NATIONAL ARCHIVES OF AUSTRALIA

Digital Recordkeeping

Guidelines for Creating, Managing and Preserving Digital Records

May 2004

ISBN 1 920807 08 X

EXECUTIVE SUMMARY

Australian Government agencies create many records in digital format. Digital records include word-processed documents, emails, databases and images.

Australian Government agencies are responsible for creating, managing and preserving their digital records for as long as they are required. Agencies should develop an integrated and comprehensive framework for digital recordkeeping.

Digital records are created as evidence of business activity and captured into recordkeeping systems along with metadata that describes their content, structure and context.

Digital records must be managed to remain accessible for as long as they are required. They can be accessed through legislation on archives, freedom of information and privacy. Digital records should be stored in accordance with the frequency of the need to refer to them. Because digital records can be easily modified, their security is very important. Agencies should plan for disasters – loss of digital records can be crippling.

Given the rapid obsolescence of digital technology, agencies should plan for the long-term preservation of digital records. Digital records that are to be retained indefinitely by the agency require preservation to ensure their ongoing accessibility.

Digital records of temporary value must be destroyed securely and in such a way that they cannot be reconstructed. Digital records of archival value should be transferred to the National Archives when immediate business needs have ceased.

CONTENTS

1. INTRODUCTION

All Australian Government agencies produce digital records. With the advent of new technology and greater levels of technological dependence within agencies, the proportion of Commonwealth records being created in digital format is increasing exponentially. Electronic recordkeeping and document management systems enable agencies to store digital records in their original digital format.

The Australian National Audit Office's (ANAO) audit reports on recordkeeping (May 2002 and September 2003) concluded that agencies were having difficulty meeting their recordkeeping obligations in the electronic business environment. The Australian Public Service Commission's (APSC) *State of the Service Report*, issued in October 2002, also revealed a lack of understanding and a high degree of confusion among employees regarding their responsibilities and ability to manage digital records.

The National Archives' own survey in late 2002 of the state of recordkeeping in the Australian Government supported the findings of the ANAO and APSC. Agency responses to the survey requested that the National Archives provide further guidance in the management of digital records. These guidelines have been developed in response to that request.

1.1 Purpose

This publication provides comprehensive guidance to Australian Government agencies on creating, managing and preserving digital records. Digital records must be actively managed in order to ensure they are available and usable for as long as required to support accountability, good business and the expectations of the public.

The guidelines contain advice on:

- the importance of managing digital records and how to manage them in an integrated way;
- creating and capturing digital records, and associated metadata, into recordkeeping systems;
- storing and securing digital records, including planning for disasters;
- preserving digital records for as long as they are required, including an overview of the National Archives approach;
- providing access to digital records; and
- disposing of digital records in an approved manner.

The guidelines also provide specific advice for some common types of digital records, such as electronic messages and web-based records.

We recommend that the strategies described in these guidelines be implemented as a matter of sound business practice.

The Digital Recordkeeping Guidelines form part of the *e-permanence* suite of products produced by the National Archives to assist in the management of government information.

1.2 Scope

The advice contained in these guidelines applies to all digital records created by Australian Government agencies as evidence of business activity. Digital records include all records that are created in a digital format (born digital), or have since been converted into a digital format.

These guidelines draw upon recordkeeping requirements for the management of digital records that are set out in various legislative instruments and best practice standards.

These guidelines replace the National Archives publications *Managing Electronic Records: A Shared Responsibility*, *Keeping Electronic Records: Policy for Electronic Recordkeeping in the Commonwealth Government* and *Managing Electronic Messages as Records*.

1.3 Audience

These guidelines should be used by all Australian Government agencies to ensure that their digital records are managed appropriately. They are relevant to all agency staff members with responsibility for managing digital records.

There are two distinct audiences for these guidelines:

- those with responsibility for managing information technology (IT) and communications, including e-business and websites; and
- those with responsibility for managing records, information and knowledge.

These guidelines contain detail that is required to meet the information needs of both audiences. Some sections may include information that is considered unnecessary by the members of one audience. For instance, information about the IT requirements of digital records has been included for the information of records, information and knowledge managers. Information about the management of digital records has been provided to assist the IT audience.

A glossary has been provided at Appendix A to define terminology that may be unfamiliar.

1.4 Related products

1.4.1 *e-permanence* products

The National Archives' *e-permanence* suite of recordkeeping products provides much advice that is relevant to digital records. Rather than duplicating that advice, readers are referred to other products at the relevant point in this publication. At each such point, the relevance of the other *e-permanence* products to digital recordkeeping is explained.

1.4.2 Digital recordkeeping checklist

To complement the guidelines, the National Archives has developed the *Digital Recordkeeping Self-Assessment Checklist.* The checklist has been designed to enable Australian Government agencies to evaluate their management of digital records.

1.5 Structure

These guidelines are arranged in a series of short sections. Each section provides advice on a particular aspect of digital recordkeeping.

We expect that users of these guidelines will 'dip in and out', reading sections individually in order to obtain specific advice. We encourage readers employing this strategy, however, to read the following sections carefully:

- 2 – The importance of digital records
- 3 – Digital recordkeeping framework

Each section is prefaced with a series of key points. The key points summarise the most important issues covered in the section. The subsection elaborating each key point is identified, so readers can navigate to issues of interest.

At the end of each section is a summary of the actions that may be taken to put the advice into practice.

2. THE IMPORTANCE OF DIGITAL RECORDS

Key points

- Digital records are evidence of business conducted by an organisation (2.1).
- Digital records must be managed to support the efficient conduct of business and to meet requirements for accountability, community and best practice (2.2.1 and 2.2.2).
- The nature of digital technology presents unique challenges for the management of digital records (2.2.3).
- Australian Government agencies are responsible for creating, managing and preserving their digital records for as long as they are required (2.3.1).
- The National Archives provides advice, and sets standards, to help Australian Government agencies manage their digital records appropriately (2.3.2).

2.1 What are digital records?

Records are evidence of business conducted by an organisation. Records can be in any form, including digital.

Digital records are records created, communicated and maintained by means of computer technology. They may be 'born digital' (created using computer technology). Or they may have been converted into digital form from their original format (eg scans of paper documents).

Organisations create and store digital records in a variety of ways. Common types of digital records include word-processed documents, spreadsheets, multimedia presentations, email, websites and online transactions.

However, digital records can be found in many systems throughout an organisation – including databases and business information systems, shared folders and hard drives.

The following list is not exhaustive, but highlights the range of digital records covered by these guidelines.

Documents created using office applications:

- word-processed documents
- spreadsheets
- presentations
- desktop-published documents

Records generated by business information systems:

- databases
- geospatial data systems
- human resources systems
- financial systems
- workflow systems
- client management systems
- customer relationship management systems

Records in online and web-based environments:

- intranets
- extranets
- public websites
- records of online transactions

Electronic messages from communication systems:

- email
- SMS (short messaging services)
- MMS (multimedia messaging services)
- EDI (electronic data interchange)
- electronic document exchange (electronic fax)
- voice mail
- instant messaging

- systems developed in-house
- content management systems
- EMS (enhanced messaging services)
- multimedia communications (eg video conferencing and teleconferencing)

These records are subject to the same legal requirements as records on paper or any other format.

To be of value as evidence, a digital record must possess content, context and structure. (These and other recordkeeping terms are defined in the glossary at Appendix A.)

This means that a digital record:

- has information content that is, and continues to be, an accurate reflection of what occurred at a particular time;
- can be placed in context so that the circumstances of its creation and use can be understood in conjunction with its information content; and
- can be reconstructed electronically when required so that each component part is brought together as a whole and presented in an intelligible way.

The best way to preserve the content, context and structure of a record, is to manage it within a recordkeeping system.

Many agencies use specialised software applications (known as electronic records management systems or ERMS) to manage digital records. A recordkeeping system is not just a piece of software. It is a framework for the capture, maintenance and accessibility of records over time.

A business information system is not necessarily a recordkeeping system. Recordkeeping functionality can be built into business information systems (see 4 – Creating digital records).

2.2 Why manage digital records?

Digital records created by Australian Government agencies in the course of their business activities are Commonwealth records subject to the provisions of the *Archives Act 1983*.

Digital records must be managed for the same reasons records in other formats need to be managed. Records allow government business to be conducted efficiently and effectively. There are accountability and legislative obligations that government agencies must meet, and community expectations concerning the documentation and transparency of government actions. Further, special challenges, such as technological obsolescence and media degradation, make it imperative for digital records to be carefully managed.

2.2.1 Efficient and effective business

Australian Government agencies routinely create and accumulate records as they undertake their business. Those records serve as evidence of a business transaction, the players involved in the transaction and its outcome.

Inadequate records and poor recordkeeping practices can contribute to accountability failures and inefficient business performance. Effective recordkeeping strategies can lead to many business benefits.

