

Report on the 2010 digital recordkeeping survey

This is a report on an online survey conducted with 309 public offices in September and October 2010. The survey sought to measure compliance with the first phase of requirements of the *Standard on digital recordkeeping* and progress with implementing the second phase of requirements.

The basis of the survey was provided by the Ministerial Memorandum M2009-11 (NSW Standard on Digital Recordkeeping) which advises that public offices will be monitored by State Records for compliance with the Standard. In addition, section 12(4) of the *State Records Act 1998* requires each public office to report on its records management program in accordance with arrangements made with State Records.

The survey was quantitative and provided results and information which will be used to report on compliance with the Standard in State Records' Annual Report and will be applied to the *Future Proof Strategy* to assist public offices in implementing good digital recordkeeping practices.

This report includes a discussion of survey results and issues, see

- Appendix A for a detailed statistical report of the survey results
- Appendix B for a brief discussion of the types of new business systems acquired by public offices, and
- Appendix C contains feedback from public offices on the survey.

Standard on digital recordkeeping

The *Standard on digital recordkeeping* was issued in September 2008, with minimum compliance requirements commencing from 30 June 2009. Ministerial Memorandum M2009-11 (NSW Standard on Digital Recordkeeping) noted that the Standard provided measurable benchmarks for digital recordkeeping systems and practices, with full compliance by June 2012.

Requirements within the *Standard on digital recordkeeping* have been phased in, so that public offices had sufficient time to implement requirements. The Compliance timetable, issued with the Standard in 2008 identifies the three tiers of requirements to be introduced from 30 June 2009 to 30 June 2012:

1. From 30 June 2009 public offices need to define digital records for any new system that was acquired or built after this date, ensure that recordkeeping requirements were built into new systems and that metadata mappings of new systems were made. Additionally all public offices were reminded that from the date of the issue of the Standard, that the disposal of recordkeeping metadata should be in accordance with the requirements of the *State Records Act 1998*.
2. From 30 June 2011 public offices need to define digital records for high risk business processes supported by existing systems.
3. From 30 June 2012 public offices need to be able to demonstrate that existing systems which capture and manage records of high risk business processes meet the requirements of a digital recordkeeping system as specified in the Standard and that metadata mappings of such systems are complete.

The purpose of the survey was to seek responses from public offices in order to gauge compliance with the first set of requirements and to gauge progress within the NSW

public sector in implementing the second set of requirements. The discussion of responses to the survey below indicate that the NSW public sector is still grappling with the challenges of the digital environment and the requirements of the *Standard on digital recordkeeping*.

Awareness of digital recordkeeping

The 2010 survey has focused attention on digital recordkeeping within senior management in many public offices and has raised awareness of the need for further clarification about the challenges and issues that digital recordkeeping poses to public sector organisations.

A very early issue to emerge during this survey was the level of understanding amongst public offices of the *Standard on digital recordkeeping* and associated guidance which had been issued by State Records. It has been obvious that there is a level of confusion amongst public offices about the distinctions between business systems, records management systems, and digital recordkeeping systems. To clarify these misunderstandings the following definitions have been used in the survey:

Business systems are technology based systems in an organisation which are not identified as a records management or information asset management system. Business systems can take many different forms and have 'system owners' who are generally in a role/position that pertains to the type of information or data that is kept in the system. Some common examples of business systems include:

- a web content management tool
- a collaboration tool such as Sharepoint
- an application that is being used or deployed across the organisation for financial management, human resources management, project management etc, such as SAP or Sybase
- an application that is available from a website, such as the whole of government e-Recruitment system
- a custom designed or off the shelf case management system tailored to meet the needs of the organisation.

All the above systems create and capture records. Public offices need to evaluate how well the systems create and capture records and determine strategies for ensuring that records created using these systems are managed appropriately. In some cases, the system meets the requirements of the Standard and the records can reside in the business system. In other cases, it is better for the records to be exported from the system and managed in the organisation's records management system or information asset management system.

Records management systems or information asset management systems are software applications systems such as Electronic Document and Records Management System (EDRMS), a Records Management Application (RMA) or an Enterprise Content Management (ECM) system. NSW Government agencies purchase such systems through the whole of government panel contract for Information Asset Management Software (IAMS). Products currently on this contract are: ELO Digital Office, EMC (Documentum), Interwoven, Netcat, Objective, Opentext, Oracle, Sharepoint, TRIM, and Vignette.

Digital recordkeeping systems are systems that comply with the requirements of the Standard. They can be:

- a business system which includes recordkeeping functionality, or

- a business system which is linked to a records management / information asset management system, or
- a dedicated records management / information asset management system.

Survey pool

309 public offices were surveyed, including:

- 132 NSW Government agencies / authorities / state owned corporations (43% of survey pool)
- 151 local government organisations (49% of survey pool)
- 16 public health organisations including Area Health Services (5% of survey pool), and
- 10 universities (3% of survey pool).

The response rate for the survey was 100% with responses received from 309 public offices.

In the following discussion of survey results, percentages are used with number results in brackets. For a complete statistical report on each question of the survey, please see Appendix A.

