Manager

Documentation	***Relevant content***	***Source***
	managed stringently to ensure the integrity of the information, and that records are kept for the required period. A robust risk assessment will inform the level of evidence required of the records, and therefore how stringent recordkeeping controls need to be within the new system.	
Agency Information Security Policy	Agency information security policies should include the information security classification for the business information that the system will manage. If the business information is classified at a high level (PROTECTED OR HIGHLY PROTECTED) then more stringent controls will need to be put in place for the management, access and destruction of the records.	Agency Information Security Officer/Project Manager
Legislation, Regulations and Standards	Look at legislation and standards that apply to the business area, as legislation and standards are often very specific in terms of the records you need to keep, and the information that these records need to contain. (See Table 2).	Thelaw.tas.gov.au Standards Australia website
Agency Policy and Procedures	Review Policy and procedure statements that document what records need to be created from specific processes. Are these records being created? For example, if the internal business procedures for case management say that 'a record must be kept of each action in a case in the Case Management System, including the date of the action and who approved it', the system will need to be designed to do this.	Agency Intranet
Corporate Governance Documents	Understand corporate accountability controls and reporting requirements. Will the business system manage information required to support corporate governance and reporting?	
Reporting data metrics and analysis by the business area	What reporting occurs in the business area now? Understand business needs for information dissemination and sharing. Examine the data, metrics and analysis that is required to account for the performance and operation of certain business operations.	
Current case files created in the business area	Identify the information needed to support clients, projects and cases in the short and medium term.	

Identify the Value of the Records the Business System will create

Once you have reviewed your documentation, identify recordkeeping requirements of the system you are designing. The following sources will assist:

- *Advice 36 Legislative Mapping*
- *Checklist How to identify Recordkeeping Requirements*
- *Template Recordkeeping Requirements*

You should then identify value of the records that the business system will create. A step by step process for this is covered TAHO *Advice 18 Managing records in Business Systems Part 1*

Undertake an Information Risk Analysis

Risk is a key factor to incorporate into the development of appropriate strategies for managing State records in business systems. Analysis involves an assessment of the agencies exposure to information risk. Risk management is 'the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects' [1].

Risks may arise from not creating records in the first place, from disposing of records too soon, or from not ensuring the accessibility and readability of the records over time. Possible consequences arising from these risks may include adverse publicity, inefficient business activity and a reduction in the agencies capacity to prosecute or defend allegations.

To understand the agency risk and build risk mitigation into business systems, you need to identify high risk areas of business. What is the business that the system will support? Is the business high risk?

The following resources available from GISU's website will assist:

- *Advice 60 Introduction to Risk Management Processes Part 1 - Overview*
- *Advice 60 Introduction to Risk Management Processes Part 2 – Applying Risk Management Processes*
- *Advice 60 Introduction to Risk Management Processes Part 3 – Template Information Risk Register*
- *Advice 60 Introduction to Risk Management Processes Part 4 – Identifying Information Risk that might be impacting on high risk business*
- *Advice 60 Introduction to Risk Management Processes Part 5 – Successfully manage Information Risk that can occur during system migration*
- *Guideline 25 Managing Information Risk*

Minimum Recordkeeping Requirements for Systems Managing Permanent Value State Records

Once you have determined the value of the records to the agency, and the level of risk associated with the records, you can start to define a list of minimum requirements and appropriate strategies for managing records in the business system.

This section includes a description of the required recordkeeping functionality for business systems managing permanent value State records. There are also recordkeeping requirements that relate to the functionality a

[1] Australian Standard AS/NZS 4360-1999, Risk Management.

system should have to support good recordkeeping. These requirements are just as important, as they ensure that records are created and maintained in appropriate ways to ensure they function as evidence. Described here is the qualities business systems should have, and the types of operations they need to be able to perform. To operate effectively, systems have to meet a defined set of characteristics. These characteristics are summarised here to provide an overview of the types of qualities your business systems should possess if it is managing permanent value state records.