Good records enable business planning. Records provide a comprehensive view of an organisation's activities. This allows decision-makers to see opportunities for new business or to streamline existing processes.

Capturing records into corporate recordkeeping systems means they can be found when required. This helps an organisation meet its business needs and accountability requirements. Staff can also identify and retrieve the authoritative version of a record where multiple versions exist.

Records preserve an agency's history and form its corporate memory. Information about previous decisions and actions can improve service quality and effectiveness. Timely access to relevant data allows action officers to make decisions and do better business.

Greater control over information assets is another key benefit of recordkeeping. This includes reduced costs through timely disposal of records. Conversely, vital records are maintained for as long as they are required. Access to secure or sensitive records can be restricted to authorised personnel.

Successful organisations assign responsibility for different aspects of recordkeeping at appropriate levels in the organisation. Good recordkeeping supports good business.

The Auditor-General has noted the value of good recordkeeping to Australian Government agencies:

> Up-to-date, accessible, relevant and accurate records can ensure that decisions made by an agency are consistent, based on accurate information; are cost-effective; engender a sense of ownership of decisions throughout the agency; and place the agency in a considerably better position to justify to Parliament and the public any decisions made.
>
> Loss of corporate knowledge has been a significant issue for the public sector in recent years where … we have seen an enormous drain on the retained knowledge of the APS through the departure of many experienced individuals. The creation and maintenance of suitable records can alleviate this problem to some extent, particularly in relation to decision-making.[1]

2.2.2 Accountability, community expectations and best practice

Australian Government agencies have legal obligations to manage their digital records.

- *Archives Act 1983* sets the legal framework for disposal, transfer, custody and access to Commonwealth records.
- *Freedom of Information Act 1982* provides for access to records that are not otherwise publicly available.
- *Privacy Act 1988* aims to ensure information about individuals is created and kept for the right reasons and that access is only given in specified circumstances.
- *Evidence Act 1995* sets the criteria by which records are admissible as evidence in courts, regardless of format.

[1] PJ Barrett, Auditor-General for Australia, 'External scrutiny of government decisions – trends and lessons learnt', Institute of Public Administration of Australia, ACT Division, half-day seminar, 31 May 2002, published online at www.anao.gov.au/WebSite.nsf/Publications/4A256AE90015F69B4A256BCD007C8E50

- *Electronic Transactions Act 1999* covers aspects of the retention and maintenance of transactions undertaken in the electronic environment, and obligations to ensure their integrity and accessibility over time.

Records are a major support for the accountability and transparency of government. The Auditor-General has stressed that records are critical for good governance as follows:

> Records are an indispensable element of transparency, and thus of accountability, both within an organisation and externally. Records are consulted as proof of activity by senior managers, auditors, members of the public or by anyone inquiring into a decision, a process or the performance of an organisation or an individual.[2]

Australian Government agencies account for their actions, and the expenditure of resources provided by parliament on behalf of the community, by keeping records of their actions. Records also support the rule of law, protect the rights and entitlements of individuals, are evidence of interactions between the people of Australia and their elected governments, and preserve the national memory.

The National Archives of Australia endorses the *Australian Standard for Records Management*, AS ISO 15489 as a source of best practice recordkeeping advice for Australian Government agencies. The Archives also produces standards, policies and guidelines to assist agencies in meeting requirements for accountability and best practice.[3]

2.2.3 Challenges associated with digital records

Managing digital records involves the following unique challenges:

- Digital technology evolves at a rapid rate. The software and hardware used by an agency to create digital records tends to be short-lived, quickly replaced by upgrades or improvements. Because of this hardware and software obsolescence, digital records can quickly reach a point where they cannot be read or understood. Yet, in order to meet legislative obligations, records must remain accessible for as long as they are required.
- The general manipulability of digital records means that they can quickly and easily be updated, deleted or altered. However, digital records are evidence of business activity and must be managed securely to prevent unauthorised modification.
- Metadata can be intrinsically linked to a digital record, or it may be contained within the systems used to generate or store the records. Capturing and maintaining metadata, including technical specifications, is necessary in order to ensure the preservation of digital records and their continued accessibility over time.

[2] PJ Barrett, Auditor-General for Australia, 'Achieving better practice corporate governance in the public sector', International Quality and Productivity Centre seminar, 26 June 2002, published online at www.anao.gov.au/WebSite.nsf/Publications/4A256AE90015F69BCA256BE4000827D3)

[3] See Recordkeeping Overview at www.naa.gov.au/recordkeeping/overview/summary.html.

With more government business being conducted electronically, and a push for providing government services online, the importance of managing digital records effectively and appropriately has never been greater.

2.3 Who is responsible for managing digital records?

Both the National Archives and Australian Government agencies have roles to play in managing Commonwealth records in digital form.

2.3.1 The role of Australian Government agencies

Australian Government agencies are responsible for:

- managing all digital records for which the organisation is responsible, (including those documenting outsourced functions or in the possession of outsource providers), in an integrated manner in accordance with their importance as corporate assets (3 – Digital recordkeeping framework);
- creating full and accurate digital records of business transactions and capturing them into systems with recordkeeping functionality (4 – Creating digital records);
- creating and keeping metadata about digital records (5 – Creating information about digital records);
- identifying legal, business and community requirements to retain digital records (6 – Determining how long to keep digital records);
- storing digital records in appropriate conditions to ensure their continuing accessibility (7 – Storing digital records);
- providing effective security and authentication controls to ensure digital records are safe from malicious damage and unauthorised tampering (8 – Securing digital records);
- implementing adequate business continuity plans for digital records (9 – Business continuity planning for digital records);
- maintaining digital records in accessible formats for as long as they are required (10 – Preserving digital records for the long term);
- providing access to digital records (11 – Providing access to digital records);
- securely destroying digital records in accordance with legal requirements and so that they cannot be reconstructed (12 – Disposing of digital records);
- transferring digital records of archival value, and information about them, to the National Archives (12 – Disposing of digital records); and
- managing digital records in accordance with their specialised recordkeeping requirements (13 – Managing some common types of digital records).

2.3.2 The role of the National Archives

The National Archives will assist Australian Government agencies by:

- providing advice and setting standards on creating, managing and preserving digital records for as long as they are required;
- considering whether nominated groups of digital records have archival value;
- issuing authorisation for the disposal of digital records when they are no longer required to meet legal, business and community needs;
- taking digital records of archival value into custody and preserving them; and
- providing public access to digital records.

3. DIGITAL RECORDKEEPING FRAMEWORK

Key points

- Australian Government agencies should develop an integrated and comprehensive framework for digital recordkeeping (3.1).
- Senior management commitment to digital records as corporate assets is essential to the success of a digital recordkeeping framework (3.2).
- A digital recordkeeping framework must ensure compliance with all relevant legislative requirements (3.3).
- The digital recordkeeping framework will include policies, procedures and guidelines that set out the agency's approach to digital recordkeeping (3.4).
- Responsibility for digital recordkeeping should be assigned to staff with appropriate skills, knowledge and experience (3.5).
- Agencies should design and implement systems with recordkeeping capability (3.6).
- Records creators should be educated in their digital recordkeeping responsibilities (3.7).
- The digital recordkeeping framework should cover records that are owned by the Australian Government but created by outsource providers (3.8).

3.1 Integrated and comprehensive approach

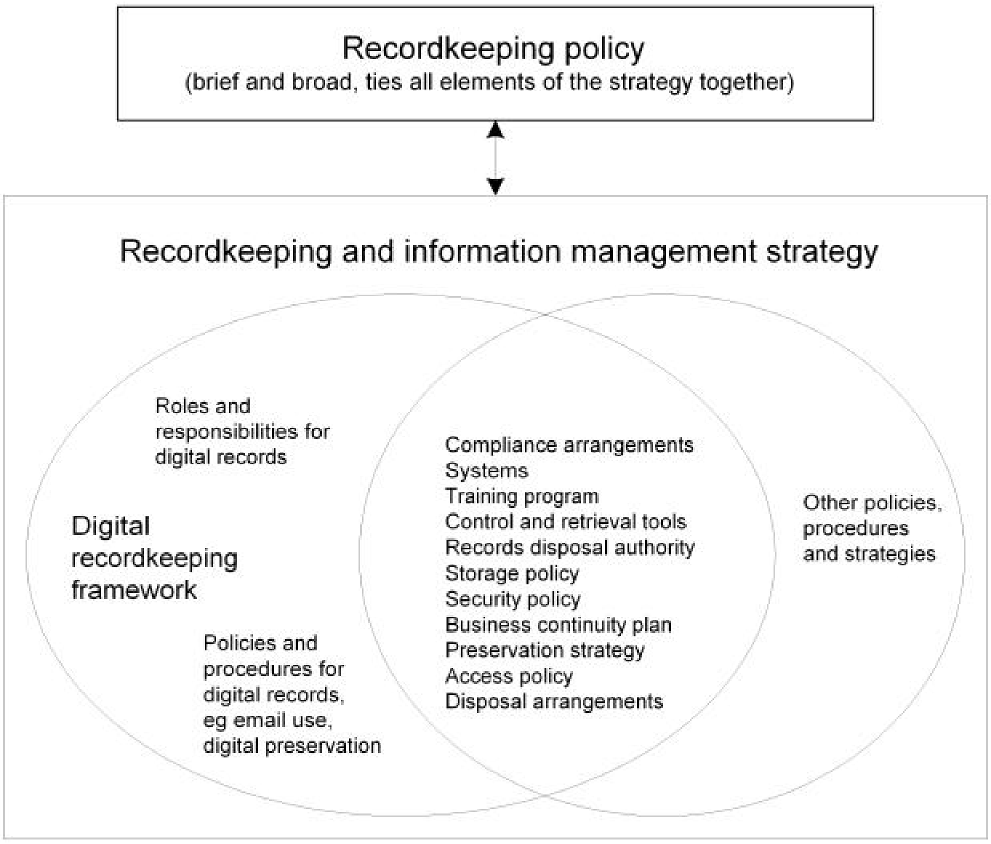
Australian Government agencies should establish a digital recordkeeping framework for the management of their digital records. The framework should be integrated into the total recordkeeping and information management strategy for the organisation.

