Managing recordkeeping risk in business systems

Business systems are replacing traditional paper-based ways of doing business. However, if they are not appropriately designed, configured and monitored, they may not create or manage records - this can create risks to organisational business.

Do all business systems need to create and manage records?

No. Some systems will contain duplicate or facilitative data, or contain short term, low risk business information, or will not relate to official business. Generally, these types of systems do not have to make and manage official records.

However, if business systems support high risk business operations such as financial management, client support, project management, significant investments, high profile activities, legal matters etc., then it is important that these systems are able to create records of these operations.

Many systems that support these kinds of business operations are not designed to make and manage records. This can create significant organisational risks.

For example, an emergency services agency had a geographical information system to manage incidents. While the right data was created in this system for their needs, it was overwritten when new incidents occurred. As a result, the agency could not maintain and provide access to the information that was in the business system at a particular time in the past and therefore could not defend themselves in court regarding actions taken on that information.

When using business systems, it is vital to ensure that these systems can create and maintain or export the information your organisation needs to support its business operations.

What are the risks if business systems do not create and capture records?

Business systems don't always create 'data in context' which limits evidentiality and understanding. Data in these systems can sometimes be overwritten, changed or deleted. Sometimes the systems are configured to only retain data for limited periods of time or to keep limited metadata, which inhibits information accessibility, use and understanding.

In addition business systems don't generally flag which information within them needs to be kept and which can be thrown away. Sometimes they have no audit trails and sometimes they are designed to only perform short term business operations and to leave no lasting, understandable record of what these operations were. These systems are also changed and upgraded regularly - these frequent changes can corrupt, delete or alter business information.

As a result the integrity, accessibility, authenticity and useability of the information generated by business systems can frequently be questioned. If these systems are supporting high risk, long term or strategic business operations, this could impair your organisation's ability to function and to account for its actions, both immediately and in the longer term.

Where do I start to mitigate these risks?

To mitigate recordkeeping risks in business systems you should identify the business systems that support key, high risk digital business operations. Focus on these systems and work to ensure that the information they generate is complete, meaningful, trustworthy, accessible and kept for as long as you have business needs and requirements for it.

What are some strategies for recordkeeping in business systems?

With existing systems, to ensure you have the information you need to support your business operations in the short and long term you can:

- configure business systems so they are able to make and manage records, or
- ensure that business systems have the capacity to export data which can be captured and managed in another, secure corporate recordkeeping system, or
- integrate business systems with records management systems and automate record capture in defined workflow processes, or
- run regular, defined reports from databases and capture these in secure corporate recordkeeping systems.

Note: It is important not to assume that records can be recreated by re-querying business systems. Data may be changed or deleted over time and the system configuration may change. This will affect the ability to perform the same searches and the integrity of search results.

How can the specific risks to records in business systems be managed?

Recordkeeping risks can also be mitigated at particular points during system design, management and migration.

At systems design and configuration it is important to define what records (if any) need to be captured to support business requirements and how long these records need to be kept to meet business and statutory requirements and community expectations. Organisations also need to determine what the 'records' need to be, i.e. what particular fields need to be brought together and what metadata do they need to be connected with to provide the evidence required. It is vital to plan for good data quality to ensure that the records captured will be complete and meaningful. At design and configuration it is also important to plan for the export of information with long term value and its supporting metadata so that it can be maintained through system change, and to enable the routine purging of time-expired information when authorised to do so.

Note: It is vital that design and configuration decisions, including metadata configurations, are well documented to promote the management of records through time. Any system reconfigurations should also be documented.

At systems integration it is also important to document decisions made. Risks can arise when changes or upgrades are made to either system involved in the integration and integration pathways need to be retested or redefined at system alteration or upgrade.

At systems migration information and the metadata that describes and manages it must be supported through the migration. Significant meaning, integrity, accountability and understanding will be lost if it is not.

It is important to ensure that all current data that is needed for the new system is migrated. Other information should be deleted according to approved disposal authorities. If there are records that are not being migrated to the new system but which are still subject to retention requirements, responsibility for their ongoing management will need to be planned for and allocated. These records must not be orphaned in legacy systems.

As formats become obsolete or unsupported it is important to try and proactively manage them and any rendering tools required to view them. Unusual, ageing and complex formats will also need to be monitored through time and through system upgrades and similar changes.

When moving to cloud based business or storage environments organisations will need to carefully assess and mitigate recordkeeping risks. NSW public offices will also need to conform with the requirements of *General authority for transferring records out of NSW for storage with or maintenance by service providers based outside of the State* (GA 35). They need to ensure that the quality and trustworthiness of records are not compromised in the cloud environment and that data export capacities ensure that records and their metadata can be returned to them in accessible formats.

Further information

State Records NSW runs a free workshop *Managing recordkeeping risk in business systems* for NSW public offices. See our current training calendar at www.records.nsw.gov.au/recordkeeping or contact State Records NSW at: govrec@records.nsw.gov.au After each workshop information is posted on the Future Proof blog. Further information on cloud computing is also available via the blog.

http://futureproof.records.nsw.gov.au
Future Proof: protecting our digital future