Recordkeeping systems should possess the following characteristics, in order to produce and maintain authoritative records:

Table 2: Characteristics of business systems managing permanent value State records

The characteristic of …	***Means that systems should…***
Reliability	• routinely capture all records • organise records appropriately • provide adequate information about the records within them • provide ready access to records and make records of system operation
Integrity	• prevent unauthorised access, destruction, alteration or removal of records
Compliance	• be managed in compliance with all requirements that apply to the business documented within them
Comprehensiveness	• manage all records resulting from the business activities that are documented or managed by the system
Fixity	• store records in ways that mean they cannot be tampered with, deleted inappropriately or altered
Accessibility	• allow records to be shared as information resources across a work space, business unit or agency

Source: Many of these requirements are derived from AS ISO 15489.1-2002, Records Management - Part 1: General

Functions of Business Systems Managing Permanent Value State Records

In addition to having the characteristics defined in the previous section, business systems must be capable of performing a range of standard recordkeeping functions.

Table 3: Functions of Business Systems Managing Permanent Value State Records

The function of…	*Means that systems should be capable of…*
Registration	• capturing records by assigning them unique identities and attributing brief descriptive information to them, such as a title and date
Classification	• arranging records into categories based on the business activities they document, as a means of facilitating record control, retrieval, disposal and access
Indexing	• establishing access points to facilitate record retrieval
Access and security modelling	• assigning and implementing rights or restrictions that protect records against unauthorised or inappropriate use or access
Tracking	• monitoring record use to ensure no inappropriate use occurs, and an auditable record of use is maintained
Disposal	• utilising retention and disposal schedules, linking disposal periods to records, triggering any required disposal actions, reviewing any history of use to confirm or amend disposal status, and maintaining an auditable record of disposal (retention, destruction or transfer) actions
Storage	• appropriately maintaining records in consideration of their form, use and value for as long as they are legally required
Searching, retrieval and rendering	• making records available as corporate information resources • identifying and presenting records in response to user search requests and, where appropriate, enabling records to be printed on request
Reporting	• generating any reports deemed necessary by the agency

Requirements

To operate effectively, business systems have to meet a defined set of requirements. These requirements are discussed here to provide an overview of the types of qualities your systems should possess- and are described at a high level. Each agency will use techniques and strategies to achieve outcomes depending upon the type of system, and the agency's individual needs. There are 3 levels of requirements the system will need to meet:

- agency requirements,
- system level requirements, and
- records level requirements.

Table 4: Requirements of Business systems managing permanent value state records

Requirement	***What this means…***
Agency Level Requirement	
Managing a record in any form	• managing electronic records, scanned images, voice files, video clips, digital plans, databases, information from other applications etc. • managing electronic signatures and encrypted records, where appropriate Some systems may only be required to manage records in one format, while others will need to be capable of managing multiple formats.
The agency must commit to sustaining business information for as long as it is required.	Many business records will have a lifespan beyond the system in which they are created and managed. To sustain business information, the agency must be committed to migrating systems and the records they contain, or the export of long term value business records along with their relevant metadata, into new business applications as and when required. Plans for sustaining business information and migrating into new systems should be developed in conjunction with records staff.
Plan for how you will sustain datasets	Many new business systems will leverage large datasets, in order to present and repurpose information online. This is a great strategy but when utilising this approach it is important to be aware that maintaining accessibility to, and the specific meaning of, data over time is a complex undertaking. Long term dataset accessibility, particularly spatial dataset accessibility, is very challenging because of the complex and various data overlays and data formats used, which are often tied to specific proprietary software. Any dependencies here in terms of licencing, support, format or software upgrades, connections with related datasets etc., can cause a lot of complexity when trying to manage the data for long periods of time. These dependencies need to be sustained in order to maintain data accessibility. Proactive planning can resolve these issues. Firstly, you should investigate whether maintaining accessibility is likely to be problematic for some of the forms of data you will be managing. If it will be, there may need to be arrangements made for regular dataset maintenance to ensure ongoing accessibility.
System Level Requirements	
The system must create and keep defined records	The system must be able to routinely create and keep the records that are required to support and document the business performed within the system. Records must be organised appropriately with required metadata. Records staff