The National Archives publication *Developing a Policy: How to Develop a Recordkeeping Policy* provides guidance on developing an organisation-wide recordkeeping policy. This policy relates to all agency records, regardless of format. A digital recordkeeping framework covers a subset of an organisation's records (ie its digital records) and forms an integral part of the recordkeeping policy.

A digital recordkeeping framework incorporates arrangements for compliance with relevant standards and legislation (section 3.3), formal written policies, procedures and guidelines (section 3.4), identification of key roles and responsibilities (section 3.5), design and implementation of recordkeeping systems (section 3.6) and user education and training (section 3.7).[4] The framework should cover all aspects of digital recordkeeping discussed in these guidelines.

[4] This notion of a digital recordkeeping framework has been adapted from content in a forthcoming publication of the State Records Office of Western Australia, *Electronic Records Handbook*, Perth.

Figure 1: Digital recordkeeping framework


Recordkeeping policy
(brief and broad, ties all elements of the strategy together)
Recordkeeping and information management strategy
Roles and responsibilities for digital records
Digital recordkeeping framework
Policies and procedures for digital records, eg email use, digital preservation
Compliance arrangements
Systems
Training program
Control and retrieval tools
Records disposal authority
Storage policy
Security policy
Business continuity plan
Preservation strategy
Access policy
Disposal arrangements
Other policies, procedures and strategies

Agencies are encouraged to pursue a holistic approach to recordkeeping that is based on legal and business requirements, rather than record format. A digital recordkeeping framework allows the management of digital records to be integrated and consistent with the management of records in other formats.

3.2 Senior management support

Senior management recognition of digital records as corporate assets, and commitment to their effective management, is essential to the success of an organisation's digital recordkeeping framework. Appropriate resources must be provided to develop and implement a sustainable organisation-wide framework.

The scope and complexity of the framework an organisation develops will depend on the organisation's size, the complexity and riskiness of its business, resource availability, and the volume and type of digital records created.

3.3 Legislation and standards

It is vital that a digital recordkeeping framework ensures compliance with all relevant legislative requirements.

The *Archives Act 1983* requires National Archives approval for the disposal of Commonwealth records and allows for the provision of access to Commonwealth records. The *Freedom of Information Act 1982*, *Privacy Act 1988*, *Evidence Act 1995* and *Electronic Transactions Act 1999* also place accessibility and evidential obligations on Australian Government agencies.

In addition to legislation that all Australian Government agencies must abide by, agencies may need to abide by requirements contained in legislation specific to their business, in particular enabling legislation. Agencies that have already systematically identified their recordkeeping requirements, in accordance with *DIRKS: A Strategic Approach to Managing Business Information*, will be able to make use of that analysis.

Agencies should also consider relevant standards. The National Archives has endorsed the *Australian Standard for Records Management*, AS ISO 15489 for best practice guidance on recordkeeping for Australian Government agencies. Agencies are encouraged to adopt many of the practices set out in the standard by using the DIRKS methodology (see 3.6).

There may also be relevant information technology (IT) standards for agencies to use when developing digital recordkeeping solutions, eg data format standards and protocols like XML (eXtensible Markup Language), SGML (Standard Generalised Markup Language) and X.400 (an electronic message interchange protocol).

3.4 Policies, procedures and guidelines

Policies and procedures for managing digital records are an important element of a digital recordkeeping framework. Policies define the organisation's approach to managing digital records and provide the necessary senior management authority for the implementation of the framework. Procedures outline how the policies will be implemented and provide clear instructions for their practical application. Where necessary, policies and procedures can be supplemented by guidelines to provide additional clarification and direction.

The policies and procedures developed as part of a digital recordkeeping framework should cover all aspects of digital recordkeeping dealt with in these guidelines.

Agencies should use the *Australian Standard for Records Management*, AS ISO 15489 as a best practice guide when developing policies and procedures for managing digital records.

Policies, procedures and guidelines should be developed to suit the organisation's size, complexity, corporate culture and structure. A small agency, for instance, may have a single policy covering the management of all digital records. Larger agencies may have multiple policies covering specific areas of digital recordkeeping, such as electronic messages, preservation of digital records, web-based digital records and digital records security.

The organisation's IT environment should also be considered – for example, how many systems currently exist, potential for integration, what types of records are generated (eg data sets, spreadsheets, messages, images), whether staff work from the hard drive, shared folders or through an interface to multiple repositories. Considering these issues will help agencies choose a records management solution, and develop and implement effective policies and procedures.

Some issues that may be covered by policies, procedures and guidelines are:

- setting up and managing the agency's electronic workspace;
- developing and implementing document and directory naming conventions;
- responsibilities for particular staff members or sections;
- processes for capturing digital records into corporate recordkeeping systems;
- conditions of use for the electronic messaging system, including private use by staff;

- implementing access controls and security measures;
- coordinating document storage and disposal; and
- aligning IT management procedures with best practice digital recordkeeping.

3.5 Roles and responsibilities

Chief Executive Officers are ultimately responsible for the management of records within their agencies. In most organisations, this responsibility will be delegated to an appropriate senior position, such as the Chief Information Officer (CIO).

The senior officer with this delegation should be familiar with the agency's IT and communication infrastructure. They should also understand the organisation's recordkeeping requirements, the nature of its records and how to ensure their integrity over time. Records created on behalf of the organisation by outsource providers remain the responsibility of the agency and are included in the senior officer's responsibilities (see 3.8).

An important goal for the officer in this position is to promote collaboration between information management, records management, e-business, website management, IT and line of business staff. The skills, knowledge and experience of all areas are required for agencies to meet the challenges of digital records. As such, responsibility for digital records is shared across the organisation. In particular, records managers play an important role in the development of recordkeeping and business information systems and in ensuring that records are created and maintained appropriately.

Responsibility for identifying corporate records created in the course of an agency's business activity is the responsibility of all agency staff. Staff may also be required to add metadata to records they use and create (see 5 – Creating information about digital records). With adequate training (see 3.7) and clear and precise policies, procedures and guidelines (see 3.4), staff should feel confident to identify records that need to be incorporated into the agency's recordkeeping systems.

3.6 Systems design

The recordkeeping practices set out in the policies, procedures and guidelines need to be supported by systems that are capable of keeping records. A digital recordkeeping framework should identify recordkeeping functionality in existing systems or recommend the design and implementation of new systems. These systems should be endorsed as corporate recordkeeping systems and their use incorporated into business processes.

Achieving better digital recordkeeping through systems design has many advantages. These include more reliable metadata captured in association with digital records, more comprehensive and systematic capture of digital records, and greater security and control over access to digital records.

Innovative technical solutions can reduce the need for conscious employee involvement in the recordkeeping process, reduce reliance on staff making records selection decisions and improve overall workflow by streamlining records capture.

Some software applications lend themselves to built-in recordkeeping functionality. For example, finance and human resources systems already support a high degree of control, such as audit trails and user access logs. In many cases, automated or semi-automated capture of recordkeeping metadata may be possible with minimal customisation.

Other applications will require the user to manually capture a record into a separate recordkeeping system. Workflow systems and procedures that incorporate recordkeeping practices can seamlessly support core business processes.

Please note that storing digital records on structured network drives is not a substitute for a controlled recordkeeping system. However, improving the way files are stored on private drives and shared directories will assist the overall management of corporate information. For example, establishing a classification scheme and naming conventions can create a semi-structured environment for digital objects. This can be a useful interim measure, until recordkeeping systems are developed.

