TAHO
Tasmanian Archive + Heritage Office

Information Management Advice 60 Part 5 Successfully manage Information Risks during System Migration

Introduction

Most high value business information exists in complex information systems used across agencies and even whole of government. During government administrative change agencies and systems undergo significant change and that can put the records they contain at risk. Change currently occurring in Tasmanian Government includes the move of systems to the cloud and whole of government data centre proposals. These projects involve significant data migration and this puts records at risk.

This advice is intended to outline important considerations and risks when migrating information between systems, in order to help records and information managers provide appropriate guidance on migration projects. The advice outlines an important role for records and information managers in system migration projects, but is not intended to be a comprehensive methodology for system migration.

Migration Defined

Migration is any activity undertaken to move data from one system or platform to another. Migration may occur between major version upgrades of a system, or between applications on different platforms.

Migration is necessary because the many protocols and software components that enable records to be read and used are constantly evolving.

1. Understand that migration is a regular feature in your business environment

Migration is a constant factor for any Agency that conducts its business digitally. All digital systems will eventually be unsuitable for ongoing business purposes or for long term preservation of digital information. This may be because:

- they are built using technologies which become unsupported or difficult to support
- they become expensive to keep relative to alternatives
- they become superseded by technology with more advanced features
- they are rationalised onto a single technology platform as the result of an organisational merger
- the business function they perform is outsourced
- the business function they perform moves to a shared service arrangement
- the business function they perform ceases to exist

Even the best designed and best implemented systems will become obsolete for one or more of these reasons. As such, it is important that your Agency's records and information management strategy incorporates an understanding of the key technologies on which high value and high risk records are dependent.

2. Understand that successful migration is a complex project

Any major system migration is a complex project. It requires the input and support of a broad range of people in your Agency. Effectively managing a system migration depends on:

- understanding the information in your current system, the way it is managed, the way it is used in business processes, and the dependencies it has on other data sources
- the new system having appropriate functionality to accommodate the core data, metadata and functionality of the existing system
- undertaking a rigorous migration process which is well planned and tested before and after data migration is performed, to have confidence that the data was migrated as intended, the functionality exists as planned, and that the data can continue to be relied on as a record
- a robust quality assurance process.

Records and information managers have a central role in a migration project. This includes:

- assessing and understanding the information in the current system
- providing requirements specifications for the implementation of the new system
- determining which information must be migrated to the new system, and which information may be able to be managed in another way, and
- assisting with the development of testing procedures to ensure records and information are successfully migrated.

Any system migration is a complex and usually expensive process, involving multiple internal and external parties. Key roles that a records and information manager would interact with during a migration process include:

- *Project manager* – responsible for management and overall delivery of a project
- *Business analysts* – IT staff who analyse business requirements and translate these into system requirements
- *Architects* – IT staff who do a detailed overall design of a system's technical functionality
- *Test managers and/or testers* – responsible for defining, overseeing and performing tests to confirm whether processes and systems operate as intended

In smaller or more straightforward projects, a records and information manager might have significant responsibility for some of these functions. However, any best practice migrations are likely to be performed in accordance with standard project management methodologies. This advice focuses on core considerations and responsibilities for records and information managers, and does not detail a recommended methodology for conducting migration projects. See *Tasmanian Government Project Management Guidelines*[1].

3. Before migration, be aware of key record requirements

Records have certain defining features that must be supported during migration operations. Understanding these features is critical to maintaining record authenticity, integrity, reliability and useability during migrations.

The defining features that you need to understand before you plan for and implement migration operations are:

- records are complex
- metadata is critical
- essential characteristics must be preserved.

[1] http://www.egovernment.tas.gov.au/project_management/tasmanian_government_project_management_guidelines

Records are complex

Records are not simply data. In order to serve as evidence and information they are comprised of a complex set of related information:

- structure – the form and layout of the record
- content – the informational value of the record – this could be simple text or a complex aggregation, such as a word processed document containing a spreadsheet or a web page containing images
- context – information about who created the record, why and when they created it, how it has been managed and what other records it is related to.

All of this information must be maintained during migration to preserve the evidential and informational value of records.

Metadata is critical

Metadata is used to describe, access and manage records. It is generally the means by which much of a record's context is documented and is the ultimate means by which the integrity, trustworthiness, and authenticity of a record can be proven. It is essential that metadata is preserved and that connections between a record and its metadata are maintained during migration.

Metadata relationships that must be safeguarded during migration include:

- structural – that is within the document, such as a document containing a linked spreadsheet or images, between versions and renditions of the record
- between records – e.g. between records documenting related aspects of business
- between records and/or 'containers' – e.g. documents aggregated to files/folders
- between records and other entities – e.g. between records and creating agents
- between records and control tools such as Business Classification Schemes, Retention and Disposal Schedules, access and security controls and mandates.[2]

Importantly, metadata documenting the process of migration must also be captured.

For more information see Guideline 5 Recordkeeping Metadata.[3]

Essential characteristics must be preserved

Essential characteristics are those features that are critical to a record's meaning, use, or organisational value. All migration operations should be designed to preserve the essential characteristics of the records being migrated.

Each Agency needs to determine the essential characteristics that apply to their own specific records. Generally, essential characteristics will differ according to record type and the business purpose served by the record.

For example, a report contains a map where colours are used to signify different agricultural areas, these colours have meaning and the report could not be interpreted accurately if these colours were lost through migration to another format. For this report, the colours are a critical characteristic and any migration performed on this report must ensure that they are maintained.

[2] Queensland State Archives, Migrating digital records, 2012, page 18

[3] http://www.informationstrategy.tas.gov.au/Records-Management-Principles/Document%20Library%20%20Tools/Guideline%2005%20Recordkeeping%20Metadata.pdf

4. Plan for migration

Once you know a system is going to be upgraded, there are numerous issues to consider when developing your plan of how your migration will be performed.