	can help to define what these records are, in liaison with the system owner and relevant business staff.
The system must be able to register, classify and index and track records	Capturing records by assigning them unique identities, and attributing brief descriptive information to them, such as a title and date. The system must be able to record the retention value of the system they create and include functions to support retrieval and access. The system needs to be able to establish access points to facilitate record retrieval. The system needs to be monitoring record access and use to ensure no inappropriate use occurs, and an auditable record of use is maintained.
Integration with electronic applications	Integration with applications used for transactions of business (office utilities, email, websites, database applications, workflow etc.).
The system must be well documented	Documentation of system configuration, metadata design, system customisation and enhancement must be documented and maintained. This documentation is needed to understand and manage the information within the system, and to assist with any necessary system migration, or record export.
The system must allow data migration, or able to export records and their metadata as required	Many business records will have a lifespan beyond the system in which they are created and managed. To enable records and their supporting contexts to be carried forward into new operating environments, or to remove them from environments where they are not adequately protected and managed, systems must be able to be migrated or must be able to export records and their associated metadata.
The system must support the metadata that is required for business and management purposes	The system must support the metadata that the business needs for its operations. The system must also capture and support recordkeeping metadata, which enables records to be managed and interpreted now and over time. Where possible, metadata should be system-generated.
The system must be able to implement appropriate security controls	The system should incorporate safeguards to limit who can view or access records and their metadata. The system must also have the capacity to control the ability to perform specific processes, or to track actions that individuals or groups can take (e.g. viewing, printing, editing, copying, transmitting, deleting). Systems must not allow unauthorised modification of records or their metadata.
The system must enable the destruction of time-expired information	The system needs to be able to destroy records and some associated metadata in a systematic, auditable and accountable way in line with business and legal requirements, while maintaining the accessibility, trustworthiness and useability of records with ongoing business relevance. No records should be able to be deleted or removed from the system without appropriate authorisation. The system needs to be able to utilise Retention and Disposal Schedules, linking disposal periods to records, triggering any required disposal actions, reviewing

	any history of use to confirm or amend disposal status, and maintaining an auditable record of disposal (retention, destruction or transfer) actions.
The system must produce necessary reports	The system needs to be able to produce reports that are required by the business, or that are required to monitor information destruction, storage and use.
Plan for the longevity of your core business information	It is likely that some of the information in your system will need to outlive your new system, and will need to make its way into new business frameworks and future business systems that evolve. It is crucial to consider this longevity requirement in your very early system planning and development processes. Strategies can be built into system design that support information longevity, such as considering how information could be partitioned or segmented based on different business information retention needs, or using different workflows to facilitate the export of identified data or reports for ongoing management, or developing specific migration pathways for data of long term business value.
Build authorised disposal into your system	Agencies need to focus only on managing the information they need to manage within their systems, and to design all systems from the outset so that they can appropriately destroy all possible information at regular time-appropriate intervals. Digital data volumes in agencies are growing exponentially and unsustainably, and the impacts of this are starting to be felt across government. Active management and appropriate planning decisions about: • what data can be routinely disposed of and when, and • what data needs to be sustained and how are needed to ensure there is no ongoing digital legacy that agencies will have to resolve into the future.
Consider format vulnerabilities and their implications	It is crucial to consider format choices, the evolution of these formats and the impacts of system upgrades into system design and choices around work processes. For example, large agencies like the US Defence Department have had challenges in maintaining ongoing accessibility and accuracy of its complex CAD records, and it is worth considering and learning from case studies like these. Defence has found that as their CAD operating environment constantly evolves, plans of complex assets such as aircraft carriers are slightly altered with each software upgrade. Mitigating this form of information risk could be a critical consideration in some business systems and processes.
Assess your need for extensive system	Remember systems are records of how we do business, it is important to manage the information *about* your business system, not just the information *in* your business system. Agencies need to consider the business purpose of the system. The records created within the system may not be significant, however