3.6.1 Tools for systems design

The National Archives is developing generic specifications for records and information management systems for agencies wishing to purchase, or build, systems with recordkeeping capability. This document will specify the functionality that systems should have in order to keep records.

The DIRKS Manual can help agencies design and implement systems to manage records and information. It is based on the systems development life cycle, and reflects the best practice approach to recordkeeping set out in the *Australian Standard for Records Management*, AS ISO 15489. This methodology provides a framework for addressing a range of information management needs. It is flexible, scalable, and particularly useful for meeting the challenges of managing digital records.

Pathways through DIRKS are identified at the end of each section of these guidelines. Each pathway will assist users to implement the advice contained in that section.

3.7 User education and training

Formal policies, procedures and guidelines to codify an agency's approach to digital recordkeeping provide a solid foundation for managing digital records. But the effectiveness of such a strategy will depend on the extent to which endorsed practices are actively adopted throughout an agency.

It is necessary to invest in staff education and training to encourage widespread adoption of digital recordkeeping. Training and user education programs must be recognised as an integral, vital and ongoing component of an agency's digital recordkeeping framework.

All agency staff, regardless of level, should be made aware of the legal requirements for Australian Government agencies to create and maintain records, and should be educated about the digital recordkeeping policies adopted by the agency. Staff with responsibility for digital recordkeeping in an agency should be proactive in developing and delivering training to familiarise staff with the appropriate procedures for creating, managing and preserving digital records.

Key topics that staff training programs should cover include:

- importance of records;
- which records are digital records;
- staff responsibilities;
- practices for capturing digital records into the agency's recordkeeping system;

- security issues for digital records; and
- capture of appropriate metadata.

To assist in teaching agency staff about their recordkeeping responsibilities, the National Archives has developed the *Keep the Knowledge – Make a Record!* training package. Designed specifically for agency trainers to use in educating creators of records, this kit explains what records are, what kinds of records employees should make and keep, and when they can access and dispose of records.

To ensure that agency staff are aware of their obligations and that agencies create and maintain full and accurate digital records, active and sustained promotion of the importance of keeping digital records is essential. Including digital recordkeeping training in induction programs for new staff is central to the continued effectiveness of an agency's digital records education and communication strategy.

3.8 Records created outside agency systems

The continuing trend within the Australian Government of using external providers for government business activities raises a number of challenges for government accountability.

Records relating to agency functions must be created, managed and disposed of in an accountable manner, even if the agency does not directly create, manage or dispose of them.

Contractual arrangements with external providers should:

- explain that records remain the property of the Australian Government;
- ensure the provider has the technical capability, for the duration of the contract, to manage digital records and enable their viewing as required;
- verify that the provider's systems will be compatible with those of the agency for the duration of the contract, in order to facilitate transfer of records back to the agency at its conclusion;
- specify that business continuity strategies are in place, including system backup procedures;
- provide for agency access to, and retrieval of, records and provide for public access to records under the *Archives Act 1983*, *Privacy Act 1988* or *Freedom of Information Act 1982*;
- facilitate sentencing and disposal of records, including effective destruction where required; and
- specify how the provider can ensure the level of security required to safeguard the records.

These provisions will ensure that external providers can be held accountable for their actions, and enable agencies to meet their government and public obligations.

Similar issues may arise where agencies exchange data or share integrated systems. Ownership and responsibility should be agreed, to determine who will capture and keep these records. Clear procedures and guidelines will ensure that vital records are retained.

The digital recordkeeping framework should take into account digital records created by external providers, or within shared systems. These records should be managed in accordance with agency policies.

For further advice on the recordkeeping issues involved in an outsourcing arrangement, see *General Disposal Authority 25 – Records Issues for Outsourcing*.

Where to from here?

Evaluate your current digital recordkeeping framework using the Digital Recordkeeping Checklist, Section 3.

Develop a digital recordkeeping framework according to the advice in this section. The following *e-permanence* products will assist:

- *How to Develop a Recordkeeping Policy*
- generic specifications for records and information management systems (forthcoming)
- *DIRKS: A Strategic Approach to Managing Business Information* (see below for relevant pathway)
- *Keep the Knowledge – Make a Record!*
- *General Disposal Authority 25 – Records Issues for Outsourcing*

Pathway through DIRKS

- Use Step A to investigate the role of your organisation, its structure and business, the regulatory and sociopolitical environment, and major factors that affect recordkeeping practices.
- Use Step E to develop policies, procedures and training strategies for recordkeeping.
- Use Step F to convert those strategies and tactics into a blueprint for a digital recordkeeping framework. This includes establishing policies, assigning responsibilities, redesigning work processes, and developing specifications for recordkeeping systems.

4. CREATING DIGITAL RECORDS

Key points

- Digital records are created as evidence of business activity (4.1).
- Digital records should be captured into recordkeeping systems (4.2).
- Failing to capture digital records into recordkeeping systems puts an agency at risk of serious consequences (4.3).
- Business information systems may not have recordkeeping capability and should not be used to capture digital records (4.4).
- Australian Government agencies should implement and support systems with recordkeeping capability (4.5).

4.1 Identifying and creating digital records

Australian Government agencies must create records to document their activities. Those records should be captured and maintained in recordkeeping systems. This process applies equally to digital records as to records in other formats (see 2.1 – What are digital records?).

Australian Government agencies should investigate the records they need to create to properly document their business activity. *DIRKS: A Strategic Approach to Managing Business Information* outlines the process involved in identifying recordkeeping requirements (see the pathway through DIRKS at the end of this section). Agencies that have already systematically identified their recordkeeping requirements will be able to make use of that analysis.

To be of value as evidence, a digital record must possess content, structure and context, and should be managed within a recordkeeping system (see 2.1 – What are digital records?).

Responsibility for creating and capturing digital records into recordkeeping systems often rests with agency staff. Agency staff identify, create and capture digital records in the course of daily business. Emails sent and received are placed on file, word-processed documents are drafted, altered and finalised within an agency's electronic recordkeeping system, and forms or correspondence are scanned into electronic document management systems. User education and training is fundamental to the success of these processes (see 3.7 – User education and training).

Where workflow (or similar) systems capture and classify records automatically, staff can be less directly involved in recordkeeping processes. In this case, a sound analysis of business activity and recordkeeping requirements will ensure adequate records are created and captured.

An organisation's recordkeeping requirements will indicate the kinds of systems needed to support accountability in business processes. Where existing systems lack the necessary functionality, the National Archives has produced tools to help address the gaps (see 4.5).

4.2 Capturing digital records into recordkeeping systems

To support work processes, digital records should be captured into a corporate system that has recordkeeping capability (see 4.5). Capture is the process of lodging a document into a recordkeeping system and assigning metadata to describe the record and place it in context, so that the record can be managed over time.

Trends such as decentralisation, the increasing use of technology in administrative processes, and inadequate control over outsourcing arrangements have created challenges for the systematic creation and keeping of records. Conscious effort is required to ensure that records supporting business activities are created and captured in recordkeeping systems (see 3.8 – Records created outside agency systems).

The procedures and practices an agency establishes to capture its digital records will depend on the recordkeeping systems in use, the types of digital records generated and the specific recordkeeping requirements the agency must satisfy.

Each Australian Government agency produces numerous types of digital records during the course of its business activities. Any procedures developed to capture those records into agency recordkeeping systems will need to cover all common digital objects (eg word-processed documents and spreadsheets) while retaining a degree of flexibility to cater for non-standard data formats (eg vector graphics).

General rules may be established to cover the capture of common record types such as email, word-processed documents, spreadsheets or common agency-specific business records. However, developing appropriate approaches to capturing non-standard digital record types, such as specialised databases and other unique agency records, will require greater thought. The skills and experience of various staff, including information and records management professionals, information technology specialists and others may be needed (see 3.5 – Roles and responsibilities).

Agencies with electronic records management software should be able to store most digital records in their native format within the system.

Capture of digital records within a paper-based or hybrid recordkeeping system presents more difficulty and should be carefully considered by agencies. Two options, neither of which is ideal, are:

- assigning an appropriate record number to digital records within the system and then storing them separately (see 7 – Storing digital records)
- printing records such as email and word-processed documents and attaching them to the relevant hardcopy file.

Approaches such as these may provide a cost-effective interim procedure while a more comprehensive solution is being developed. Step E of the DIRKS methodology can help agencies determine recordkeeping strategies for capturing and managing digital records in paper-based or hybrid systems.

4.3 Consequences of failing to capture digital records

Documenting business transactions by creating records and capturing them into recordkeeping systems is a fundamental part of government accountability. Australian Government agencies that fail to adequately capture the digital records they create will lose valuable corporate memory and vital evidence of their business activities. Employees will be in breach of their recordkeeping obligations, as set out in the Australian Public Service Commission's *APS Values and Code of Conduct* and the *Public Service Act 1999* sections 10 and 13.