Assessment and planning before the migration is essential. This means asking questions like:

- What was the business context for the creation and capture of the data? How has this evolved and have risks and requirements associated with it changed?
- How does this affect the need to retain the data? Is it low value and eligible for deletion, or needed for the very long term?
- How is metadata used to contextualise and manage other information in the system, and how can these related pieces of information be protected through change?
- Does the data contain personal information with implications for privacy protection?
- What other information does this data relate to?
- Is it both structured and unstructured? Does the data rely on proprietary systems to be read and used? Can the migration involve a process of conversion into more sustainable formats?
- Will the access and use arrangements meet requirements for now and into the future?[4]

Answering these questions provides a strong, evidence based foundation on which an appropriate migration strategy can be developed.

Once you have ascertained the parameters of the migration, it is important to analyse and identify more specific data and system issues that will require planned solutions. The following table identifies some of the data and system issues you may need to consider.

Data issues to consider in migration planning

Issue:	Discussion:
Data quality and completeness	• Does the system rely on other external data sources? • Does an audit need to be conducted to determine if the system contains a sufficiently comprehensive record of the business it was designed to capture? • Has the system been used to capture information in ways which were not part of the original specification? • Are all relevant data stores (for example, offline records – records stored in other electronic repositories) identified and included in the scope of the migration? • Are there “alternative” or informal systems which contain important evidence of the business the system was designed to capture? ? For example, video footage not being captured in the EDRMS because of file size and the records area does not have in place protocols around resizing for registration in an EDRMS.

[4] Mindful Migration, Ensuring Data Integrity through Change, Cassie Findlay, Recordkeeping Innovation Blog, 2015

	• Are data consolidation actions fully documented to help prove the integrity of the migrated records?[5] • If the business process was not fully digital, does a file audit of current locations of paper-based records need to be conducted to ascertain both the volume of records requiring storage but also so that you can incorporate the whole business process, end to end in the migration planning Does the data in the system have a relationship to the EDRMS/ECM system?
Understand user behaviour and requirements	• Establish how the system is used and what is needed to ensure people have the information they need to do their jobs • Look at how people are using existing data elements. Are people using specific fields in a variety of different ways which need to be considered when mapping to the new system's fields? For example if there is a "notes" field how is it being used? Is it being used to meet limitations of the current set of data fields e.g. inability to records a case file number from another system for example so that records can be linked together?
Implement disposal	• Can certain records and information be disposed of under an authorised retention and disposal authority, rather than migrated?
Technology dependencies	• Ensure you understand the hardware, software and underlying technical dependencies of all the records requiring migration. • Do you have systems documentation and configuration documentation in order to understand the system that you are migrating from?
Format and compatibility requirements	• Ensure you understand compatibility issues such as database management system, format requirements, encryption and compression.
Non-standard records	• Determine whether non-standard use-cases (i.e. work arounds) of the system have emerged, and therefore whether there are non-standard records that you will need to incorporate in your migration plans.
Older records that have undergone multiple migrations	• Check the earliest records in your system. Look at their quality, check their dependencies, look at what is going on with these records and what is required to support their ongoing maintenance.
Comprehensive systems testing	• Ensure that there is a comprehensive testing process in place which determines whether all records requiring migration are actually migrated.
Understand metadata	• Perform metadata mapping between the original and the target system. This will ensure that all necessary metadata fields and their values are preserved following migration.

[5] These points were principally drawn from Part II, Section 1.2 of ARMA International, ANSI/ARMA 16-2007, The digital records conversion process: program planning, requirements, procedures. No online reference.

	• Some metadata is not explicit. For example, some metadata elements, such as retention rules, security classification and access restriction, are applied through inheritance from a parent record or container. At migration you need to determine whether these values would be handled in the same way by the new system. • Migrate records management controls such as retention and disposal authorities, security classifications and record classification tools. • Maintain any additional functionality driven by metadata. If metadata is used to automate activities (such as disposal or preservation actions) or if metadata reuse or other forms of automation have been used in the system, then this functionality must be safeguarded during the migration.

Where relevant, plans should be made to address these and any other issues identified before your migration is conducted.

Once your planning is complete you will have a thorough understanding of your records as well as your current and target systems. This will enable you to:

- begin to address the issues that must be resolved before migration can commence
- identify the desired target state of your records post migration
- contribute to the development of a migration method that will convert your records, including all metadata and essential characteristics, from their current state to the target state.

At all stages of a typical migration project, value can be derived from an approach that is mindful of the business context and requirements for the data:

- **Business case** – how can the migration of the system/s be done in a way that will bring benefits from more usable, robust data? Where can these be quantified and where are there intangibles? What risks can we manage by a mindful approach to the migration?
- **Project initiation** – which stakeholders will understand the information risks and opportunities associated with the system? Which technical resources and expertise will be required to manage format conversions, metadata extraction and analysis, and more?
- **Planning** – understanding the data, metadata and any unstructured information that is to be migrated and confirming that which is to be left behind (with regard to identified regulatory, compliance and business requirements); ensuring the migration takes account of relationships and the persistence of these; confirming format/s conversion choices
- **Execution** – migration execution involves not only the management of the data that is copied to the new environment, but management of the 'source' system. Are there requirements for it to be preserved for quality assurance or other needs? Execution also means making sure you have an accountable process: tracking and recording the stages along the way.

There are a range of tools that can assist with some of the technical aspects of systems migrations, from export functions that come with the systems themselves, to data extraction and normalisation tools such as EMC's InfoArchive or specialised digital preservation tools developed in the international digital preservation community.

The use of any of these sorts of tools must be directed by the analysis and identification of the risks and requirements relating to the systems. This means a thorough understanding of optimal data models of source and target systems, and a clear idea of how to make the data sustainable over time. With this grounding, mindful migrations will ensure our critical business data is secure, rich in context and usable for as long as we need it.[6]

5. Understand the Information Risks that can occur during Migration

The information risks that can occur during migration process include:

- information that cannot be generated in a useable form
- information that cannot be maintained in a useable form
- information that is incomplete
- information that is meaningless
- information that cannot be trusted
- information that cannot be authenticated
- information that is inaccessible

The following table identifies risks that can occur during each stage of a generic migration project. It's critical to analyse the system migration process, identify possible areas of risk, and put in place risk mitigation strategies for your specific migration project.