Issues and trends

New business systems

Questions 1, 2 and 7 of the survey questionnaire were designed to assess how well public offices were conforming with the set of requirements in the *Standard on digital recordkeeping* for new business systems acquired after 30 June 2009. While some public offices responded that they had acquired new business systems which were in effect EDRMS or recordkeeping systems, generally public office records management staff responded about the new business systems which had been introduced to automate a business process and were located in various programs within the organisation and not necessarily the immediate responsibility of the records manager.

This aspect of the survey raised awareness of digital recordkeeping in many organisations, particularly as records management staff needed to involve ICT staff and system owners in the identification and assessment of business systems.

We were advised that:

- 38% (116) of survey participants have acquired / built / or contracted to use new business systems which make and keep records or are interfaced with an EDRMS
- 2% (5) public offices have acquired new business systems which they use only as an information resource and have no requirements for records to be made or kept in the system
- 6% (20) public offices are 'printing and filing' any records created in the new system, and
- 54% (168) of public offices have not acquired any new business systems.

These 116 organisations then assessed and reported on a total of **213** new business systems and whether they met the requirements of the Standard. An analysis of the

different types of systems acquired / built / contracted to use by the NSW public sector is available at Appendix B.

State Records asked a range of questions in order to determine if the new business systems met the minimum requirements for digital recordkeeping system functionality. Following is a summation of the information provided about the 213 new systems:

- Public offices have identified and defined the digital records required for business processes supported by the new business systems for 82% (175) of systems, while this work has not been undertaken for 18% (38) of systems.
- Of the 213 systems, 38% (82) of systems capture and maintain records and are identified as a digital recordkeeping system within the organisation, while 40% (85) of systems are either linked / integrated / or directly output records to a dedicated records management system such as an EDRMS. Thus 78% of these new systems are identified as a digital recordkeeping system as defined by the Standard.

Public offices identified that 83% (177) of these systems (whether stand alone business systems and/or integrated with EDRMS) meet the basic recordkeeping functionality required in the Standard. This means that 177 systems capture read-only versions of digital records, restrict alteration or deletion of digital records by users, retrieve and present digital records in human readable form, and restrict or permit access to records by specified individuals or groups.

Generally these statistics imply that the NSW Public Sector is acquiring and implementing business systems and applying the Standard to ensure that there are digital records of automated business processes. However, these statistics also reveal that there is a small proportion of systems (18%) which are potentially creating and capturing records but without adequate safeguards because public offices in acquiring these systems have not identified nor defined whether they should be creating and capturing records of a business process. Compounded with this, public offices identified that 22% of the systems assessed are keeping records in systems which may not be 'trusted' recordkeeping systems.

In responses to this question, it became clear that some of the business systems had been implemented by service providers/technology provider or the business system owner without consideration of the need to identify and define the digital records required for the business processes supported by the new systems.

Public offices are reminded that when business systems are acquired by the business or supplied by a service/technology provider, it is critically important and the formal responsibility of the public office under the State Records Act, to ensure that the new system meets any identified recordkeeping requirements associated with the business functions supported by the system and work out a strategy to meet them. This will involve discussions between the business system owner, the records management unit, and the ICT staff involved in acquiring and implementing the system. Strategies for ensuring that the system meets identified recordkeeping requirements may mean exporting records to the organisation's EDRMS or printing and filing if the organisation is still using paper-based recordkeeping systems.

It is critically important that public offices and service/technology providers work together on this issue and that service providers when acquiring and implementing new business systems ensure that the public office is not placed at risk through lack of evidence of its business processes and transactions nor at risk of breaching requirements of the *State Records Act 1998* and the associated standards.

Metadata and new business systems

Metadata is critical to the management of digital records. It is information that enables the creation, registration, classification, access, preservation and disposal of records. For digital records, the recordkeeping metadata becomes critical to understanding when the record was created, by whom, which business function the record relates to, and what has happened to the record over the course of time. Recordkeeping metadata also assists in proving that the digital record is authentic and reliable evidence of the business transaction.

The next set of questions asked participants to assess and evaluate whether the new business system met minimum metadata requirements from the *Standard on digital recordkeeping*:

- 88% (188) of digital recordkeeping systems were identified as capturing 'point of capture' metadata (identifier, title, date of creation, who/what created the record, business process it relates to, creating application, and record type)
- 90% (192) of business systems capture 'date of action' process metadata
- 89% (189) of business systems capture 'identification of who/what undertook the action' process metadata, and
- 87% (186) of business systems capture 'what action was undertaken' process metadata.

Process metadata includes registration into a recordkeeping system, application or changes to access rules, transfer of control, destruction or migration.

These results indicate that the majority of new business systems acquired and implemented since 30 June 2009 do meet the minimum metadata requirements for the capture of a record into the system and for recordkeeping processes.

Documenting disposal of digital records

The assessment of new business systems then looked to the capacity of the business system/digital recordkeeping system to document the disposal of digital records. While this section of the questionnaire looked to the future when digital State archives will be transferred to State Records' Digital State Archive, it also looked at current practices, as public offices have been encouraged for some years to undertake the timely and routine disposal of digital records.