There are considerable risks for agencies failing to maintain their digital records within a properly controlled recordkeeping system environment – whether through poor information management strategies, lack of control over record creator practices or inadequate systems design. The risks include:

- uncontrolled accumulation of ephemeral records and information
- inadvertent destruction of vital records and information
- unauthorised tampering with classified records and sensitive information
- lack of systems documentation and associated metadata.

In turn, these can place a system at risk of:

- paralysis or interference in accessing information
- costs associated with the purchase of unnecessary additional storage
- inability to migrate records from poorly documented systems
- increased risk of wholesale, unsystematic and possibly illegal destruction
- loss of valuable business and archival records
- increased risk of security breaches
- unauthorised alteration or deletion of records
- unnecessary delays, or breakdowns, in the business process
- lack of public accountability.

4.4 Business information systems not designed to keep records

A business information system is designed to support a specific business process – for example, case management systems, geospatial data systems, finance or human resource systems, call centre systems or systems that support e-business and online transactions. They are usually transaction-based systems. As such, they rely heavily on system logs (eg audit trails) to track changes to data and attempts to access their contents. Requirements for keeping and managing system logs are stipulated in the Defence Signals Directorate publication *Australian Government Information Technology Security Manual* (ACSI 33) (also see 8 – Securing digital records).

Not all business information systems are designed to act as recordkeeping systems. Many are designed to support current business needs for information but have only limited ability, if any, to keep records of the business transactions they carry out. These systems generate records, but do not have the capacity to manage those records. This can place agencies at significant risk.

Business information systems that do possess some form of built-in recordkeeping functionality may lack sufficient business context to be used as evidence or be incapable of capturing and retaining records for the required periods of time.

If business information systems have insufficient recordkeeping functionality, they will retain little or no evidence of the transactions performed. This lack of evidence represents a loss of corporate memory. Lost corporate memory can result in an agency being unable to satisfy its accountability requirements or conduct its business. In the long term, loss of government records means a loss of national cultural heritage.

The National Archives has produced a range of tools to help agencies to design or select business information systems with recordkeeping functionality (see 4.5).

4.5 Recordkeeping systems

Recordkeeping systems are specifically designed to capture evidence of business transactions. They are distinguished from business information systems by their ability to manage the content and structure of records, provide access to them over time, and maintain linkages between records and the activities they document (context).

Recordkeeping systems can be electronic or paper-based. Many agencies have a combination (hybrid) system of electronic and paper.

Electronic recordkeeping systems present the best method for maintaining digital records over time, as they provide digital records with the necessary context and safeguards to assist in their long-term preservation.

There are many information management solutions available on the market, such as EDMS (electronic document management systems), content management systems and workflow systems. These products support information-based business processes. However they may not have sufficient recordkeeping functionality. They can often be customised, or integrated with an ERMS (electronic records management system) to provide adequate control over business records.

It is probable that agencies will maintain more than one recordkeeping system in order to document the full scope of their business. For example, agencies might have a correspondence system for general files, a case management system to document interactions with particular clients or customers, a human resource system to document staff management activities and a finance system to record revenue and expenditure.

Ideally, all electronic systems that support an agency's business will be capable of capturing and managing digital records.

Agencies must ensure that the systems they employ, whether electronic, paper or hybrid, are capable of adequately managing their digital records and that the records are created and kept in appropriate conditions. The National Archives is developing generic specifications for records and information management systems to provide information on the characteristics of a system able to capture and manage records. The *Recordkeeping Metadata Standard for Commonwealth Agencies* describes the contextual information a system should be able to capture and maintain.

The DIRKS methodology can assist with systems design (see the pathway through DIRKS at the end of this section). These issues may be addressed at either the development stage or at the time of a significant upgrade to the system.

Where to from here?

Evaluate your agency's creation and capture of digital records using the Digital Recordkeeping Checklist, section 4.

Improve your agency's creation and capture of digital records according to the advice in this section. The following *e-permanence* products will assist:

- *DIRKS: A Strategic Approach to Managing Business Information* (see below for relevant pathway)
- generic specifications for records and information management systems (forthcoming)
- *Recordkeeping Metadata Standard for Commonwealth Agencies*

Pathway through DIRKS

- Use Step B to systematically analyse business activities and workflows. This will assist in identifying the points at which records and metadata should be created and captured.
- Use Step C to identify requirements to make and keep evidence of business activities. These requirements stem from business needs, legal and regulatory obligations, community expectations and potential exposure to risk.
- Use Step D to assess the recordkeeping functionality of existing systems.
- Use Step F to produce design documentation to enable new systems to create or capture digital records. The results can be used to move from a paper-based recordkeeping system to a digital system, or to manage a hybrid system.

5. CREATING INFORMATION ABOUT DIGITAL RECORDS

Key points

- Metadata is data that describes the context, content and structure of a digital record, and its management over time (5.1).
- Metadata ensures the authenticity, reliability, usability, integrity and accessibility of digital records over time (5.1.1).
- Resource discovery metadata assists retrieval of information (5.1.2).
- Australian Government agencies should capture and maintain metadata about their digital records (5.2).
- Metadata should be captured when records are created and during their management (5.2.1).
- The creation and capture of metadata should occur as a normal part of business and recordkeeping (5.2.2).
- Australian Government agencies should develop policies to ensure that metadata is created and managed appropriately (5.2.3).

5.1 What is metadata?

Metadata is data describing the context, content and structure of records and their management over time. Metadata allows users to control, manage, find, understand and preserve records over time.

Some examples of metadata are:

- the title of a record
- the subject it covers
- its format
- the date the record is created
- the history of its use
- details of its disposal.

There are two main categories of metadata that are used to manage digital records – recordkeeping metadata and resource discovery metadata.

5.1.1 Recordkeeping metadata

Recordkeeping metadata is structured or semi-structured information that enables the creation, registration, classification, access, preservation and disposal of records through time and across domains. Recordkeeping metadata can identify, authenticate, and contextualise records and the people, processes and systems that create, manage, maintain and use them.

The National Archives has produced the *Recordkeeping Metadata Standard for Commonwealth Agencies* to assist agencies in identifying and capturing appropriate recordkeeping metadata.

For digital records to be preserved over time, adequate recordkeeping metadata must be created, captured and maintained. Some metadata may need to be kept for long-term accountability or transfer to the National Archives. Other metadata may be destroyed at the time of the records' disposal. Requirements for retaining metadata and transferring it to the National Archives are set out in the *Administrative Functions Disposal Authority*.

Agencies should ensure their recordkeeping systems are capable of supporting the requirements of the Recordkeeping Metadata Standard.

5.1.2 Resource discovery metadata

One of the primary uses of metadata is to assist in the description of resources and improve methods of information retrieval. Metadata for resource discovery, such as the *AGLS Metadata Element Set*, AS 5044 – 2002, overlaps with and extends beyond the descriptive elements of recordkeeping metadata.

Better Services, Better Government: The Federal Government's e-Government Strategy requires all Australian Government agencies to describe their web-based resources in accordance with the *Commonwealth Implementation Manual: AGLS Metadata*. AGLS metadata can improve the accessibility of websites, intranets, and web-based services.

The different types of metadata are not mutually exclusive. Particular metadata schemas can serve more than one purpose and there is often overlap and inter-relationships between metadata schemas. For example, many of the elements required for resource discovery are also used for recordkeeping purposes.

Conversely, recordkeeping metadata can be the basis for a classification scheme, controlled vocabulary or thesaurus. These tools help staff choose terms for indexing, titling and retrieving records. See the end of this chapter for products that help agencies maximise the value of their metadata.

5.2 Capturing and maintaining metadata

Capturing and maintaining good recordkeeping metadata supports digital recordkeeping by:

- protecting records as evidence and ensuring their accessibility and usability;
- ensuring the authenticity, reliability and integrity of digital records;
- enabling the efficient retrieval of digital records;
- providing logical links between digital records and the context of their creation, and maintaining the links in a structured, reliable and meaningful way;
- allowing timely destruction of temporary-value records when business use has ceased; and
- providing information about technical dependencies, to help ensure digital records' long-term preservation and usability.

5.2.1 When should metadata be captured?

Recordkeeping metadata will generally be identified, and/or created when digital records are captured into recordkeeping systems. This defines the point at which the information formally becomes a record, fixes it in its context and enables its appropriate management over time.

Metadata collected at the point of capture of a digital record should document its content, structure and the context in which it was created.

Some metadata may be applied at a system level. For example, all records within a finance system will share the same metadata about the organisation creating the record, and the business activity being documented. This metadata can be automatically applied to all records generated within the finance system.

Other metadata will be generated as time progresses. Metadata related to business and recordkeeping processes will be added to a digital record during its lifetime. Examples include History of use (when the record was last viewed, whether it was accessed illegally), Location and Disposal status. Such metadata ensures the continued authenticity, security and integrity of the record.

