



NATIONAL ARCHIVES OF AUSTRALIA

# Digital Recordkeeping Self-Assessment Checklist

May 2004

© Commonwealth of Australia 2004

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the National Archives of Australia. Requests and inquiries concerning reproduction and rights should be directed to the Publications Manager, National Archives of Australia, PO Box 7425, Canberra Business Centre ACT 2610.

ISBN 1 920807 09 8

## 1 Introduction

The checklist in this document is a self-assessment tool to help Australian Government agencies manage their digital records effectively. It enables agencies to determine whether they have appropriate recordkeeping strategies, practices and systems for managing digital records, and to identify areas needing improvement. The checklist should be read and used in conjunction with the National Archives publication *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records*.

### Scope and audience

Commonwealth records in all formats must be properly managed to support business needs and meet accountability obligations. Digital records are subject to the same legislative requirements as records on paper or in any other format. Digital records include those created in a digital format (born digital) and those converted into a digital format (eg scanned documents).

The Digital Recordkeeping Guidelines provide comprehensive advice on managing digital records. This checklist helps agencies evaluate their digital recordkeeping capability in the context of their broader recordkeeping strategy.

Meeting the challenge of managing digital records requires a coordinated approach. Completing the checklist, reviewing the results and planning for the future should involve input from all sections of the organisation that have an interest in digital records, including:

- records and information management professionals
- information technology specialists
- web managers
- managers of business and e-business units.

The checklist can also be used as part of an internal audit program.

Agencies should work toward meeting all the requirements in the checklist. This will ensure that digital recordkeeping is an integrated part of the overall records and information management strategy.

## 2 Completing the checklist

The checklist covers 11 areas of digital recordkeeping discussed in the Digital Recordkeeping Guidelines. A key principle sets out the intended goal in each area, and each principle is supported by a number of indicators. To complete the checklist, agencies should assess whether or not each indicator is met. Methods of assessment may include:

- **Inspection** – physical examination of the system, facilities and/or business processes. In some cases, a qualified professional such as a database specialist, records manager, or IT security administrator should undertake the inspection. Inspections may be conducted by staff with specialist knowledge or by external professionals.

- **Documentation** – examination of records or other evidence that verify attributes relating to the system, facilities and/or business processes (eg policy statements, procedural documentation).
- **Interview** – discussions with personnel who have relevant skills or knowledge to make informed comments on the system, facilities and/or business processes.
- **Certification** – visual examination of authorisations that have been obtained as part of formal evaluation processes (eg certification by the Defence Signals Directorate under the Australasian Information Security Evaluation Program).

Agencies may choose to evaluate digital recordkeeping throughout the entire organisation. However the checklist will be most useful if applied at the level of business units or individual systems. Assessment may be conducted as part of a broader DIRKS analysis, particularly at Step D – Evaluation of existing systems. Following on with Step E will allow agencies to develop strategies to remedy any weaknesses that are identified.

Completing the checklist will require a range of skills and competencies. These include:

- an understanding of the organisation's recordkeeping requirements
- familiarity with business information systems and the technological environment
- knowledge of associated policies and procedures.

Where agencies do not have the necessary internal resources of time or expertise, they should engage consultants to undertake assessments on their behalf.

Agencies should aim to satisfy all relevant principles in the checklist. Satisfying all indicators under a principle suggests the principle is fully satisfied. Depending on the nature of the agency's recordkeeping systems, some indicators may not be relevant.

If relevant indicators cannot be satisfied, or are only partially satisfied, agencies should consider the ongoing risks in failing to satisfy the principle. All identified risks should be actively managed as part of the agency's business continuity and risk management programs, and associated recordkeeping decisions should be authorised by a senior manager. Further information about the management of recordkeeping risks can be found in Appendix 11 of the DIRKS Manual.

### **Further information**

Each section of the checklist refers to the corresponding section of *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records*.

The National Archives provides advice on digital recordkeeping at [www.naa.gov.au/recordkeeping/er/summary.html](http://www.naa.gov.au/recordkeeping/er/summary.html)

For further information contact the National Archives. Email [recordkeeping@naa.gov.au](mailto:recordkeeping@naa.gov.au) or phone (02) 6212 3610.

### **3 Digital recordkeeping framework**

#### **Key principle**

The agency has a comprehensive framework for digital recordkeeping, which is integrated into the total recordkeeping and information management strategy.

- a. The framework is supported by senior management recognition of digital records as corporate assets, and commitment to their effective management.
- b. The framework identifies all relevant legislative requirements, and outlines arrangements to ensure the requirements are met.
- c. The policies, procedures and guidelines developed as part of the framework cover all aspects of digital recordkeeping described in the Digital Recordkeeping Guidelines.
- d. Responsibility for digital recordkeeping is assigned to staff with appropriate expertise, knowledge and experience.
- e. Business information systems are designed and implemented with recordkeeping capability.
- f. Training and user education programs for record creators are an integral and ongoing component of the digital recordkeeping framework.
- g. The framework covers digital records that are owned by the Australian Government but are created or managed by external providers.

For more information, see Digital Recordkeeping Guidelines 3 – Digital recordkeeping framework.

### **4 Creating digital records**

#### **Key principle**

Digital records are created as evidence of business activity.

- a. The legal and business requirements to create digital records have been identified.
- b. Digital records are captured into recordkeeping systems.
- c. Systems that manage digital records have recordkeeping capability.
- d. Business information systems that do not have recordkeeping capability are not used to capture or manage digital records.

For more information, see Digital Recordkeeping Guidelines 4 – Creating digital records.