[6] Mindful Migration, Ensuring Data Integrity through Change, Cassie Findlay, Recordkeeping Innovation Blog, 2015

Migration Project – Generic Information Risk Assessment Project Stage/ Description

1. Migration Project Initiation

The initial stage of high-level scheduling and resource planning for the project.

Potential Recordkeeping Implications	*Risk*	*Impact*	*Risk Treatment/ Mitigation*	*Control*
Project Planning • Recordkeeping requirements are understood by project team • Risk mitigation planning is commensurate with level of value associated with the records e.g. permanent value records • Appropriate scheduling of time and resources for migration actions for digital records • Project is managed using a formal project management methodology, including change management processes.	• Limited knowledge of recordkeeping requirements of the agency • Risk planning not undertaken • Recordkeeping actions not included in project plans • Lack of comprehensive project plan for migration	• The objectives of external suppliers (e.g. vendors) become the objectives of the project. • Recordkeeping actions are not included in the project plans • Unforeseen events occur due to lack of comprehensive project planning • Permanent value records are lost or become inaccessible	• Ensure recordkeeping requirements, standards and activities are well understood by the project team, and sufficiently incorporated into the planning and scheduling for the project. • Ensure that key project team members are trained from project initiation. • Ensure project manager has sufficient skills and access to subject matter expert/s	Template for a project business plan – See *Tasmanian Government Project Management Guidelines*
Roles and responsibilities Effective management of the project requires clearly defined roles and responsibilities for the migration process, and within the project governance frameworks. Without this your staff and vendors will not have an understanding of what is expected of them, will lack accountability and will be unable to ensure a successful migration and the continuity of the records. Ensure: • A multi-disciplinary team has been assembled to manage the migration and they all understand the recordkeeping requirements, the information risk involved in the migration and the ongoing digital continuity requirements of the Agency • Records manager/ subject matter expert should be included in migration project to ensure recordkeeping requirements are integrated into the project plan, to ensure authenticity and evidential integrity of state records through the migration process. Recordkeeping requirements include: • Appraisal and disposal • Ongoing records management needs • Quality assurance of migrated records • Data mapping between source and target system to ensure records and metadata remain full and accurate • Identifying recordkeeping controls required in target system • Risk assessment of the migration project • Training, awareness raising and promoting continuous improvement for the use of the new system	• Lack of Records manager/subject matter expert included in migration project • Lack of project manager experience • Lack of adequate human resources • Lack of stakeholder involvement • Project team and/or project manager not available full time • No clearly defined roles and responsibilities for the management of the migration project	• Lack of complete or accurate information to support the decision making process in the project. • Lack of knowledge of recordkeeping requirements leads to bad decisions, and increased work / resourcing required after migration to fix issues • Vendor drives requirements in the absence of direction, leading to delivery of sub-standard result • Increased likelihood of mistakes and oversights. Lack of adherence to quality process. • Sub-projects (projects reliant on the outcome of the migration project) may fail or be seriously delayed or flawed • Unstable team environment. Unexpected and unpredictable delays. Loss of knowledge and skills result in project delays and subsequent errors • Lack of complete focus on the project can lead to major oversights and long delays.	• Ensure Records manager/subject matter expert included in migration project. If unavailable in-house, consult or look to TAHO for advice. • Train the project manager. Use *Tasmanian Government Project Management Guidelines*. Consult for project management resources. • Make the project owner and steering committee aware of the impact of the resourcing requirement • Reassess the viability of the project • Fund/source necessary resources for the project, or compromise on timeframes or quality • Make the project owner aware of the risks and potential impact on the project • Ensure contractor compliance with industry standards	Roles and responsibilities are outlined in the project business plan – See *Tasmanian Government Project Management Guidelines*

Potential Recordkeeping Implications	***Risk***	***Impact***	***Risk Treatment/ Mitigation***	***Control***
Stakeholder communications Note: this assessment assumes that appropriate change management activities are planned as part of the overall migration project project plan. See *TAHO Advice 55 Change Management: Preparing for change* • Important to engage with the overall project's communications strategy and the timing for migration. Important to plan for the impact on recordkeeping requirements and the business and stakeholders during the changeover between source system and target system. • Appropriate training needs to be identified. This may require targeted promotion, and development of new procedures for management of records in new system.	• Information owners not identified • Users not included in the migration planning and testing processes • Success of the migration process cannot be verified	• Key stakeholder dissatisfaction leading to project failure. • Loss of support from stakeholders. Evaporation of goodwill. Project may lose viability. Outputs not used. • Lack of acceptance by stakeholders – system is not used	• Develop an Information Asset Register identifying information owners See *TAHO Advice 40 The Role of an Information Asset Owner* • Complete a stakeholder analysis • Ensure key stakeholders have adequate representation and consultation (steering committee representation) • Consult stakeholders on project plans • Include stakeholders in the migration project • Stakeholder engagement plans provide the means for recordkeeping requirements to be promoted across the agency. This reduces the risk of records being lost, or inappropriate accessed due to ignorance of what the recordkeeping requirements are. • Training in records management practice provides hands-on experience of recordkeeping to agency personnel. This lessens risk by providing the opportunity for agency personnel to understand the implications of what is being asked of them so that they can raise any issues they may have, and improve recordkeeping practice.	• Information Asset Register See TAHO *Advice 39 Developing an Information Asset register* • Stakeholder Management Plan Template. See Tasmanian Government Project Management Guidelines