As with paper records, digital records should be disposed of in accordance with authorised retention and disposal authorities. Digital recordkeeping systems (either a business system or a business system linked to an EDRMS) need to be able to identify what happened to the record. Interestingly, many public offices responded that this question was not applicable for many of the new systems (75% or 159 systems), as there has not been any disposal or transfer of records from these systems.

Some public offices did choose to identify whether or not their systems had the capacity to document the disposal of records, regardless of whether or not they had undertaken disposal:

- 23% (50) of systems include an authorisation reference for the transfer or destruction of digital records (that is, a reference to a General retention and disposal authority or a Functional retention and disposal authority and the relevant disposal class), and
- 20% (43) of systems are able to identify where they transferred the records to (eg to another Government agency or to State Records).

It is important to remember that each public office needs to implement a regular disposal program for all of its records and that this needs to include digital records. Disposal is an essential strategic management tool which will allow public offices to manage their records over time and ensure that systems don't get clogged with records which can be disposed of under a *General retention and disposal authority* or a *Functional retention and disposal authority*. Documenting the disposal of records is also a requirement under *Principle 2* of the *Standard on digital recordkeeping* and *Principle 4: Accountable* in the *Standard on the appraisal and disposal of State records*.

Long term management of digital records

The last section of the assessment of new business systems looked at the management of digital records over time, and included questions on migration planning and ensuring that digital records are persistently linked to metadata in order to maintain their authenticity, integrity, reliability and useability. Of the 213 systems under assessment:

- migration has not occurred with 78% (167) of these systems
- 19% (41) of systems were identified as having digital records persistently linked to metadata when they are migrated or transferred out of their original environment,
- only 40% (85) of systems have documented metadata mappings which indicate how the metadata in the business system and/or linked EDRMS meets the requirements of the Standard of digital recordkeeping, and
- only 9% (20) of systems have a migration plan for the digital records and associated metadata in the system.

Of the 20 systems which do have migration plans, most of these plans appear appropriate. They identify how metadata has been migrated and persistently linked to records, includes all essential components of a record and ensures that these are maintained post migration, includes documentation of any changes or manipulations to records and their metadata that were necessary during the course of the migration, and that source records were disposed of in accordance with *General retention and disposal authority: Source records* (GA 33).

These results are of concern to State Records as they clearly indicate that public offices are not planning for the long term management of digital State records. Generally, most ICT systems are renewed or upgraded every 5 to 7 years and this will require the migration of digital State records. Without metadata mappings and migration plans, the potential for loss of digital State records or for the integrity of a public office's records to be questioned, is considerable. In addition, public offices are not meeting the requirements of the *Standard on digital recordkeeping* and the *General retention and disposal authority: Source records* (GA33). This could create serious storage overload as source records cannot be disposed of unless the necessary conditions for reliable migration are met.

It is important that as new systems are acquired and implemented within public offices, that time is taken to document and map the metadata in the system to the Standard. This important aspect of recordkeeping should not be trusted to chance or ad hoc approaches.

Disposal of recordkeeping metadata

Responses to Questions 3 to 5 in the survey allowed State Records to gauge if public offices have implemented Requirement 3.1 in the *Standard on digital recordkeeping*: recordkeeping metadata must be disposed of in accordance with the requirements of the *State Records Act 1998*.

These questions were responded to by all public offices, regardless of whether or not they had acquired or built new business systems. In discussions with public offices during the survey period, we had to clarify repeatedly that recordkeeping metadata was a State record and resided in the organisation's recordkeeping system or EDRMS and the business systems that the public office used which captured and maintained records.

56% (172) of public offices reported that they have identified the disposal process for recordkeeping metadata in records management policy and procedures, while 44% (137) have not. This survey question puzzled many public offices and we received a number of queries regarding this question. For the purposes of the survey, we accepted a 'Yes' response to this question if the public office had a records management policy and procedures which included the disposal of records.

Without proper policy and procedures, it is possible that recordkeeping metadata could be deleted from business systems and recordkeeping systems by individuals who are not authorised to delete this information from the business system or digital recordkeeping system for example during migration. This could have a catastrophic effect for the management of a public office's digital records, and its ability to account for when digital records were disposed of. Under the new open access regimes, it is incumbent on all government organisations to be able to account for their information.

All public offices are advised that future revisions of records management policy and procedures should include the disposal of records in all formats, and explicitly cover the disposal of recordkeeping metadata.

26% (81) of public offices advised that they document the disposal of recordkeeping metadata, while 66% (203) have not undertaken any disposal of recordkeeping metadata. This question also generated much discussion with many public offices, as there is a misconception that recordkeeping metadata may not ever be disposed of. Briefly, the disposal of recordkeeping metadata is covered in the *General retention and disposal authority for Administrative Records (GA28)*, *General retention and disposal authority for Local Government Records (GA39)* and some functional retention and disposal authorities. This disposal coverage includes capture and process metadata. Depending upon the retention and disposal action of the record, the recordkeeping metadata is required to be maintained for a number of years after the disposal of the record, or if the record is required as a State archive, the public office is required to transfer the metadata with the record.