documentation requirements	if the system was large and significant to government, records may need to be kept to show how the system operated and the system rules that were in place to protect and manage security and information access. When developing a business system, the system rules, validation and security processes, workflow authorisations, workflow processes, etc. you define are requirements that need to be documented. It is also important to capture "point in time" representations of these as, if a validation process changes, it could be important to know how the validation operated for a specified time period before that change. Depending on the level of business risk linked to your system, this level of process governance could be critical. The retention of these types of system-specific records can however be overlooked by records staff, and can be disregarded by ICT staff once a system is decommissioned. These records about systems, however, can be just as important as the information that the systems contain. In the digital business world, records need to increasingly be seen as data in context. The information we input into systems is the data, the system itself provides the context. We need to look at maintaining information about both the data *and* the system if we are going to have full, accurate, useful, evidential and meaningful information in both the short and long term. This need to account for the system and management frameworks that were used to create and transact business operations is only going to increase in the future, and so we really need to be proactive about the creation and management of this type of information now. Essentially business systems themselves are records of how agencies perform their business operations, and increasingly we will need to keep good and accountable records of them.
Plan for the end at the beginning	Technology does not last forever. Your glorious new system will one day become a legacy system, and the information it contains will need to be managed through this transition. So start to plan for this now. What information within the system is core and will need to be managed into the future? What metadata is integral to the ongoing use, understanding and accountability of this information? What information about your system will be important to sustain and keep as accountability and context for your business information, which will need to outlive the system? For instance, for high risk business processes, should you keep records of your workflows, user permissions, audit trails etc.? Recordkeeping **about** your system - as much as recordkeeping for the information **within** your system - can be really critical, so consider what your specific needs are.

Records level requirements	
Records must be accessible	For the life of the system, the records required by the business must be able to be searched for and accessed by authorised staff. The system needs to be able to support full search functionality, and support the metadata fields that staff will require for searching. The system also needs to make records available in useable, human-readable form. **Note:** Backups are not suitable systems for maintaining the accessibility of high risk or long term value records.
Records must be protected	Staff need to be able to trust that the records they access will be authentic, well managed, accurate representations of the business performed. The system needs to capture fixed, point-in-time records and be able to protect these and track their use and management so that the integrity of the records is supported. The records and their metadata must not be altered, including during migration. Records must be protected from accidental or intentional damage and destruction, and from modification.
Records must be meaningful	Records must be able to be interpreted and used for ongoing business. The system must support the ability to capture and maintain relevant metadata that describes the business that the record documents, when the business was transacted, and the staff involved. It needs to create connections between related records so that a complete picture of the business operations can be compiled, and enable records to be copied and reused for future business.
Records must be maintained	Records must be kept by the system for as long as they are needed by the business, and in accordance with legal requirements.

Some considerations when selecting an approach for managing records created in business systems

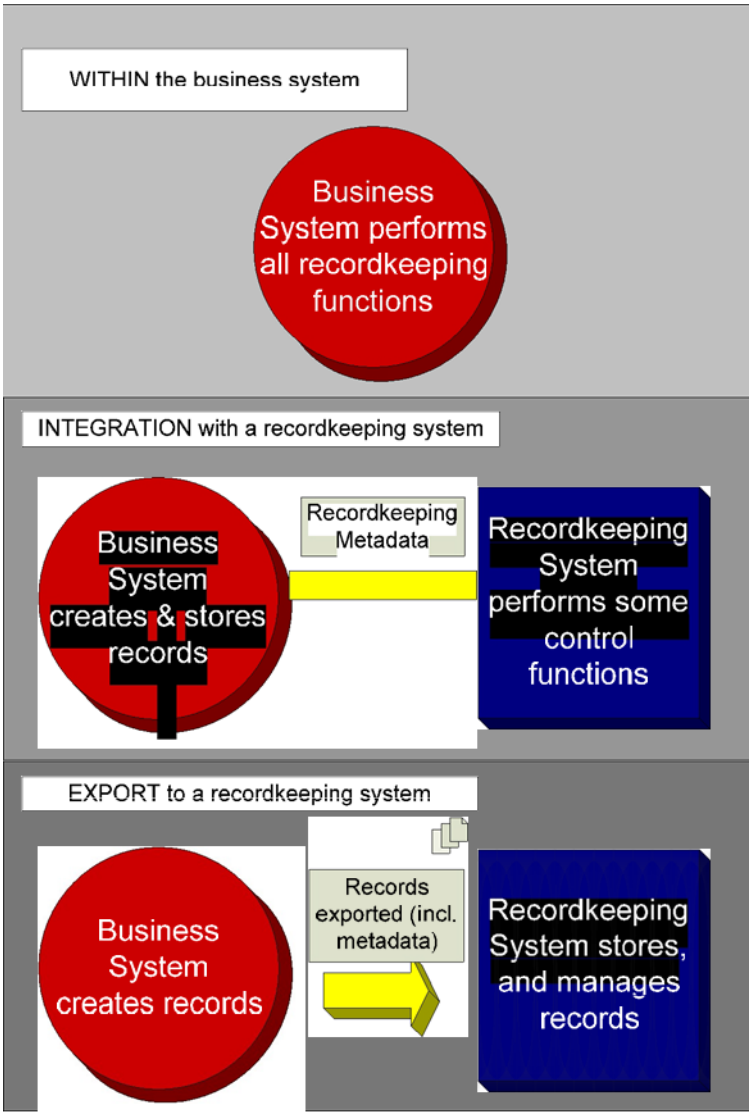
To be considered authentic and reliable evidence, content must be fixed to a point in time and unalterable. Because business systems generally contain dynamic, current data that is subject to regular updates, strategies for maintaining a 'fixed' record must be implemented. These strategies will be influenced by the decision regarding which system will manage the records, and informed by an options assessment. Agencies will need to consider the extent to which functionality for records will be provided through internal mechanisms within a business system application itself, or whether the requirements will be met by interacting with software applications external to the system that are capable of providing the necessary records management functionality.