5.2.2 How should metadata be captured?

Recordkeeping and business information systems should be designed and implemented with the necessary infrastructure to generate and capture appropriate metadata. Capture and maintenance of metadata should occur as a normal part of business and recordkeeping operations.

Where possible, the capture of metadata should be automated. Ideally, systems design should enable the greatest scope for automating the creation and capture of metadata. The greater the automation, the less likely it will be an intrusion on the daily activities of staff. Automation also ensures consistent interpretation of metadata schemas and the capture of more standard metadata, which facilitates records retrieval.

In many systems, it is likely that some metadata will be entered manually. Staff will require appropriate training and support to feel confident choosing titles or indexing terms as necessary (see 3.7 – User education and training). Simple procedures and systems that assist users to create metadata will lead to more consistency. Some applications provide semi-automated metadata capture. For example, when capturing an email, certain fields may be populated from the header. Users can be prompted to accept or override the data before a record is formally captured into the system.

Metadata required to support digital records may be captured and managed in several ways. The metadata can be:

- captured and managed within the recordkeeping or business information system in which the digital record is created and stored;
- captured into, and managed within, a separate metadata management system and linked to the relevant digital record; or
- encapsulated with the digital record, and managed as an integral part of it.

Systems that embed or encapsulate metadata into digital records have several advantages. They enable digital records to become ‘self-describing’ and remove the need for retention of metadata in parallel systems. However, this approach has disadvantages for the preservation of long-term records. There may be difficulties separating the data object from its metadata at a later date. Problems may arise when trying to maintain the metadata for disposed records, or converting a digital record to an archival format (see 10 – Preserving digital records for the long term).

5.2.3 How should metadata be managed?

Australian Government agencies should develop policies and practices to ensure that metadata is created and maintained in an appropriate manner. The aim is to standardise the metadata. Policies and procedures should be articulated in the overall recordkeeping and information management strategy for the organisation.

Policies and practices on managing metadata should:

- assign roles and responsibilities for capturing and managing metadata (see 3 – Digital recordkeeping framework);
- identify metadata elements to be captured (see *Recordkeeping Metadata Standard for Commonwealth Agencies*);
- establish when and how metadata is to be captured (see the DIRKS Manual);
- determine how long metadata needs to be retained (see 6 – Determining how long to keep digital records);
- detail how metadata is to be stored, including consideration of any persistent linkages between metadata elements and the records to which they relate (see 7 – Storing digital records);
- ensure that storage is secure and an audit trail of access, usage, and alterations or additions is kept to monitor the integrity and authenticity of the metadata (see 7 – Storing digital records);
- include adequate backup procedures and recovery mechanisms and a consideration of disaster management (see 9 – Business continuity planning for digital records); and
- provide for the preservation of metadata for as long as it is required (see 10 – Preserving digital records for the long term).

Where to from here?

Evaluate your agency's creation and capture of metadata using the Digital Recordkeeping Checklist, section 5.

Improve your agency's creation and capture of metadata according to the advice in this section. The following *e-permanence* products will assist:

- *Recordkeeping Metadata Standard for Commonwealth Agencies*
- *Commonwealth Implementation Manual: AGLS Metadata*
- *DIRKS: A Strategic Approach to Managing Business Information* (see below for relevant pathway)
- *Overview of Classification Tools for Records Management*
- *Developing a Functions Thesaurus*
- *Keyword AAA: A Thesaurus of General Terms* (Commonwealth version)

Pathway through DIRKS

- Use Step B to develop a business classification scheme (BCS). The BCS sets out the organisation's functions, activities, transactions and associated workflows. Classification tools built on the BCS enable consistent indexing, search and retrieval of digital resources.
- Use Step C to identify the essential metadata for the management of digital records.
- Use Step E to develop strategies for the creation and capture of metadata.

6. DETERMINING HOW LONG TO KEEP DIGITAL RECORDS

Key points

- The National Archives authorises disposal of digital records (6.1).
- Digital records can be retained for a variety of periods based on relevant recordkeeping requirements (6.2).
- A digital record must be managed, and remain accessible, for its lifetime (6.2).
- National Archives issues general disposal authorities and records disposal authorities to authorise the disposal of records (6.3).
- Disposal authorisation is format-neutral (6.3).
- Some records can be routinely destroyed in the normal course of business (6.4).

6.1 Authorisation for disposal of digital records

Digital records created by Australian Government agencies during the course of business are Commonwealth records for the purposes of the *Archives Act 1983* (see 2.1 – What are digital records?).

Disposal, that is, the destruction, transfer, damage or alteration of Commonwealth records, must be authorised by the National Archives under section 24 of the Archives Act unless it is:

- required by law (eg census records);
- in accordance with a practice or procedure approved by the National Archives (see 6.3.1 and 6.3.2); or
- in accordance with a normal administrative practice that the National Archives does not disapprove (see 6.4).

Disposal of Commonwealth records outside these parameters is illegal and can attract penalties under the Archives Act.

6.2 How long do digital records need to be retained?

As with other formats of records, digital records need to be retained until they are no longer required for any purpose. There are three general reasons digital records need to be created and kept:

- to meet the requirements of legislation and accountability
- to support the efficient conduct of business
- to meet the expectations of the community.

Generally, digital records, as with other records, will fall into one of the following categories.

- **Temporary value** – the records can be disposed of at an identified time (eg 'Destroy 7 years after action completed'). Temporary-value records can range in retention length from a very short period, such as one year, up to an extended period, such as 'Destroy 130 years after date of birth (of subject)'.
- **Retain permanently in agency** – the records have a long-term business use in the agency, but are not considered to have archival value.

- **Archival value** – the records cannot be disposed of but instead will be retained in the custody of the National Archives indefinitely. Agencies nominate groups of records when they develop a records disposal authority. The National Archives decides which records meet the criteria for archival value.

A digital record must be managed, and remain accessible, for its lifetime. How long a digital record needs to be kept will influence its management. In these guidelines, we refer to 'retaining digital records for the long term'. Given the vulnerable nature of most digital media and the frequency of technology change, 'long term' for digital records generally means longer than one generation of technology. Digital records that must be retained for the long term will require active management to ensure their continued accessibility (see 10 – Preserving digital records for the long term).

6.3 Obtaining approval for disposal of digital records

The National Archives produces general disposal authorities (GDAs) that can be used by all Australian Government agencies to dispose of records. The National Archives approves records disposal authorities (RDAs) developed by agencies to cover their core business records.

Generally, disposal authorisation is format-neutral. Authorisation is given to dispose of records documenting particular business activities. Those records can be created and kept in any format.

6.3.1 General disposal authorities

GDAs cover records common to many agencies. Some GDAs will be of particular interest to staff responsible for managing digital records.

Administrative Functions Disposal Authority (AFDA)

The *Administrative Functions Disposal Authority* covers the records of 17 administrative functions and is linked to the business classification scheme of *Keyword AAA: A Thesaurus of General Terms* (Commonwealth version).

Relevant classes can be found under:

- TECHNOLOGY AND TELECOMMUNICATIONS – Control, eg how long to keep audit trails, user access logs
- INFORMATION MANAGEMENT – Control, eg control records (metadata), business rules, configuration settings

GDA for source records

The *General Disposal Authority for Source Records that have been Copied, Converted or Migrated* permits the destruction of source records that have been copied, converted or migrated, provided equivalent reproductions are maintained. It also sets conditions for the proper management of copying, conversion and migration processes.

GDA for encrypted records

The *General Disposal Authority for Encrypted Records Created in Online Security Processes* permits the disposal of encrypted records created during online security processes. It covers encrypted versions of inbound and outbound electronic transactions. A number of conditions are attached to the use of the disposal authority.

GDA 24 – data matching

General Disposal Authority 24 – Records Relating to Data Matching Exercises relates to the disposal of records following data matching exercises.

6.3.2 Records disposal authorities

Agencies should develop RDAs to cover their core business records. The records manager will know whether your organisation already has an RDA. RDAs are developed using Steps A to C and Appendix 8 of DIRKS.

Agencies should ensure that disposal authorities cover all of the records they create. Generally, this will be a combination of an RDA and the GDAs issued by the Archives for records common to many agencies.

6.4 Normal administrative practice

Normal administrative practice (NAP) defines types of records that agencies may routinely destroy in the normal course of business. Agencies do not need to contact the Archives for permission to dispose of records within the scope of NAP.

NAP usually applies to information that is duplicated, unimportant or only of short-term facilitative value. For example:

- superseded system backups;
- trivial electronic messages that are not related to agency business;
- address lists and change of address notices;
- calendars, office diaries and appointment books (unless identified in a records disposal authority as having additional value);
- rough drafts of reports, correspondence, routine or rough calculations;
- routine statistical and progress reports compiled and duplicated in other reports;
- abstracts or copies of formal financial records maintained for convenient reference;
- duplicated material such as forms or templates;
- thermal paper facsimiles after making and filing a photocopy or scan.