86% (265) of public offices have measures in place to prevent the unauthorised deletion of recordkeeping metadata, while 14% (44) of public offices do not. Some public offices had difficulty in answering this question as they only have paper records managed by a records management system such as an electronic document and records management system (EDRMS) or registered in simple databases or spreadsheets. For the purposes of the survey, we accepted a 'Yes' response to this question if the public office used an EDRMS to manage paper records, while public offices using standard office applications were asked to respond 'No' as it was likely that there were inadequate protections to prevent the unauthorised alteration or deletion of recordkeeping metadata.

Public offices should ensure that all systems which capture records and recordkeeping metadata, whether they are an EDRMS or a business system, include a range of protections or security to ensure that records and recordkeeping metadata can not be altered, tampered with, or deleted. Only authorised individuals should have access rights to dispose of records and recordkeeping metadata from records management systems and business systems.

The survey results for this section of the survey indicate that there is still considerable work to be undertaken in this area of the disposal of recordkeeping metadata. The

survey, at a minimum, has raised awareness amongst public offices, that the disposal of recordkeeping metadata needs to be managed appropriately.

High risk business processes

Public offices were asked about their preparations for the introduction of the next set of requirements of the *Standard on digital recordkeeping* which are due to be implemented by 30 June 2011. These requirements focus on existing systems (business systems) in the public office which capture and manage records pertaining to the organisation's high risk business systems.

Public offices advised us that:

- 28% (85) have identified their high risk business processes, 54% (167) are progressing with this work, and 18% (57) have not undertaken this work.
- 18% (57) have defined and identified digital records pertaining to high risk business processes, 55% (170) are progressing with this work, and 27% (82) have not undertaken this work.
- 21% (64) have assessed the systems that keep the digital records pertaining to high risk business records, 50% (154) are progressing with this work, and 29% (91) have not undertaken this work.
- 11% (33) have undertaken corrective actions to meet the requirements for high risk business processes, 50% (154) are progressing with this work, and 39% (122) have not undertaken this work.

These figures indicate that many public offices have commenced or are undertaking work to prepare for the next set of requirements from the Standard, however there is still a significant number of public offices who have not yet started this work.

Of those public offices that have started this work, we were advised that many of them are re-using existing work to identify digital records of high risk business functions, for example:

- 'risk assessments undertaken by the Corporate Governance Audit and Risk Committee'
- 'development and maintenance of information asset register by ICT has informed this work'
- 'development of the organisation's business continuity plan'
- 'high risk business processes identified in the Risk Management Plan, the Information Security Threat and Risk Assessment, and Risk Register'
- 'a risk assessment/ business impact assessment process underway'
- 'the Global Risk Register identifies risks in categories based on the legislative objectives of the corporation. The register then assesses and analyses the risks towards developing treatment plans to reduce the risk as low as reasonably possible. Risks and treatment plans are allocated to identifiable owners, with specified timeframes for action'
- 'recently undertaken a comprehensive review of our Risk Assessment Framework. Through this process our high risk processes have been identified and addressed'
- 'undertaking the DIRKS process to document the functions, activities and transactions of the organisation and the recordkeeping requirements associated with these transactions. Once this is complete, we will be able to identify those transactions that are high risk and where these records are stored'

- 'high risk business processes have been identified and incorporated into electronic processes whereby they are automatically captured i.e. council minutes and financials.'
- 'high risk business processes have been initially identified in an internal audit risk process'

State Records endorses the approach of using existing risk management and audit activities for this work.

Future directions

The survey findings provide us with a great deal of valuable information on the areas in which more work is needed to achieve better digital recordkeeping outcomes across the NSW public sector. In this section of the report we look at some of the practical steps that can be taken by both State Records and public offices towards reaching this goal.

Digital recordkeeping skills and awareness

The survey highlighted that there is still some confusion and misunderstanding amongst records management professionals and others in relation to some of the basic terms and concepts of digital recordkeeping.

To help those working on digital recordkeeping in public offices with understanding some of these key concepts and techniques, State Records has a number of training and skills development offerings. These include:

- a free, 30 minute e-learning module, *Digital recordkeeping concepts*, designed to assist records managers and the staff of records management units who have some experience in records management to understand basic digital recordkeeping concepts
- a face to face one day training course, *Managing digital records: an introduction*, which provides participants with an understanding of some of the frameworks and tools required to manage digital records appropriately. It helps participants to understand and implement the requirements in the Standard, and
- a free, half day workshop, *Managing recordkeeping risk in business systems*, which is based on *State Records' Checklist for assessing business systems (RIB 42)*. It explains an approach to assessing business systems that may not be operating effectively as recordkeeping systems, where it is necessary for them to do so. It has also been developed in order to assist public offices to work towards compliance with the Standard.

We would also encourage records managers who are working with digital records to develop their knowledge and skills not only by participating in training, but also by sharing examples of good practice with one another by networking in online and face to face forums. We hope to publish more case studies and examples on the *Future Proof* blog to support this kind of collegiate approach.