The functional requirements outlined in this advice include core recordkeeping process that must be addressed when managing permanent value records in business systems. Options to implement these requirements are shown in Figure 1 below and may include:

- designing the business system to internally perform the records management functions;

- integrating with an identified records management system, such as an electronic records management system; or
- designing export functionality into the business system to directly export records and their associated metadata to an identified records management system.

Possible system options for managing records created in business systems



Source: *Principles and functional Requirements for Records in Electronic Office Environments Module 3 Guidelines and Functional Requirements for Records in Business systems*, International Council on Archives

These options are not exhaustive and others may be explored by organisations in determining a suitable approach.

For business systems that manage distinct digital objects, 'fixing' a record can be done through system controls, such as setting the object as 'read only', and applying record metadata that documents the record's management and use over time, for example, event history metadata.

Database systems usually contain data that is frequently updated, manipulable and non-redundant or current, and therefore can pose challenges for ensuring the fixity of a record. Strategies to address this could include:

- Designing controls that prevent the overwriting or deletion of specific data into the system. For example, this could involve permitting the updating of data but recording the previous values in a history status field. The record is formed by the combination of specified fields and the associated event history information. This does not mean all changes to data in the system are required to be retained. It is only applicable to those data elements that have been identified as forming the content of the evidential requirements.
- Bringing together the selected data elements (this may be from within the same table or selected data from rows in different tables) and creating a distinct digital object that is fixed and unalterable. This strategy could be satisfied by the generation of a report, or a read-only 'historical' version of the database.

Regardless of what strategy is selected, it is essential to ensure all core recordkeeping processes are addressed so that records are not only created and managed, but can also be appropriately disposed of.

Table 5: Examples

For Example…
A staff member enters details of a new client into the system. The client later changes their name and the staff member updates the system with the new details. The original name is still retained by the system, and is managed and maintained as part of the record accordingly.
The value of assets for an insurance policy is automatically indexed each year and the 'asset value' field is automatically updated. To prove the value of the assets at the time of a claim, the information from the 'asset value' field is moved to a 'previous value' field when the update occurs. The system maintains previous values for the past three years (as a claim must be made within three years of an event), **and** for every year where a claim was made, in accordance with an approved Retention and Disposal Schedule. The system logs the deletion of expired data, including appropriate approvals.
An organisation uses a business system with a workflow engine to support the processing of loan applications. When the application is finalised, the system automatically generates a report giving details of the process, which is then stored as a record in their electronic records management system. The appropriate contextual information of the process, in the form of metadata, was gathered as it was routed through the engine and exported with the record to the electronic records management system.
A database is used to maintain customer orders. According to the organisation's Retention and Disposal Schedule, order details are required to be retained for two years after the order is completed. Once a year, a query is run on the system to identify all orders that were completed more than two years previously. The results of this query are checked by relevant staff to ensure they do not relate to any outstanding issues, and once approved, relevant fields are deleted. The report, sign off and confirmation of deletion are kept as evidence of this process. The process was carefully designed to ensure only fields relevant to the order would be deleted, and customer details (which are required to be retained for longer) were not affected.