The National Archives can disapprove a normal administrative practice if it believes that important records are being put at risk. If you receive a notification from the Archives disapproving a normal administrative practice, you must cease the practice immediately.

The NAP provision must not be used to:

- destroy records of significant agency operations;
- destroy records that document the rights and obligations of the government or private individuals;
- cull documents within files; or
- destroy business-related electronic messages before they become part of the formal record.

NAP should not be applied to records or information that can be used as evidence.

For further information about normal administrative practice, see Archives Advice 18 – Normal administrative practice.

Where to from here?

Evaluate your knowledge of how long your agency's digital records need to be kept, and your arrangements for keeping them, using the Digital Recordkeeping Checklis*t*, section 6.

Improve your knowledge of how long your agency's digital records need to be kept, and your arrangements for keeping them, according to the advice in this section. The following *e-permanence* products will assist:

- *Administrative Functions Disposal Authority*
- *General Disposal Authority for Source Records that have been Copied, Converted or Migrated*
- *General Disposal Authority for Encrypted Records Created in Online Security Processes*
- *DIRKS: A Strategic Approach to Managing Business Information* (see below for relevant pathway)

Pathway through DIRKS

- Use Step A, Step B, Step C and Appendix 8 to determine how long records should be kept to meet legal, business and community needs and develop a records disposal authority.

7. STORING DIGITAL RECORDS

Key points

- Digital records can be stored online, offline or nearline depending on the frequency of the need to refer to them (7.1).
- Digital records required for long-term retention, or identified as being either vital records or of archival value, should be stored online (7.2).
- Selecting the appropriate digital storage device for digital records involves a range of considerations (7.2.1).
- Digital storage devices on which digital records are stored should be maintained and stored in suitable physical surroundings (7.3).
- Digital storage devices should be monitored and records periodically refreshed, ie transferred from obsolete or ageing storage devices to suitable replacements (7.4).
- If digital storage devices are not refreshed, digital records may be lost (7.5).

7.1 How are digital records stored?

To ensure the ongoing protection of digital records, agencies require efficient and effective means for maintaining, handling, and storing digital records – both active and inactive – over time. Policies, guidelines and procedures for the storage of digital records should be an integral component of an agency's digital recordkeeping framework (see 3 – Digital recordkeeping framework).

There are three ways in which agencies may store digital records – online, offline or nearline.

- **Online** – Online records can be contained on a range of storage devices (eg mainframe storage, network attached storage or PC hard drive) that are available for immediate retrieval and access. Generally, records stored online will be active digital records – ie records that are regularly required for business purposes. Electronic messaging systems and word-processed documents saved to the network server fall into this category.
- **Offline** – Offline digital records are contained on a system or storage device that is not directly accessible through the agency network and which requires human intervention in order to be made accessible to users. Digital records that are stored offline are usually retained on removable digital storage media (eg magnetic tape, CD, DVD) and are generally inactive digital records not regularly required for business purposes. Offline digital records may be stored offsite as part of an agency's business continuity plan (see 9.3 – Counter disaster strategies).

  Digital records stored offline are not immediately available for use. Agencies must take responsibility for monitoring and guarding against environmental degradation and changes in technology that may adversely affect the storage media employed (see 7.3).
- **Nearline** – Nearline storage of digital records means the records are contained on removable digital storage media, but remain relatively accessible through automated systems connected to the network. These digital records are technically considered to be offline. The use of systems such as CD jukebox or magnetic tape silos allow them to be made available through agency networks, in

relatively short periods of time and without the need for human intervention (ie staff are not required to physically retrieve the storage media on which the required information is retained).

Generally, digital records will begin life as online records and, as the immediate business need to refer to them diminishes over time, they will be moved to either nearline or offline storage, depending upon the technology available to the agency, the ongoing relevance and value of the records and their retention requirements.

Based on relevant recordkeeping and business requirements, Australian Government agencies must decide which digital records are to be captured and maintained online and which digital records can be retained in nearline or offline storage.

7.2 Selecting the appropriate storage method

We strongly recommend that digital records of vital significance to an agency, as well as digital records required for long-term retention within agencies, and digital records of archival value, be stored online.

Online storage devices, such as network storage devices and mainframe storage, have the following advantages.

- Digital records stored online will, in most cases, be retained on the magnetic hard drives that form an agency's network, where they will be readily accessible to users and can be maintained and controlled as an integral part of the agency's recordkeeping system.
- Large storage capacities allow for significant quantities of digital records to be retained on a single storage device.
- Regular integrity checks of digital records can be more readily performed and, in some instances, it may be possible to automate these tasks.
- Digital records stored online have a greater likelihood of being identified and included within any changes made to agency IT systems, such as system-wide migration processes.
- Online storage devices need not be linked directly to an agency network. Where security concerns, business considerations or other factors warrant, agencies may opt to establish standalone online storage systems.
- Increasingly, online storage systems can support sophisticated automated techniques and redundant designs that aid digital record control, monitoring and backup.

The automated nature of nearline systems means that they share many of the advantages of online systems, even though the digital records stored on nearline systems are retained on physical storage media such as DVDs, CDs and magnetic tapes. Where it is not possible for digital records to be maintained online, agencies are encouraged to use nearline storage devices, such as CD jukeboxes and magnetic tape silos.

For storing digital records, the National Archives does not recommend CDs, DVDs, magnetic tape and other removable digital media formats that are physically maintained, but not accessible from active computer systems. Offline digital storage devices are suitable only for storing relatively low-value digital records and are not recommended for long-term digital records, vital records or records identified as being of archival value.

Offline digital storage devices present the following challenges.

- The records are not immediately accessible to users, as the storage media must first be physically retrieved.
- Individual media need to be labelled and stored in a manner that permits them to be easily accessed. Failure to adequately store removable digital media formats may result in digital records being physically misplaced or lost.
- Removable media are less likely to be routinely accessed and may be missed when conducting routine integrity checks.
- Similarly, offline media are often overlooked when agency systems are upgraded and digital records are migrated to new formats. This can result in the digital records contained on offline media becoming inaccessible.
- Device failure is only detected when an attempt is made to use the records.

7.2.1 How to select a digital storage device

Regardless of whether agencies adopt an online, offline or nearline storage method, Australian Government agencies should take the following into account before selecting a specific storage device.

- How often and how quickly will the records need to be accessed?
- Is the proposed storage device versatile and has it the capacity to accommodate the size, number and complexity of digital records to be stored?
- Is the longevity, reliability and durability of the proposed storage device sufficient to meet the required retention periods for the digital records it is to contain? In the case of long-term digital records, the selected format should be robust and have a clearly definable migration path and widespread industry support to improve the chances of forward compatibility.
- Are the technical standards associated with the storage device technology open source? Proprietary storage formats may be less widespread and less likely to be sustained and supported over time.
- Will the selected storage device have any special physical or environmental storage requirements?
- Do the assessed costs and benefits of the proposed storage device suit the needs of the agency and the digital records to be stored? Costs include migrating records, the storage device and associated hardware, and any training that may be required.

7.3 Maintaining records in storage

To keep digital records over time, Australian Government agencies should consider not only the storage devices, but also the facilities for housing them and the computer systems that generate the records.

Digital records are more vulnerable than paper records, so agencies need to devote more time and resources to their accommodation. The earlier an agency can plan for the storage and retention of digital records, the better, in terms of the records' longevity.

Storage conditions should support record protection, make records accessible, and be cost effective. Digital storage devices are susceptible to fluctuations in humidity, temperature and radiation, so the National Archives strongly advises that stable environmental conditions be maintained.

Periodically, agencies should undertake risk analysis to ensure that storage conditions are appropriate for both digital storage devices and information systems.

Agencies should also perform regular and ongoing integrity checks of all digital storage devices, such as data object checksums, to ensure that no deterioration or data loss is occurring.

Advice on appropriate storage conditions for computer and information systems and digital storage devices can be found in the Defence Signals Directorate publication *Australian Government Information Technology Security Manual* (ACSI 33) and the *Commonwealth Protective Security Manual*, issued by the Attorney-General's Department.

For information on the requirements for the storage of digital media, please refer to the National Archives' best practice *Standard for the Physical Storage of Commonwealth Records* and the supporting guidelines.

Digital storage technology is always improving, with new digital storage devices evolving to replace older, outmoded devices. Agencies should be aware of developments in storage technologies with a view to ensuring that there are clear migration paths for the storage device technology they currently employ (see 7.4).

7.3.1 Special requirements for offline digital storage devices

The life expectancy of offline digital media varies depending on the format and quality of the media, storage conditions, and handling and treatment. Damage resulting from deterioration will differ depending on the types of media involved and may vary from corrupt sectors on a disk, resulting in one or more files becoming inaccessible, to the complete loss of all information on the media.