Potential Recordkeeping Implications	***Risk***	***Impact***	***Risk Treatment/ Mitigation***	***Control***
Project governance Your information governance structures affect your ability to manage a migration to ensure the continuity of your digital records. Effective management of digital continuity requires senior ownership and coordination of the project from across the Agency. Gaps or failings in your information governance structures will leave you exposed to risk. Note: this assessment assumes that the governance structures for the overall project are in place, documented and signed off in the project plan. Specifically, governance around the migration process needs to ensure: • Appropriate migration planning and documentation is produced and signed off by the steering committee. See *Interim Guideline 24 Migrating Digital Records.* • Steering committee understands the information risks facing the agency as a result of the migration project • Is the steering committee aware of the potential impact on business integrity should the confidentiality, integrity or availability of information be compromised? • Has the risk of each stage of the project been assessed and mitigated and the migration plan signed off by the project steering committee? • Has any personal or sensitive information been identified in the data being migrated?	• Absence of data governance policies • Lack of steering committee • Poor leadership of the project • Unidentified project sponsor • Lack of management understanding, control/governance of digital information • Lack of project planning and scoping	• Proposed project conflicts with existing policy / cultural norms around information governance, and hence not fully utilized or marginalised • Lack of direction will delay decisions, extend project timeframes, drive project in the wrong direction, resulting in outputs that are not fit for purpose. • Inability to resolve significant business and project management issues in timely manner • Limited utilisation of project outputs (the new system) resulting in failure to deliver the agreed project outcomes • Digital records not migrated or inaccessible	• Develop a data governance policy • Form steering committee • Identify project sponsor and outline their role in the project business plan. Obtain agreement from the project sponsor and steering committee • Document the business purpose of major digital information assets. • Document and assign roles and responsibilities for management of the digital information. • Ensure mechanisms are in place for addressing changes in technology and/or responsibilities. Plan for the end of contracts with vendors, by ensuring the contracts address the current and future control of the digital information, for example, post-contract.	Project governance arrangements should be outline in the project business plan – for a template see *Tasmanian Government Project Management Guidelines*
Vendor Management Note: this assessment assumes that appropriate vendor management activities are planned as part of the overall project plan. Specifically, vendor management for the migration process needs to ensure: • Appropriate migration planning and documentation are produced by the vendor and signed off by the steering committee. Ensure that the Vendor contract specifies exactly what migration tasks you want the contractor to perform. This could include planning, identification of issues for remediation, metadata mapping, testing, implementation etc. You must also ensure that you specify exactly what documentation you want from the contractor. User Acceptance Testing (UAT) includes a formal process of sign off by stakeholders.	• Vendor lacks experience in migration processes • Project team inexperience in management of contractors, leads to the migration being completed without adequate verification and documentation • Inadequate signoff verification/ confirmation of the results of the migration	• Lack of adequate verification testing during migration processes • Migration process cannot be verified • Required documentation not produced • Source system cannot be approved for decommissioning/destruction • Permanent value records are lost and inaccessible	• Contractual obligations of vendors make it clear the standards to be met. Ensure documentation/ process requirements are outlined in the contract • Ensure documented testing and verification process are signed off by stakeholders. A process for managing vendors performance against these standards, including looking at their activity during the process should be developed	*Information Management Advice - Questions for vendors when selecting new business systems.*

2. Determining what is to be migrated

The stage where the scope of the migration is established

Potential Recordkeeping Implications	***Risk***	***Impact***	***Risk Treatment/ Mitigation***	***Control***
Identifying the records Details about the records must be established to inform decisions about what needs to be migrated. Digital records include a complex set of related information including: • The context of the records • The contextual metadata, information about who created the record, how it has been managed, relationships to other records • Structure that enables the record to be accessible and meaningful e.g. the database table headings Clearly scope and document the records prior to migration. If records cannot be easily identified and described then you will need to undertake an analysis of the business processes associated with the system use to identify the information that records the evidence of business activity and transactions.	• Recordkeeping analysis and appraisal not carried out • Crucial relationship between data tables not identified • Contextual metadata is lost during the migration process • The records lose their context	• Records are migrated without meaningful metadata, they lose their context and cannot be relied upon. • The records cannot be used as evidence of business activity potentially leading to negative outcome for the department during Royal Commission or litigation	Analyse the records prior to migration. Determine an appropriate migration / disposal strategy for each category of record. This assessment will make it easier to estimate the amount of work required to migrate the legacy data successfully	• Checklist *Advice 18 Managing Records in Business Systems Part 1* • See *ISO 16175 Principles and Functional Requirements for Records in Electronic Office Environments.*
Establishing the retention requirements • Identify the retention period for the records by reviewing relevant Retention and Disposal Schedule/s and consider any other legal obligations e.g. records subject to litigation, discovery process. • If there are no longer any legal, business or legislative requirements to retain the records, undertake an authorised process to dispose of any records that have met their minimum retention period. If there is no authorised Retention and Disposal Schedule covering the migrated records, disposing of them is unlawful. Contact TAHO to appraise the records.	Records retention requirements are not identified	Records are migrated without contextual metadata required for retention and destruction process (their classification). This will require reassignment of classification to each record resulting in extensive manual work	• Mapping of retention requirements for the data being migrated • Clear guidance on what records need to be kept and how long for	• Document data cleansing and disposal decisions • *Advice 9 Disposal of Scheduled Records* • Advice 18 Managing Records in Business Systems Part 3 & Part 4 • Relevant Retention and Disposal Schedules