Source: *Principles and functional Requirements for Records in Electronic Office Environments Module 3 Guidelines and Functional Requirements for Records in Business systems*, International Council on Archives

The decision as to which approach to take for a particular business system will be affected by a number of factors:

- the business needs, including the risk level for the particular business function. High-risk functions require more stringent documentation and records management controls;
- the overarching records management framework, including whether a distributed or centralised approach to records management is preferred; and
- consideration of what is technically feasible given the particular systems concerned. For example, this may include:
    - whether the organisation has an electronic records management system;
    - how easy integration with it would be;
    - associated costs with initial integration and maintaining the integration through product upgrades/versions over time;
    - the existing functionality of the business system and what changes would be necessary;
    - the anticipated lifespan of the existing system; and
    - whether upgrading the system to include the necessary functionality is feasible.

Table 6: below provides some indicative challenges and benefits for each of the system management options.

System Options	***Benefits***	***Challenges***
Designing the business system to internally perform the records management functions.	• Makes creating and managing the records a core component of the business process • If a component-based technical architecture is used, the records management component can be re-used for other systems • Provides additional historical data capability	• Storage issues • Increased development costs • Ensuring consistent management of related records across the entire agency
Integrating with an identified records management system, such as an electronic records management system	• Business system records can be managed collectively with records created by other systems • Exploits re-use of external records management system	• Seamlessness of process may be affected by the capability of the identified records management system • Complexities arising when upgrading either system • Challenges for disaster recovery and maintaining appropriate audit trails • May require customised interface

System Options	*Benefits*	*Challenges*
Designing export functionality into the business system to directly export records and their associated metadata to an identified records management system	• Business system records can be managed collectively with records created by other systems • May be more suited to existing systems	• Duplication of records in the business system and identified records management system • Possible shortcomings in the import /export process • Users will need to know two systems (the business system for 'active' information, and the records system for the older information) unless a continued interface is provided

Source: *Principles and functional Requirements for Records in Electronic Office Environments Module 3 Guidelines and Functional Requirements for Records in Business systems*, International Council on Archives

In summary

Developing systems that include sufficient recordkeeping requirements to effectively manage information risks, provides agencies with systems that include structures and controls within which accurate, accountable and information-rich records are created and maintained.

Recommended Reading

- Information Management Advice 18 - Managing records in business systems, Part 2: Assessing recordkeeping functionality in business systems
- TAHO Guideline 25 Managing Information Risk
- Australian Standard AS/NZS 4360-1999, Risk Management.
- Strategies for documenting government business: The DIRKS Manual, State Records Authority of New South Wales, Sydney, Australia 2003
- Principles and functional Requirements for Records in Electronic Office Environments Module 3 Guidelines and Functional Requirements for Records in Business systems, International Council on Archives
- AS ISO 15489.1-2002, Records Management - Part 1: General

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

- Planning for the Management of Information asset in new business systems, Future Proof, State Records New South Wales.
- Planning EDRMS implementation, Future Proof, State Records New South Wales.
- Systems are records of how we do business: managing the information about your business system, not just the information in your business system, Future Proof, State Records New South Wales
- Strategies for documenting government business: The DIRKS Manual, State Records Authority of New South Wales, Sydney, Australia 2003
- Characteristics and functionality of recordkeeping systems, State Records Authority of New South Wales, Sydney, Australia
- Principles and functional Requirements for Records in Electronic Office Environments Module 3 Guidelines and Functional Requirements for Records in Business systems, International Council on Archives
- Identifying information risks that might impact on high risk business, Future Proof, State Records New South Wales
- Fact Sheet Managing Records in Business Systems, Public Records Office of Victoria
- AS ISO 15489.1-2002, Records Management - Part 1: General

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	September 2015	Allegra Huxtable	Initial Release	All

Amendments in this Release

Section Title	Section Number	Amendment Summary

Issued: September 2015

Ross Latham
State Archivist