The importance of managing recordkeeping metadata

The findings of the compliance survey in relation to the identification and management of recordkeeping metadata were concerning. The importance of having good quality, properly managed metadata documenting digital records and what you do with them cannot be underestimated. Recordkeeping metadata is another type of record itself and

is just as valuable as the records it relates to. For a concise overview of what recordkeeping metadata is and why it is important, see *Recordkeeping in brief: Introducing recordkeeping metadata* (RIB 18).

There are some simple steps that can be taken by records managers and other relevant staff to make sure that recordkeeping metadata is secure and works for the organisation in the long term. It is important to create metadata mappings between the digital recordkeeping system/s and the metadata required in the Standard. This will allow you to protect and use the data in the important fields in the system and not worry about extraneous metadata (this is especially useful to know when it comes time to migrate the system/s). Performing a metadata mapping of this type should be a relatively simple process. It is in essence a matter of checking off the elements in the system against the requirements of the Standard. It is also an opportunity to identify any additional recordkeeping metadata requirements that you might have over and above the minimum requirements from the Standard and which should also be identified for future migration. A basic template for performing this assessment is provided in our *Short guide to implementing the Standard on digital recordkeeping*.

Simple measures can be put in place to prevent the unauthorised disposal of recordkeeping metadata. The disposal of this valuable business record is often considered at points such as system migration and is too often, left in the hands of personnel who are not aware of its value or of the need to check retention and disposal rules. Measures might include specifying which metadata must be preserved into system migration plans, policy and procedures which state explicit rules about disposing of metadata, and briefing migration teams ahead of a migration project.

While these steps can be carried out without needing very much expert knowledge of metadata management, we would also acknowledge that many of the terms and concepts associated with the area of recordkeeping metadata can be confusing and even a little intimidating. That is why State Records will be issuing some new guidance on recordkeeping metadata later in 2011. This guidance will be in three parts; the basics for beginners; getting started; and using metadata in more sophisticated ways to bring additional business benefits.

Managing the risks associated with migration

As noted in relation to recordkeeping metadata above, migrations can be a time of particular risk for digital records and their metadata. The survey results indicate that while a great deal of effort is going into setting up compliant digital recordkeeping systems, little work has been done to date on planning for the safe migration of digital records through systems change.

We would encourage public offices to consider the long-term need for digital records and how those records will be managed. When a migration is planned, it is important to:

- consider how the content and essential characteristics of the records will be maintained and what quality control measures are going to be put in place to test whether these are being protected
- use metadata mappings to identify and plan for maintaining the persistent links between records and their recordkeeping metadata through the migration process
- set up a way to record the migration in the records' metadata – usually this would be done at a high level of aggregation, across the whole system. This metadata should then be persistently linked with the records.

- only delete the records in the source system (that you have migrated from) when you are satisfied that you have met the conditions in the *General Retention and Disposal Authority – Source records that have been migrated (GA33)*.

In 2011 State Records will be producing a short guide to planning for and managing the recordkeeping risks associated with migration, with an emphasis on establishing appropriate quality control measures and liaising with ICT staff on how to identify and protect important metadata during the migration process.

Dealing with digital records of high risk business processes

The survey found that there is still some work to be done by public offices towards meeting the second milestone of the compliance timetable. State Records is aware of the need to keep this on the radar not only of records management personnel, but also of senior managers. We will therefore be sending reminders to all senior managers with responsibility for records management compliance in the lead up to the June 2011 deadline, as well as using our normal communications channels to send reminders and advice on how to comply.

In terms of practical tools and assistance on identifying and analysing high risk business processes for records requirements, there are a number of resources currently available, including:

- *Strategies for documenting government business: The DIRKS Manual*, in particular *Step A: Preliminary investigation* and *Step B: Analysis of business activity*
- the *Short guide to implementing the Standard on digital recordkeeping* includes a section on identifying high risk business processes, including a new section containing examples of high risk business processes and associated systems in Local Government Councils, and
- the free half day workshop, *Managing recordkeeping risk in business systems*, which takes participants through a methodology for prioritising the assessment of business systems according to risk and carrying out an assessment of their existing recordkeeping capabilities.

One of the best resources, however, will be real world examples of business process analysis and documentation of digital recordkeeping requirements. That is why we would encourage records managers and others to share such documentation, and State Records will publish these on our website or on the *Future Proof* blog. We will use our usual communication channels including *For the Record* to seek these examples from public offices.

Using new systems under shared service arrangements or in the cloud

The survey findings confirmed for us that public offices are increasingly using systems for corporate services under shared service arrangements and are also embracing the use of 'cloud based' applications. State Records has been aware of these trends for some time and has developed specialised guidance to help public offices to navigate through the issues for digital recordkeeping.

These include:

- *General authority for transferring records out of NSW for storage with or maintenance by service providers based outside of the State*

- *Recordkeeping in brief: Considering digital recordkeeping as part of systems development or procurement (RIB 52)*
- *Recordkeeping in brief: Keeping recruitment records using e-Recruitment (RIB 56)*
- *Recordkeeping in brief: Storage of State records with service providers outside of NSW (RIB 54), and*
- *Recordkeeping in brief: Using shared services for records management (RIB 44).*

Public offices can take action to ensure records are properly made and managed by incorporating records requirements into contractual arrangements and service level agreements, and insisting on assurances from service providers regarding records formats and export capabilities for the return of the records when entering into arrangements to use cloud based applications.