Potential Recordkeeping Implications	*Risk*	*Impact*	*Risk Treatment/ Mitigation*	*Control*
Determining recordkeeping metadata • ***Point of capture metadata, and audit trail and version metadata*** Recordkeeping metadata is not a static profile of a document. It initially defines a record at the point of capture, but is also dynamic and accrues through time, to provide information on how a record has been used or managed. This characteristic of recordkeeping metadata is essential for preserving the authenticity of records. • ***Identify metadata relationships*** Documenting this metadata will help to highlight all the necessary data that must be migrated, particularly metadata which records the information about relationships and connections between data. Relationships requiring safeguarding may be: o structural – that is within the document, such as a document containing a linked spread sheet or images o between records – e.g. between records documenting related aspects of business o between records and/or 'containers' – e.g. documents aggregated to files/folders o between records and other entities – e.g. between records and creating agents o between records and control tools such as Business Classification Schemes, Retention and Disposal Schedules, access and security controls and mandates. • Some of this metadata may be outside the system e.g. Business Classification Scheme. This will need to be captured. • Map the metadata from source to destination system to record the record context and authenticity of the records • Capture metadata about the migration, as it is an event in the lifecycle of the record • Identify other metadata to capture, for example linking or key tables.	• Failure to perform metadata mapping between the original and the target system • Failure to migrate records management controls (these are retention and disposal schedules, security classifications and record classification tools.) Maintain any additional functionality driven by metadata. If metadata is used to automate activities (such as disposal or preservation actions), or if metadata reuse or other forms of automation have been used in the system, then this functionality must be safeguarded during the migration.	• no metadata mapping means that all necessary metadata fields and their values may not be preserved following migration. The records context and authenticity may be lost. • Functionality may be lost and expense incurred if these tools and the functionality they deliver is not adequately identified and migrated to the target system. Complex relationships can exist between one or more of these tools, and some or all records in the system	Perform a metadata mapping exercise between the original and the target system	• *Advice 18 Managing Records in Business Systems – Part 2* • **Metadata Mapping** Metadata mapping is a critical part of migration planning. Mapping fields between the old and new systems will help to identify all your critical metadata and will make sure that it is all migrated. See the Metadata Mapping template in TAHO Metadata toolkit • **Configuration Specification** System configurations, including hardware configuration, software settings, metadata definitions and metadata mappings should be documented.

Potential Recordkeeping Implications	***Risk***	***Impact***	***Risk Treatment/ Mitigation***	***Control***
Understanding characteristics of the records and the recordkeeping system Analyse and document the characteristics of the records including: • **Content** – information content within the record, e.g. text, still and moving images, audio, and other intellectual productions. • **Context** - information that describes the environment in which the content was created and managed, e.g. creator name, date of creation, file format. • **Structure** - information that describes the extrinsic or intrinsic relationship between content, required to reconstruct the performance of the record, e.g. e-mails and their attachments. • **Appearance/rendering** - any information that contributes to the re-creation of the performance of the record, e.g. font type, colour and size, bit depth. • **Behaviour** - properties that indicate the method in which content interacts with other stimuli, e.g. hyperlinks. **Technical dependencies**, identify other systems, platforms, formats • consider the characteristics from different business perspectives and usage requirements. • advise on the priority of the characteristics that need to be carried over with the migration. • at a minimum, those characteristics that contribute to the authenticity, access, usability and meaningfulness of the records should be preserved. • undertake a risk analysis of the characteristics which will or will not be carried over, and justify and document decisions about acceptable change and/or loss	The characteristics of the records are not defined prior to migration	Migration process doesn't take into account the unique characteristics of the records, and may change the records. For example, formats of the records are not identified and earlier versions of word documents do not migrate successfully, resulting in corrupt, inaccessible records.	Develop a comprehensive migration plan that identifies types of records, formats, metadata, etc.	• Risk analysis – *TAHO Guideline 25 Information Risk* and *Advice 60 Applying Risk Management Processes* • Migration Plan

3. Determining where & how to migrate

The stage when decisions are being explored and made about the approach, method and target system(s) for the migration

Potential Recordkeeping Implications	***Risk***	***Impact***	***Risk Treatment/ Mitigation***	***Control***
Verifying target system/s recordkeeping capabilities To determine migration options identify: • What records are required for ongoing business purposes – active or inactive records? • Whether different migration options should be applied to inactive records? • business, recordkeeping and technical issues/ constraints which determine migration options • record controls in the current system e.g. are they built into the system or exported and managed through a separate system? • the ability of target system to meet recordkeeping requirements • record retention periods (this will influence migration options). • Whether all relationships, links and dependencies between records can be maintained in target system	• Recordkeeping features are not identified • Recordkeeping controls are not identified as necessary and migrated with the data • Target system lacks adequate recordkeeping capabilities	Data quality is affected, recordkeeping controls are not migrated, leading to additional work and cost to manage records through their lifecycle	• Investigate if strategies 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 • Audit log security • Auditing access to records • Auditing changes to records • Change control procedures • Data logging • Documenting testing • Privileged user controls • Read-only settings	• System Functionality Comparisons • *Advice 18 - Managing Records in Business Systems - Part 5* and the attached *Assessment tool: Measuring recordkeeping compliance in business systems*

Potential Recordkeeping Implications	***Risk***	***Impact***	***Risk Treatment/ Mitigation***	***Control***
Making file / record format decisions • Ensure that the target system/s have recordkeeping capabilities and/or will meet the requirements for retention management. • Plan to minimise the need for record migrations by determining a target system/s and record format(s) that suit the records' retention periods and record types. • Understanding the retention requirements, conversion formats and their associated stability also involves an active and ongoing commitment to their monitoring and maintenance.	• Lack of understanding of the range of formats held in the system - these have not been identified and analysed for accessibility. • Poor choice of digital file formats may introduce risks of the information becoming unusable or inappropriately accessed through technology dependence, format obsolescence or limited choice of rendering or viewing software. • Reliance on proprietary formats that can only be used with specific technology products. • Reliance on specialist, bespoke or legacy systems. • Use of file formats that are at high risk of technical obsolescence. • Creation of information that is highly structured or has complex interdependencies, including datasets and databases.	Corruption of older formats during migration process renders records inaccessible	Use formats that are: • standards based • widely supported and • not reliant on the use of proprietary software.	• **Migration Plan** A documented and approved plan must - be devised, that comprehensively outlines the approach to be taken for all of the information in the business system and for the corresponding security classification. • **Migration Project Plan** This may be included in the migration plan. It will detail the dates/times of the migration activities and the people involved, including their roles and positions. • **Project Variations** Any variations to plans around the recordkeeping considerations, and any necessary variation in records structure, metadata, format or content that will, or has, resulted from the migration

