TAHO
Tasmanian Archive + Heritage Office

Information Management Advice 18 - Managing records in business systems

Part 5: Strategies for improving recordkeeping functionality in business systems

Introduction

Before migrating records and decommissioning a legacy system, agencies should assess if the replacement business system has recordkeeping functionality. Part 2: Assessing recordkeeping functionality in business systems guides agencies through a process to determine if the replacement business system has sufficient inbuilt recordkeeping functionality to maintain records of enduring or high value. If there are gaps, the system does not have sufficient recordkeeping functionality.

This section of the Advice introduces various techniques that can be utilised to improve the quality of records within a business system. These can be applied both within the system, and to the broader system environment, including the creation of business rules and procedures, not just modifying software functionality.

Techniques	Actions
Audit log security	Audit logs must be retained securely. Options include: • Storing audit logs in a separate system (e.g. save in the recordkeeping system as a read-only record) • Using digital signatures on audit logs • Purchase audit log management software
Auditing access to records	Retain a record of users who access the business system. If not within the system's audit log, then retain this as a record in the agency's recordkeeping system.
Auditing changes to records	Apply record metadata that documents the record's management and use over time, i.e. event history metadata. Retain user identity and dates each time a record is created or changed. This metadata must not alterable by other users or system administrators. If this cannot be implemented in the software, capture this metadata outside the system in the agency's recordkeeping system.
Change control procedures	Formal procedures for change control should be adopted. Make a record of: • Which version of the system was used • What system operations were made accessible to users and when • When software upgrades are performed • What quality assurance testing was carried out

Techniques	Actions
Data logging	The record is made up of metadata and data - i.e. the combination of specified data fields, and the associated event history information. Allow data updating, but capture all previous data values in a history status field as metadata. This does not necessarily mean that all data changes must be retained; only those elements that make up the record.
Documenting testing	All procedures for testing and all results should be documented. This includes analysis and testing of audit logs, event histories and access controls.
Metadata capture	Where possible, systems should be designed to capture mandatory record identifier, title, date, creator, business and format elements in the business system automatically. Where records in a business system have the same dependencies, some metadata can be applied at the aggregate or system level if preferred.
Metadata management	Metadata does not have to be retained with the record's content, but must be linked or associated in some way. Examples of externally maintained metadata include XML and other data schemas, document naming protocols, and business classification schemes which allow the records to be identified and understood over time.
Preservation metadata	Metadata is also useful to develop migration and other preservation strategies for records in the business system. For long term preservation, it is critical to record the operating system and the necessary peripherals that support each record in the system. Identify specific format dependencies for each record type, and determine the metadata that will need to be recorded about each of them.
Privileged user controls	Audit logs and controls on privileged users must be stronger than controls on other users. Define and document user roles and their associated permissions.
Read-only settings	When the business system manages distinct digital objects, 'fixing' a record can be done through system controls, such as setting the object as 'read only'. If this cannot be applied to individual records, another way to achieve this may be to produce a report (which can be saved into an EDRMS) or a read-only 'historical' version of the database.
System linkages and dependencies	The records in the business system may not be understood in isolation, so additional key information about the work processes and the business system may need to be captured. This includes: • System size and location • Known issues and faults • File formats • Security & privacy management • Data structures • Workflow rules • Audit trails • Business rules, associated policies and procedures • Links to other systems or data-sets (hard-copy or digital) • Retention and disposal requirements (e.g. Disposal Schedules)
User account management	Create procedures which reflect the level of risk related to the records in the business system: • Timeliness in removing user access after they leave a position • System access granted to users only on application, or after completion of required training, not by default

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 Guideline 22 - Use recordkeeping metadata for digital recordkeeping
- TR 16175.3:2012 Principles and Functional Requirements for Records in Electronic Office Environments, Module 3: Guidelines and Functional Requirements for Records in Business Systems (2008)

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
2.0	16-04-2014	Samara McIlroy	Initial Release	All
1.0	26-11-2007	Inter Agency Policy and Projects Unit (IAPPU), Department of Premier and Cabinet	Initial release	All

Amendments in this Release

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

Issued: May 2014

Ross Latham
State Archivist