Records managers and others can also help by sharing examples of documentation such as service level agreements or contractual provisions, particularly for systems that are widely used across government. Where given permission to do so State Records will share these via our website and the *Future Proof* blog.

We also plan to continue to work closely with the providers of shared corporate services and the Department of Premier and Cabinet to ensure that wherever possible recordkeeping considerations are part of the planning and development of systems and services, not an afterthought.

The rise of Sharepoint

It is obvious that many public offices are adopting the Microsoft tool Sharepoint for a range of information management uses, including the capture and management of digital records. Sharepoint, while not approved for all modules of the most recent whole of government contract for Information Asset Management Systems (GSAS 2602: Information Asset Management Systems (IAMS) Software Applications <http://www.nswbuy.com.au/information-technology.aspx>), has a range of capabilities for capturing and managing digital content, including as records. Public offices who are expanding their use of Sharepoint to meet recordkeeping needs are encouraged to contact us to share details about their efforts, so we can provide case studies and practical tips to other public offices who might be going down the same path.

Disposal of digital records

The survey results indicate that the disposal of digital records is another area in which public offices are finding it difficult to make progress. Indeed, in many cases it seems no disposal of digital records is taking place at all.

Through research activities in 2010 including the 'Digital State archives at risk' project and the ICT Attitudes survey, we have identified a number of obstacles for records managers who are seeking to implement processes for the disposal of digital records. Accordingly, we have commenced a new strategy to address some of these obstacles and provide public offices with practical advice and guidance on carrying out disposal in the digital environment. Key deliverables of this work will include:

- the development of short information leaflets on the importance of disposal in the digital world, risks associated with offline storage and other relevant topics

- a disposal implementation project with our own digital records to be written up as a case study, and the gathering of other case studies from public offices who are carrying out disposal of digital records
- participation in an Australasian Digital Recordkeeping Initiative (ADRI) project to streamline and simplify disposal triggers in official records retention and disposal authorities, and
- promoting the use of State Records' XML schema for disposal authorities, to generate more useable disposal data for import into systems.

Further monitoring

As noted previously, the full set of requirements of the *Standard on digital recordkeeping* will be in place from 30 June 2012. We expect public offices to be working to ensure that their digital recordkeeping is compliant and is able to support Government business processes. We will be conducting another survey with public offices in 2012 to measure conformity with all requirements of the Standard.

Appendix A – Survey statistics

What type of public office is your organisation?

- 43% (132) NSW Government agencies / authorities / state owned corporations
- 49% (151) local government organisations
- 5% (16) public health organisations including Area Health Services, and
- 3% (10) universities.

Where is your organisation primarily located?

52% (160) organisations primarily located in Sydney:

- (105) NSW Government agencies / authorities / state owned corporations
- (38) local government organisations
- (12) public health organisations
- (5) universities

19% (59) organisations primarily located in a regional centre

- 31 local government organisations
- 20 NSW Government agencies / authorities / state owned corporations
- 4 public health organisations
- 4 universities

29% (90) organisations primarily located in a rural area

- 82 local government organisations
- 7 NSW Government agencies / authorities / state owned corporations
- 1 university

What size is your organisation?

- 3% (10) are very small (less than 20 FTE)
- 26% (80) are small (20 – 80 FTE)
- 28% (88) are medium sized (80 – 250 FTE)
- 27% (82) are large (250 – 1000 FTE)
- 16% (49) are very large (1000+ FTE)

Question 1: Has your organisation acquired / built / contracted to use any new business systems after 30 June 2009?

	Yes	No	Yes but info system only	Yes and 'print & file'
NSW Government	51	65	5	11
Local Government	48	95	0	8
Universities	7	2	0	1
Health organisations	10	6	0	0
TOTAL	116 (38%)	168 (54%)	5 (2%)	20 (6%)

Question 2: If you ticked A to Question 1, please list the top 5 business systems you have acquired or built since 30 June 2009?

See separate analysis at **Appendix B**

Question 3: Do records management policy and procedures identify the disposal process for recordkeeping metadata?

	Yes	No
NSW Government	77	55
Local Government	81	70
Universities	5	5
Health organisations	9	7
TOTAL	172 (56%)	137 (44%)

Question 4: Is the disposal of recordkeeping metadata documented?

	Yes	No	No disposal undertaken
NSW Government	35	11	86
Local Government	40	13	98
Universities	3	1	6
Health organisations	3	0	13
TOTAL	81 (26%)	25 (8%)	203 (66%)

Question 5: Are measures in place to prevent the unauthorised deletion of recordkeeping metadata?

	Yes	No
NSW Government	110	22
Local Government	133	18

Universities	8	2
Health organisations	14	2
TOTAL	265 (86%)	44 (14%)

Question 6: The next set of requirements of the Standard on digital recordkeeping are due to be implemented by 30 June 2011. How are you tracking with being compliant with your existing high risk business systems?

a) Have you identified your high risk business processes?