Potential Recordkeeping Implications	*Risk*	*Impact*	*Risk Treatment/ Mitigation*	*Control*
Establishing migration approach • Document and secure approval for the plans that describe what will happen to all of the information within the system including the corresponding security classifications. The plan should describe: o both the source and target business system o formats for the information/records o the tools that will be used to achieve the migration o details of any manual intervention activities o security requirements for the information o business rules and quality assurance procedures, and o roll back strategy for mitigating risks to the records, if affected by an unforeseen migration event. • Select tools which can best facilitate the maintenance of full and accurate records throughout the migration process. • Ensure migration approaches, including any transforming of the data, loading and any reliance on manual extraction is supported by clear business rules and quality checking processes. • Ensure the approach includes a tested roll back strategy, as part of risk mitigation planning	• Lack of approved migration plan • Incomplete migration plan • Migration management processes are not well understood or followed within the agency or by vendors. • Project team do not have enough understanding of information or technology to conduct meaningful verification assessments following the migration. • Project team do not test for the continuity of information assets following change.	• Migration plan lacks sufficient detail to ensure that permanent records were migrated successfully. Migration verification testing has to be repeated or approval for decommissioning of legacy system cannot be given • Migration takes longer and costs more than estimated.	• Cutover and roll back strategy • Testing and validating the cutover and roll back strategy • A cut over strategy could be planned. Ideally use of the source system should cease, and the source system be frozen before migration commences. Business transactions may be suspended or recorded manually until the data is migrated and the new system is up and running. • If the system is critical to the functioning of the business, a snapshot may need to be taken. Data additions, changes or deletions or functions performed must be logged so the changes can be repeated in the new system. • Certain non critical functions in the source system might be suspended during the cut over period to simplify this process. For example, only new records may be allowed to be entered. • Changes to existing records may be manually recorded and performed in the new system once the initial migration is validated and signed off. • New records could be migrated to the new system in a second step to synchronise the two systems once the new system is signed off as functional, and the source system frozen • Establish a separate environment to conduct all data migration tests.	• Migration Plan • Migration Project Plan • Configuration Specification • Risk Management Plan • Migration Issues Checklist attached to *Interim Guideline 24 Migrating Digital Records*

4. Ensuring Quality

The stage when quality assurance, including testing and validation processes, are identified, planned and undertaken.

Potential Recordkeeping Implications	*Risk*	*Impact*	*Risk Treatment/ Mitigation*	*Control*
Preparing records for migration • Check accuracy of the content and metadata of the records • Sentencing projects prior to migration to dispose of records that have met their minimum retention periods • Ensure any records stored in encrypted forms are decrypted as appropriate, as maintaining unnecessary encryption poses significant risks to continuing usability and readability of state records • Document any disposal decisions arising from data cleansing activities prior to migration, and ensure the documentation is retained • Check that all relationships, links and dependencies between records are captured in record metadata prior to migration in target system	• Poor quality data in the legacy system does not migrate properly • Inadequate preparation for migration included in plan leads to failure of migration processes	• Users don't trust the system, and develop workarounds or store records in other places • Migration has to be repeated, due to inadequate preparation of records • Data corruption, leading to inability to access records	Have more than one person check accuracy and content of records	Document disposal decisions, data cleansing that occurred preparing the records for migration
Testing and validation Documented approved migration plan that includes: • Pre-migration in a test environment and post- migration in the live system • Process involves documenting baseline information about the records themselves and establishing benchmark standards and allowances. Testing procedures and processes should include steps to follow when validation or testing falls short of the standards set. • Check for completeness of the records • Check for maintenance of integrity and authenticity • All agreed characteristics of the records are maintained • Any errors or corruption during transmission are flagged e.g. identified through checksums • Check for meaningfulness and access and usability for the records e.g. real time checks of a sample of the records to ensure they remain readable and understandable • Check for reliability for the system/s including functionality, processes and integrated systems and peripherals e.g. after roll-out the system is stable and operating within acceptable error log margins that have been established	• Failure to adequately validate and test the data migration process. • Failure to identify all sources of data that need to be migrated. • Failure to identify cross-object dependencies,-and discovering new sources of data late in the project.	• System contains corrupted or incomplete data. • Blow-outs in migration timeline • System doesn't perform as expected • More UAT is required, and stakeholder engagement suffers	Check testing and validation processes within project team environment before pushing it out to larger stakeholder groups	• Testing and validation checklist attached to *Interim Guideline 24 Migrating Digital Records* • Signoffs

Potential Recordkeeping Implications	***Risk***	***Impact***	***Risk Treatment/ Mitigation***	***Control***
Assessment of Information Risks • business purpose, litigation potential and value of the records and the risks associated, including the potential business, financial and legal implications of any loss of trustworthiness or access • level of assurance that 'full and accurate' records have been achieved through the migration, including the maintenance of the completeness and authenticity of records • level of assurance that the migrated record is being well managed in a robust recordkeeping environment • thoroughness of the migration processes, including quality assurance processes and the size and complexity of the migration • extent of usage and level of integration into the operational environment of the records. **Please note:** Records that are likely to be immediately used after migration may not need to be retained for 6 months after migration as use will quickly highlight any problems. Those records that are unlikely to be used in the immediate period following migration, may need to be considered for a longer retention that fits into a quality evaluation and validation plan before disposal.	• Lack of risk assessment • Stakeholders not included in risk assessment • Risk assessment not complete	Information risks are realised and records are lost or inaccessible	• An assessment of the information risks of the migration process has been developed • Risk assessment covers the key risks and determines how critical they are to the migration processes and ongoing management of the records • This assessment uses the agency risk management framework, and embeds information risk management within the overall risk model • This assessment includes a plan for managing risks including: o Mitigation plan o Owners of actions identified o All key stakeholders including vendors • Stakeholders and vendors understand their role in managing risk • Regular monitoring and assessment of how well the plan is being implemented	TAHO *Guideline 25 Information Risk Management* and *Advice 60 Applying Risk Management Processes*
5. Performing Migration The stage concerned with the actual undertaking of the migration to extract / export, transfer and load / import the records into the target system(s).				
Testing Roll back strategy Ensure that a roll back strategy is included in planning and has been tested prior to undertaking migration activities.	• Inadequate testing and roll back strategy leads to cut over failure • Inadequate testing and roll back strategy leads to migration failure • Inadequate testing and roll back strategy leads to data loss or data corruption • Inability to restore data • Inability to roll back	Cut over aborts Aborting the migration strategy may be another consequence of errors in data transfer. What's more, cut-over aborts may happen even if data transfer seems to accomplish properly.	Documented testing and roll back strategy that has itself been tested prior to migration	• Documented testing and roll back strategy. This may be documented as part of the migration plan. • Test the roll back strategy prior to migration
Recordkeeping during cut over period • Business arrangements will need to be made to maintain recordkeeping continuity during the period when the migration activities are performed, up to when the target system becomes live and available for use. • Certain business transactions may need to be suspended or recorded manually until the new system is available, with any updates made or repeated in the new system once it is live.	• Inadequate planning for operational processes during migration may lead to extended down time, and impact capacity to work as usual because of migration failure. • System is unavailable for extended periods. • Staff continue to use legacy system even after cut-off date.	• Staff use alternative repositories for storing records, and do not change habits back once system is available again • Legacy system contains data that was not migrated to new system and cannot be decommissioned.	• Migration includes arrangements for recordkeeping during periods of system unavailability • Migrations are scheduled during user down time	***Migration Project Plan*** This may be included in the migration plan. It will detail the dates/times of the migration activities and the people involved, including their roles and positions.

