



## What is a recordkeeping system?

All of the business systems that an agency relies on should be capable of making and keeping full and accurate records and routinely performing fundamental recordkeeping processes on a continual basis – either individually or through linked operations – so that the full range of the agency’s business activities are properly documented. These systems do not have to be dedicated recordkeeping systems. They can be business systems (such as database applications or web content managers) that incorporate the functionality required to keep records. They do not need to be large or centralised or accessible by everyone in the agency, but their recordkeeping role must be identified and administered appropriately.

Agency business systems must keep information as records. All business systems used by an agency must be capable of capturing, maintaining and providing evidence of its business activities over time to satisfy the agency's recordkeeping needs. Every agency should identify what evidence of its unique business activities it needs to keep and what particular form or content such records should have. While the purpose and content of records will vary between agencies, much of the system capability required to capture, maintain and access such records is common to all agencies. All agencies, irrespective of their unique business activities, require systems that capture full and accurate records and perform processes for managing those records over time.

In order to be full and accurate, records must be authentic, reliable, complete, unaltered and useable and the systems that support them must be able to protect their integrity over time. These terms have particular meanings for system design purposes.

- **Authentic** – it must be possible to prove that a record is what it purports to be and that it has been made or sent by the alleged person and at the time purported. Records need to be protected against unauthorised addition, deletion, alteration, use or concealment, and the making, receipt and transmission of records needs to be controlled to ensure that records makers are authorised and identified.
- **Reliable** – it must be possible to trust the content of a record as an accurate representation of the transaction to which it attests. It should be made and captured in a timely manner by an individual who has direct knowledge of the event or generated automatically by processes routinely used by the organisation to conduct the transaction.

- **Complete and unaltered** – it must be possible to protect a record against unauthorised alteration and to monitor and track any authorised annotation, addition or deletion.
- **Useable** – it must be possible to locate, retrieve, render and interpret a record and understand the sequence of activities in which it was made and used for as long as such evidence is required.
- **System integrity** – it must be possible to implement control measures, such as access monitoring, user verification, authorised destruction, security and disaster mitigation to prevent unauthorised access, destruction, alteration or removal of records and to protect them from accidental damage or loss.

The type of structural and contextual information, or metadata, which is built into an agency's business systems, and the way in which that metadata is applied, influences such characteristics. See *Territory Records Standard for Records Management No 3 – Records Description and Control* for more information.

In order to capture, maintain and provide evidence over time, systems must also be capable of performing various fundamental recordkeeping processes. These processes govern the following operations:

- **Capture** – formally determine that a record should be made and kept;
- **Registration** – formalise the capture of a record into a designated system by assigning a unique identifier and brief descriptive information about it (such as date, time and title);
- **Classification and indexing** – identify the business activities to which a record relates and then link it to other records to facilitate description, control, retrieval, disposal and access;
- **Access and security** – assign rights or restrictions to use or manage particular records;
- **Appraisal** – identify and link the retention period of a record to a functions-based disposal schedule at the point of capture and registration;
- **Storage** – maintain, handle and store records in accordance with their form, use and value for as long as they are legally required;
- **Use and tracking** – ensure that only those employees with appropriate permissions are able to use or manage records and that such access can be tracked as a security measure; and
- **Disposal** – identify records with similar disposal dates and triggering actions, review any history of use to confirm or amend the disposal status, and maintain a record of disposal action that can be audited.

This material has been taken from the National Archives of Australia publication *DIRKS: A Strategic Approach to Managing Business Information* available online at <http://www.naa.gov.au>.