## **5 Creating information about digital records**

### **Key principle**

Metadata about digital records is captured and maintained.

- a. Metadata is captured when records are created and during their management.
- b. Creation and capture of metadata occurs as a normal part of business and recordkeeping operations.
- c. Policies and practices ensure that standardised metadata is created and maintained.
- d. The *Recordkeeping Metadata Standard for Commonwealth Agencies* is implemented for digital records.
- e. The *AGLS Metadata Standard, AS 5044* is implemented to facilitate retrieval of online content.
- f. Classification tools have been developed to assist with titling, indexing and retrieving digital records.

For more information, see Digital Recordkeeping Guidelines 5 – Creating information about digital records.

## **6 Determining how long to keep digital records**

### **Key principle**

Digital records are retained, and remain accessible, until no longer required for any purpose.

- a. We have determined how long to keep digital records, to meet legal, business and community needs.
- b. The agency has a records disposal authority to cover its core business records in any format including digital.

For more information, see Digital Recordkeeping Guidelines 6 – Determining how long to keep digital records.

## **7 Storing digital records**

### **Key principle**

Digital records are stored in appropriate conditions to ensure their ongoing accessibility.

- a. Digital records are stored on appropriate devices based on business needs, preservation requirements and costs.
- b. Digital storage devices are subject to regular integrity checks.
- c. Digital storage media are monitored and periodically refreshed to prevent data loss through media degradation.
- d. Digital storage media are stored in accordance with the *Standard for the Physical Storage of Commonwealth Records*.

For more information, see Digital Recordkeeping Guidelines 7 – Storing digital records.

## **8 Securing digital records**

### **Key principle**

Effective security and authentication controls ensure digital records are safe from intentional or unintentional damage and unauthorised tampering.

- a. Security of digital records is maintained in accordance with the *Commonwealth Protective Security Manual* and *Australian Government Information Technology Security Manual* (ACSI 33).
- b. Procedures and practices control the assignment of access permissions to users, and the allocation of protective markings to digital records.
- c. Procedures are in place to identify and respond to incidents or attempted security breaches of systems that create or store digital records.
- d. Systems and practices prevent unauthorised alteration of digital records, and ensure their authenticity.
- e. Procedures ensure that security and authentication mechanisms do not inadvertently make digital records of archival value inaccessible in the long term.

For more information, see Digital Recordkeeping Guidelines 8 – Securing digital records.

## **9 Business continuity planning for digital records**

### **Key principle**

The agency has an adequate business continuity plan for digital records, to prevent, prepare for and recover from a disaster.

- a. Procedures and practices are in place to minimise the risk of digital records being lost or damaged as a result of disaster.
- b. Vital records and digital records of archival value are recognised as high priority in business continuity plans.
- c. Business continuity plans include priority recovery and restoration procedures for digital records.

For more information, see Digital Recordkeeping Guidelines 9 – Business continuity planning for digital records.

## **10 Preserving digital records for the long term**

### **Key principle**

The agency has a strategy to preserve digital records and ensure they are accessible for as long as required.

- a. An approach to preserving digital records has been selected based on business needs, how well the approach will serve them, and the agency's capacity to support the approach (financially and technically) in the long term.
- b. Preservation strategies are implemented and proactively promulgated to relevant staff.
- c. Digital records and associated metadata are usable and accessible with current technology.

For more information, see Digital Recordkeeping Guidelines 10 – Preserving digital records for the long term.

## **11 Providing access to digital records**

### **Key principle**

The agency can provide secure access to digital records in its custody, in accordance with legislative requirements.

- a. Long-term digital records and their metadata remain accessible and usable.
- b. Infrastructure is in place to meet public and official demands for access to digital records.
- c. Mechanisms are in place to supervise access and to protect digital records from unauthorised alteration.

For more information, see Digital Recordkeeping Guidelines 11 – Providing access to digital records.

## **12 Disposing of digital records**

### **Key principle**

Digital records are disposed of lawfully and according to the *Archives Act 1983*.

- a. Disposal of digital records is in accordance with an appropriate general disposal authority, records disposal authority, a normal administrative procedure that the Archives does not disapprove of, or other legislative requirement.
- b. Digital records of archival value are transferred to the National Archives when they are no longer required for business purposes.
- c. Where digital records are retained permanently within the agency, preservation strategies are capable of retaining the integrity and functionality of the records.
- d. All mandatory recordkeeping metadata is transferred to the National Archives when digital records reach their final disposition status.
- e. When digital records are authorised for destruction, appropriate methods of destruction are used and all extant copies are destroyed in such a way that they cannot be reconstructed.
- f. When digital records are transferred between agencies, the records and associated metadata are transferred in data formats that are accessible and functional for the receiving agency, and adequate system documentation is included.

For more information, see Digital Recordkeeping Guidelines 12 – Disposing of digital records.

### **13 Managing some common types of digital records**

#### **Key principle**

Particular types of digital records (such as electronic messages, web-based records, records subject to online security processes) are managed in accordance with their specialised recordkeeping requirements.

- a. Electronic messages are kept in accordance with the Digital Recordkeeping Guidelines.
- b. Web-based records are kept in accordance with the Archiving Web Resources Policy and Guidelines.
- c. Records subject to online security processes, such as encryption, are kept in accordance with *Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption*.
- d. Records in business information systems are kept in accordance with the Digital Recordkeeping Guidelines.
- e. Personnel with responsibility for digital recordkeeping monitor emerging technologies to ensure any resulting digital records are managed appropriately.

For more information, see Digital Recordkeeping Guidelines 13 – Managing some common types of digital records.