Potential Recordkeeping Implications	*Risk*	*Impact*	*Risk Treatment/ Mitigation*	*Control*
Migration of Records • Migration will involve extraction/export, transformation and import/loading of data into the target system. Metadata should be captured to record the actions carried out on the data as it progresses through this extraction, transformation and loading process. Once records have been successfully migrated and all testing/validation processes accepted, it is important that stakeholder expectations are clearly communicated to the business e.g., it should be clear that the source record is no longer the official record, and business rules and processes should be established to ensure that the source records cannot be altered inadvertently or continue to be used for documenting business activity.	• Failure to maintain authenticity and integrity of records • Failure of extraction/export, transformation and import/loading of data into the target system.	• Ineffective management of records migration when software is upgraded, modified or changed may result in degraded, lost or inappropriately accessed digital information. • Loss of readability and accessibility • Inadvertent loss of records	• Appraise the nature of digital records to be migrated in accordance with approved disposal schedules to assist in determining potential risk value • Carefully manage software migration or upgrade projects to ensure continued usability and integrity of all business information. • Test for access and integrity prior to migration. • Manage in accordance with relevant records authorities. • Test cutover and roll back procedures prior to migration • Test verification procedures prior to migration	• Project Variations • Verification testing • Migration plan
Quality assuring results of the migration • Testing and validation of migration process post-migration is similar to the process undertaken pre-migration and requires the same thoroughness. • Results should be assessed, documented and a report compiled and signed off by the assigned project team and stakeholders. • This report provides essential context to records that have undergone migration and is a key event in the lifecycle of digital records. This documentation should indicate, at a minimum, that the migrated records were inspected, that metadata and characteristics were compared to the original records and were intact in their entirety, that the records were properly migrated, and that all necessary control procedures were applied during the process. Only after the post-migration testing and validation report has been signed-off, should the disposal authorisation for the digital source records be activated.	• Migration project lacks adherence to project management methodology and standards • Ineffective use of quality management practices and procedures • No testing and validation of migration process. Post-migration results not documented or signed off by project stakeholders	• The project tasks are not co-ordinated. There is high incidence of unplanned and unmanaged events. Strategies not implemented effectively. • Lack of formalised and documented process can lead to issues not being raised until critical times. Issues raised and identified can remain unresolved. • Source records destroyed without verification of effective migration.	• Use Tasmanian Project Management Guidelines for project management methodology • Maintain project quality through commitment to a proven quality assurance, testing and validation process during the migration project. Ensure commitment is gained via Business Plan. • Ensure quality assurance, testing and validation methods results are assessed, documented, and a report compiled and signed off by the assigned project team and stakeholders	Acceptance Testing Documentation

4. Post Migration

The final recordkeeping considerations prior to project closure

Potential Recordkeeping Implications	*Risk*	*Impact*	*Risk Treatment/ Mitigation*	*Control*
Verifying conditions for disposal of source records Keep the records in the legacy system for at least six months after successful migration. Retaining the source records for this minimum period will enable a repeat of the migration, if you discover that some or all of the migrated records do not meet quality control standards or business requirements. Conduct a risk assessment to consider: • The business purpose of the records and what risks are associated with the business • The implications if the newly migrated records are lost or damaged (legal, financial, business) after the legacy system has been decommissioned • Size and level of complexity of the migration and likelihood of problems arising from the process • The complexity of the records being migrated and the level of assurance that migration was successful • The capacities of the new system, with regards to recordkeeping functionality • The state and health of the legacy system	Staff discover that some or all of the metadata crucial for understanding or using the records have not been migrated	• Legacy system cannot be decommissioned • Verification process need to be repeated post migration to verify successful migration	• Risk Assessment • Keep the records in the legacy system for at least six months after successful migration	**Project Variations** Any variations to plans around the recordkeeping considerations, and any necessary variation in records structure, metadata, format or content that will - or has - resulted from the migration
Capture of mandatory recordkeeping documentation ***Metadata Mapping*** Metadata mapping is a critical part of migration planning. Mapping fields between the old and new systems will help to identify all critical metadata and will make sure that it is all migrated. ***Data cleansing and disposal*** Any data cleansing activities should be documented prior to migration. If any decisions about disposing records are made prior to migration these must also be documented, endorsed and retained permanently by the agency, as required by TAHO's guidelines and advice**.**	• Migration process not adequately documented • Vendor does not provide sufficient detail regarding technical migration process	• Source records cannot be destroyed because the State Archivist won't approve destruction • Agency must maintain legacy system until they can provide evidence that the migration was successful • In the future, Permanent records cannot be transferred to TAHO because there is insufficient metadata captured	Carefully document the migration process. See controls for details of documentation.	• Metadata Mapping – See template for Metadata Mapping in the TAHO Metadata Toolkit • Data cleansing and records disposal (including Register of Records Destroyed) See *Advice 69 Register of Records Destroyed* • Migration Plan • Migration Project Plan • Configuration Specification • Risk Management Plan • Acceptance testing documentation • System Functionality Comparisons • Sign-offs • Project Variations • Proposed list for disposal of source records approved by Agency Senior Executive