	Yes	No	In progress
NSW Government	57	15	60
Local Government	20	38	93
Universities	3	1	6
Health organisations	5	3	8
TOTAL	85 (28%)	57 (18%)	167 (54%)

b) Have you defined / identified digital records pertaining to high risk business processes?

	Yes	No	In progress
NSW Government	36	26	70
Local Government	16	52	83
Universities	1	1	8
Health organisations	4	3	9
TOTAL	57 (18%)	82 (27%)	170 (55%)

c) Have you assessed the systems that keep these digital records to ensure that the system is compliant with the Standard on digital recordkeeping?

	Yes	No	In progress
NSW Government	33	31	68
Local Government	29	54	68
Universities	0	2	8
Health organisations	2	4	10
TOTAL	64 (21%)	91 (29%)	154 (50%)

d) Have you undertaken any corrective actions to meet the requirements for high risk business processes?

	Yes	No	In progress
NSW Government	18	47	67

Local Government	12	66	73
Universities	1	3	6
Health organisations	2	6	8
TOTAL	33 (11%)	122 (39%)	154 (50%)

Question 7 Assessment of new business systems

Note: this question was answered only by those public offices who had identified that they had acquired / built / contracted to use a new business system after 30 June 2009.

1. Have you identified and defined the digital records required for the business processes supported by the new system?

	Yes	No
Universities (7 universities responded to Q7)	16	0
Local Government (47 councils responded to Q7)	60	16
NSW Government (50 agencies responded to Q7)	80	16
Health organisations (10 organisations responded to Q7)	19	6
TOTAL	175 systems (82%)	38 systems (18%)

2. Digital records captured into an official digital recordkeeping system?

	into the new business system which meets the recordkeeping functionality of the <i>Standard on digital recordkeeping</i>	into the new business system which is linked or integrated with a dedicated records management system such as an EDRMS system	into a dedicated records management system such as an EDRMS	Other
University systems	7	2	2	5
Local Government systems	23	23	18	12
NSW Government systems	38	12	25	21
Health organisation systems	14	1	2	8
TOTAL	82 systems (38%)	38 systems (18%)	47 systems (22%)	46 systems (22%)

3. Does your official digital recordkeeping system (identified above) meet the recordkeeping functionality identified in the Standard on digital recordkeeping?

	Yes	No
University systems	15	1
Local Government systems	69	7
NSW Government systems	73	23
Health organisation systems	20	5
TOTAL	177 systems (83%)	36 systems (17%)

4. Does the business system and/or linked EDRMS capture the following metadata for each record:

- unique identifier
- title
- date of creation
- who/what created the record
- the business/process it relates to
- the creating application, and
- a record type (e.g. letter / memo / report / contract / fax / schematic / blog / or locally defined types)

	Yes	No
University systems	15	1
Local Government systems	72	4
NSW Government systems	81	15
Health organisation systems	20	5
TOTAL	188 systems (88%)	25 systems (12%)

5. When recordkeeping processes are performed on digital records (eg registration into the recordkeeping system, application or changes of access rules, migration, destruction, or transfer of control), does the business system and/or linked EDRMS capture the following process metadata about the digital record:

• the date of the action	Yes	No
University systems	15	1
Local Government systems	70	6
NSW Government systems	86	10
Health organisation systems	21	4
Total	192 (90%)	21 (10%)
• identification of who/what undertook the action	Yes	No
University systems	15	1

Local Government systems	70	6
NSW Government systems	85	11
Health organisation systems	19	6
	Total	189 (89%)
		24 (11%)
• what action was undertaken	Yes	No
University systems	15	1
Local Government systems	67	9
NSW Government systems	85	11
Health organisation systems	19	6
	Total	186 (87%)
		27 (13%)

6. When digital records are destroyed or transferred, does the business system and/or linked EDRMS update metadata to include documentation of:*

**Please note, Question 6 does not add to total of 213 systems due to the way that organisations responded to this question*

• an authorisation reference for the transfer or destruction of digital records (ie a reference to a GA or FRDA and relevant disposal class)	Yes	No
University systems	2	6
Local Government systems	12	21
NSW Government systems	33	20
Health organisation systems	3	3
	Total	50
		50
• receiving organisation (in the case of transfer)	Yes	No
University systems	2	6
Local Government systems	12	13
NSW Government systems	26	20
Health organisation systems	3	3
	Total	43
		42
• not applicable, as we haven't disposed or transferred any records	Yes	No
University systems	13	3
Local Government systems	58	10
NSW Government systems	71	8

Health organisation systems	17	8
Total	159	29

7. Are digital records persistently linked to metadata when they are migrated or transferred out of their original environment?

	Yes	No	no migration has occurred
University systems	3	0	13
Local Government systems	11	2	63
NSW Government systems	26	3	67
Health organisation systems	1	0	24
Total	41 (19%)	5 (3%)	167 (78%)

8. Do you have a migration plan for the digital records and associated metadata in this system? **

** Only those organisations who responded yes to Question viii were invited to respond to Question 9

	Yes	No
University systems	4	12
Local Government systems	3	73
NSW Government systems	13	83
Health organisation systems	0	25
Total	20 (9%)	193 (91%)

9. Does your migration plan for digital records and associated metadata identify:

*This question was answered for only 20 systems

• How metadata has been migrated and persistently linked to records	Yes	No
University systems (question only applicable to 4 systems)	4	0
Local Government systems (question only applicable to 3 systems)	3	0
NSW Government systems (question only applicable to 13 systems)	13	0
Health organisation systems (no response to this question)	0	0
Total	20	0
• Includes all essential components of a record and ensures that these are maintained post migration	Yes	No
Universities (question only applicable to 4 systems)	4	0

Local Government systems (question only applicable to 3 systems)	3	0
NSW Government systems (question only applicable to 13 systems)	13	0
Health organisation systems (no response to this question)	0	0
Total	20	0
<ul style="list-style-type: none"> Includes documentation of any changes or manipulations to records and their metadata that were necessary during the course of the migration 		
Universities (question only applicable to 4 systems)	4	0
Local Government systems (question only applicable to 3 systems)	3	0
NSW Government systems (question only applicable to 13 systems)	13	0
Health organisation systems (no response to this question)	0	0
Total	20	0
<ul style="list-style-type: none"> Disposal of source records is undertaken according to the <i>General Retention and Disposal authority – Source records that have been migrated (GA 33)</i> 		
Universities (question only applicable to 4 systems)	3	1
Local Government systems (question only applicable to 3 systems)	3	0
NSW Government systems (question only applicable to 13 systems)	13	0
Health organisation systems (no response to this question)	0	0
Total	19	1

10. Are metadata mappings documented and maintained indicating how the metadata in the business system and/or linked EDRMS meets the requirements of the Standard on digital recordkeeping?

	Yes	No
University systems	7	9
Local Government systems	30	46
NSW Government systems	39	57
Health organisation systems	9	16
Total	85 (40%)	128 (60%)

Appendix B – Analysis of types of new business systems

NSW public offices have acquired / built / contracted to use a wide range of business systems since 30 June 2009. Here are a brief listing of some of the types of system that have been deployed:

- applications that have been deployed across organisations for managing finances, human resources, project management
- asset management systems
- business intelligence systems
- call management systems
- case management systems
- collaboration tools
- consultation management systems
- contract management systems
- contractor safety management systems
- customer request management systems
- development application systems
- disaster recovery systems for data
- electronic medical record systems
- email management and email archiving systems
- e-recruitment applications
- facilities management system
- GIPA applications
- grant funding management systems
- incident management systems
- inspection and maintenance management systems
- learning management systems
- local government business paper management systems
- mapping / geographical / spatial systems
- patient / medical systems
- rating and property management systems for local government
- records and document management systems (InfoXpert, TRIM, Objective, NetCat)
- student management systems
- tender applications, and
- web content management tools.

Appendix C – Feedback from public offices

- 'Completing this survey was a highly beneficial and useful exercise. The process of completing this survey provided an opportunity to consult with system Administrators and explain their digital recordkeeping obligations in a consultative manner, and also to monitor other systems producing digital records. The most challenging implementation aspect of this Standard for [my organisation] will be the migration of digital records and planning for this process. The Records Unit will take a consultative approach with other units especially ICT in planning for any migration of digital records. It would be a good idea if State Records could facilitate or present workshops, roundtable discussions or forums for interested public offices'
- 'Continuing challenges in relation to the Shared Services environment, corporate services review of government and the deployment of changed arrangements within the Super Department environment will all impact [our] response to these issues.'
- 'This survey has brought to light some of the issues around digital records that we have not yet considered. We are going to look into this more deeply in the new year and work out a schedule in order to meet the required timeframes.'
- 'A full information asset audit, business system assessment and upgrade/integration of business systems to an official digital recordkeeping system have been assigned as projects in [our] Information Asset Management Strategy for 2010-2013.'
- '[We are] in the process of a strategic planning phase with a view to understanding the requirements of the Standard on Digital Recordkeeping and upgrading its suite of systems and tools to ensure better compliance and greater interoperability and integration.'
- '[Our] digital recordkeeping program and progress in complying with the Standard on Digital Recordkeeping is constrained by limited resources and the shared corporate services reform program. [We have] budgeted this financial year to undertake an assessment of key business systems compliance with the Standard on Digital Recordkeeping.'
- '[We have] created a procedure that must be completed for all new Business Systems. As part of the implementation, of any new Business System must be approved by the Records Manager. As part of this approval the digital records stored in the system must be created as well as a metadata map to the mandatory metadata elements.'
- 'After speaking with some of my colleagues in local government, I'm wondering whether a list of 'high risk' records could be developed specifically for local government after the style of GDA 10 which could be a starting point for all local government authorities and could either be adopted or modified to suit the organisation. This could form a reference point to start asking questions. The model list might be achieved through a working party comprising local council representatives and someone from State Records. Perhaps this could be co-ordinated through the Local Government Chapter of the RMAA?'
- 'Thanks for taking the time to read our survey - I am grateful for the good work of State Records ☺'