Potential Recordkeeping Implications	*Risk*	*Impact*	*Risk Treatment/ Mitigation*	*Control*
Migration Plan A documented and approved plan must to be devised, that comprehensively outlines the approach to be taken for all of the information in the business system, and for the corresponding security classification. ***Migration Project Plan*** This may be included in the migration plan. It will detail the dates/times of the migration activities and the people involved, including their roles and positions. ***Configuration Specification*** System configurations, including hardware configuration, software settings, metadata definitions and metadata mappings should be documented. ***Risk Management Plan*** Risk assessments and risk mitigation planning and controls should be documented ***Acceptance testing documentation*** This includes testing and quality assurance plans and results, pre and post migration, documenting the recordkeeping related testing and validation checks that were completed. This documentation must indicate, at a minimum, that the migrated records were inspected, that metadata and record characteristics were compared to the original records and were deemed intact, that the records were properly migrated, and that all necessary control procedures were applied during the migration process. ***System Functionality Comparisons*** Any reports that compare original system functionality to target system functionality, and documented variations. ***Project Variations*** Any variations to plans around the recordkeeping considerations, and any necessary variation in records structure, metadata, format or content that will - or has - resulted from the migration				

Potential Recordkeeping Implications	***Risk***	***Impact***	***Risk Treatment/ Mitigation***	***Control***
Disposal of digital source records The disposal of the source records must be documented. This includes approved assurances (as part of acceptance testing) that the minimum conditions were met and the appropriate further period of retention had elapsed, as required by TAHO's guidelines and advice. Records disposal can only occur if conditions in the *Disposal Schedule for Source records (DA 2159)* are met including: • Agreed quality assurance procedures as described in stage 3 of this assessment, have been conducted and any remediation need has been satisfied, • The verification of the conditions for the disposal readiness as outlined in stage 3 have been met, and • Their eligibility for disposal signed off by senior executive of the department	• Disposal occurs before period of retention has elapsed • Disposal occurs without verification of results of migration	Records not successfully migrated and are lost leading to a breach of the *Archives Act 1983*.	• Agreed quality assurance procedures as described in stage 3 of this assessment, have been conducted and any remediation need has been satisfied • The verification of the conditions for the disposal readiness as outlined in stage 3 have been met, and • Their eligibility for disposal signed off by senior executive of the department	• Proposed list for disposal of source records approved by agency senior executive • Various Retention and Disposal Schedules • *Advice 18 managing Records in Business Systems* - outlines documentation required • *Guideline 8 Digitisation and Disposal of Source Records*

6. Make records of your migration

The entire migration process and associated project planning should be documented as records. This is a requirement in *Guideline 1 Records Management Principles*

Migration should be undertaken in accordance with best practice project management methodologies. Comprehensive records of the project should include:

- a description of the records being migrated and the business function they relate to
- the identified essential characteristics of the records
- all system configurations, including metadata definitions and mappings
- a description of the factors triggering the migration project
- all reports that compare original system functionality to target system functionality
- all decisions, including decisions not to migrate certain metadata components of a record
- risk assessments
- details of any disposal and data clean-up performed prior to migration, including records of decisions and the processes undertaken
- records of management approval of migration plans
- the technical requirements of the original and target systems
- technical reports on the migration itself and the personnel involved
- details of all testing, pre and post migration, and comprehensive test reports which confirm the system is functioning successfully and that all expected data and metadata has been migrated.
- documentation of any necessary variation in records structure, design, metadata, format or content that will or has resulted from the migration
- details of the disposal of the source records used, once the appropriate quality assurance period has elapsed.[7]

7. Keep source records for at least six months

Following their successful migration, source records (the records that were used as the input to the migration) must be kept for at least six months. Retaining the source records for at least this period will enable the migration to be repeated if it is discovered that some or all of the migrated records do not meet quality control standards or business requirements.

The six month retention period should begin to be calculated from the conclusion of successful post migration testing, where the migration and all outstanding issues associated with it have been signed off by the appropriate senior manager (often the Chief Information Officer).

[7] This list draws on Queensland State Archives' guide to recordkeeping documentation contained in "Migrating Digital Records", pages 33-34.

The general retention and disposal authority requires that the Agency has properly planned, tested and documented the migration. In some scenarios, retaining source records for longer may be an appropriate risk mitigation strategy. However, the core concern for high value and high risk records and information is ensuring that the migration planning, testing and documentation is extremely robust. Increasing the retention period of the source system will not substitute for performing those processes inadequately.

Recommended Reading

Managing Information Risk (2014: Guideline 25)

Risk Management - Part 1: Introduction (2014: Advice 60)

Risk Management - Part 2: Applying Risk Management processes (2014: Advice 60)

Risk Management - Part 3: Information Risk Register template (2014: Advice 60)

Advice 18 Managing Records in Business Systems

Guideline 8 Digitisation and Disposal of Source Records

Metadata Mapping Template

Advice 69 Register of Records Destroyed

Advice 18 - Managing Records in Business Systems - Part 5 and the attached Assessment tool: Measuring recordkeeping compliance in business systems

Advice 18 Managing Records in Business Systems

Advice 9 Disposal of Scheduled Records

ISO 16175 Principles and Functional Requirements for Records in Electronic Office Environments

Tasmanian Government Project Management Guidelines

Advice 39 Developing an Information Asset register

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

- *Migrating Digital Records*, Queensland State Archives 2012
- *Effectively manage the migration of your digital records*, State Records NSW, revised February 2015
- *Mindful Migration, Ensuring Data Integrity through Change*, Cassie Findlay, Recordkeeping Innovation Blog, 2015
- ARMA International, ANSI/ARMA 16-2007, *The digital records conversion process: program planning, requirements, procedures*. No online reference.

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
	September 2015	Allegra Huxtable	Initial Release	All

Amendments in this Release

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

Issued: September 2015

Ross Latham
State Archivist