Given the potential for digital records to be lost as a result of media deterioration, it is critical that agencies monitor digital media integrity and schedule periodic refreshing of media (see 7.4).

Specific advice on the care, handling and maintenance of digital storage media is available from Archives Advice 5 – Protecting and handling magnetic media and Archives Advice 6 – Protecting and handling optical disks.

7.4 Refreshing digital storage devices

Online, offline and nearline digital storage devices have limited life expectancy. It is imperative to monitor them continuously and refresh them periodically – ie migrate the data to a suitable replacement. Examples of migration include the transfer of digital records from an outmoded online storage system to a replacement online system, or the transfer of records stored on an outmoded offline digital media format, such as a floppy disk, to a replacement media format, such as a compact disk.

The greatest problem in planning for the refreshment of digital storage devices, is identifying when it is appropriate to replace them. Unlike paper-based records, deterioration of digital storage devices does not become obvious until the point of data loss and, by that stage, it can often be too late to salvage the records.

The fact that most digital storage devices have only emerged recently, means that the life expectancy for these devices is largely unproven. Rapid cycles of technological obsolescence occurring within the IT industry present the possibility that digital storage devices may well become outmoded, unsupported and obsolete due to unavailability of the software and hardware required to access the records stored on them long before the storage devices themselves physically degrade.

Australian Government agencies are therefore advised to be conservative when planning for the refreshment of storage devices, and to err on the side of caution, rather than risk the loss of digital records from storage device deterioration. In deciding when to refresh storage devices, agency staff will need to consider the following factors:

- vendor claims of storage device life expectancy (preferably supported by evidence from independent tests);
- technological advancements that make the current storage device obsolete;
- ready access to equipment capable of reading and rendering the digital records contained on the current storage device;
- relevant standards (eg ISO 18921 on estimating the life expectancy of compact disks based on the effects of temperature and relative humidity); and, most importantly,
- the results of ongoing internal storage device integrity checks.

When contemplating refreshing digital storage devices, agencies should consider the selection criteria for digital storage devices (see 7.2.1). Where digital records are transferred to a new digital storage device, the content, context and format of the digital records contained on the existing storage device must not be altered as a result of the transfer.

Standard error checking techniques should be used to assess the quality of the blank storage device to be used. And after the transfer has been completed (and before the source records are destroyed), spot checks should be undertaken to ensure that the digital records have been reliably and accurately transferred to the new device. Verification techniques, such as checksums, should be used to confirm digital record integrity.

After each transfer it is advisable to perform a test restoration of the data to verify the success of the process and ensure that the digital records are still accessible.

7.5 Recovering lost digital records

Where digital storage devices are not refreshed in a timely manner there is a significant chance that the digital records they contain will become corrupted and inaccessible. Allowing digital records to become inaccessible may be viewed as a breach of the *Archives Act 1983*.

In cases where digital records cannot be accessed due to the failure or corruption of the storage device, agencies should seek assistance from commercial data recovery services and take all reasonable steps to recover the digital records. The feasibility and cost of recovering the lost digital records will depend on the type of digital storage device used, the level of degradation and the complexity of the recovery process required. While it may not always be possible to completely recover digital records from damaged storage devices, in most cases there will be a reasonable prospect of at least partial success.

Agencies will need to balance the value and significance of the lost or damaged digital records with the cost of their recovery. Where the digital records involved are of temporary value, and the loss of the records does not pose an unacceptable risk to the agency, the cost of recovery may not be justified.

In cases where digital records of archival value are concerned every effort should be made to recover the records.

Agencies faced with the task of recovering inaccessible digital records of archival value should contact the National Archives for further assistance.

Where to from here?

Evaluate your agency's storage of digital records using the Digital Recordkeeping Checklist, section 7.

Improve your agency's storage of digital records according to the advice in this section. The following products will assist:

- Archives Advice 5 – Protecting and handling magnetic media
- Archives Advice 6 – Protecting and handling optical disks
- *Standard for the Physical Storage of Commonwealth Records*
- *Storing to the Standard: Guidelines for Implementing the Standard for the Physical Storage of Commonwealth Records*
- *Australian Government Information Technology Security Manual* (ACSI 33)
- *Commonwealth Protective Security Manual*
- *DIRKS: A Strategic Approach to Managing Business Information* (see below for relevant pathway)

Pathway through DIRKS

- Use Step C to identify and document the organisation's recordkeeping requirements. This fundamental step provides the basis for designing systems that facilitate recordkeeping processes, and the benchmark for measuring system performance.
- Use Step D to assess the effectiveness of existing systems or off-the-shelf software. Particular attention may be paid to a system's capacity to store and maintain digital records for as long as they are required.
- Use Step F and Step G to design and implement new systems to ensure they address requirements for storing digital records over time. Functional specifications can be built on the results of Step C.
- Use Step H to evaluate the performance of a recently implemented system, and take corrective action if necessary.

8. SECURING DIGITAL RECORDS

Key points

- Digital records can be easily modified, so their security is very important (8.1).
- Australian Government agencies are required to provide adequate security for their records (8.2).
- Australian Government agencies may adopt some basic practices to secure their digital records and systems (8.3).
- Australian Government agencies must implement systems and practices that prevent unauthorised alteration of digital records (8.4).
- Particular care should be taken that digital records of long-term value remain authentic and accessible (8.5).

8.1 Why is security important for digital records?

Security is important for all records. The manipulable nature of digital records means that, in the absence of appropriate safeguards, it is relatively easy to alter or delete them – whether intentionally or unintentionally. Alterations to digital records can be virtually undetectable, undermining their evidential value as records.

When implementing systems, agencies must therefore take special care to ensure they are secure, reliable and capable of producing records that are acceptable for legal, audit and other purposes.

The remainder of this section describes security measures to be taken to prevent data loss, data corruption, unauthorised data access and to ensure the integrity, reliability and confidentiality of digital records.

8.2 Security and planning for digital records

The *Commonwealth Protective Security Manual* issued by the Attorney-General's Department directs Australian Government agencies to consider the security needs of their systems and to devise policies and plans to ensure that systems are appropriately protected. Australian Government agencies are required to prepare an agency security plan that describes the security mechanisms and procedures that have been implemented to protect digital records and systems.

As a first step towards developing an agency security plan, formal threat and risk assessments should be conducted on all agency computer systems (including information systems, recordkeeping systems and online services provided by the agency) by an appropriately qualified body or agency. System vulnerabilities and potential threats should be identified and strategies developed and implemented to reduce the likelihood of security breaches occurring.

Security measures must be implemented for all systems. The *Australian Government Information Technology Security Manual* (ACSI 33), developed by the Defence Signals Directorate, provides detailed guidance to Australian Government agencies on protecting systems and digital records.

8.3 Methods of securing digital records and systems

The following are some basic practices and protocols Australian Government agencies may adopt to ensure they maintain adequate security for their digital records and systems. This list is not exhaustive. Agencies should select a combination of methods to suit their needs.

- Limit access to digital records, and the systems on which those records are created and kept, to authorised personnel in order to protect the integrity of the records and prevent unlawful alteration or destruction of records.
- Establish network security systems, such as firewalls, to protect against unauthorised access (eg hackers) to systems that are accessible through external connections, such as the Internet.
- Install appropriate gateway filter software on messaging systems, and ensure that filter definitions are regularly updated, to protect against spam, denial of service attacks and malicious code, such as computer viruses (see 13.1.3 – Messaging system management tools).
- Implement public key infrastructure (PKI) encryption technologies to ensure secure transmission of digital records to external parties (see 13.3 – Records subject to online security processes).
- 'Lock' final digital records to prevent any subsequent alterations or inadvertent destruction (eg finalising records as 'read-only' within an electronic recordkeeping system).
- Use digital signature technologies to authenticate digital records and provide security and confidence in authorship (see 13.3 – Records subject to online security processes).
- Store vital digital records either offline or on systems without external links (see 9 – Business continuity planning for digital records).
- Establish appropriate systems backup procedures and disaster recovery strategies to protect against loss of digital records (see 9 – Business continuity planning for digital records).
- Develop and implement audit trails to detect who accesses a system, whether prescribed security procedures were followed and whether fraud or unauthorised acts have occurred, or might occur.

Physical storage security standards for computer rooms, workstations and digital media storage areas are issued by the Defence Signals Directorate in ACSI 33 and by the Attorney-General's Department in the *Commonwealth Protective Security Manual*. The level of security required will differ depending on the value and sensitivity of the information held by the agency and the risk posed by the potential loss of the records.

Standards such as *Information Technology – Code of Practice for Information Security Management,* ISO/IEC 17799 – 2000, *Information Security Management – Specification for Information Security Management Systems*, AS/NZS 7799 – 2003 and *Guidelines for the Management of IT Security*, ISO/IEC 13335 may also be used to provide benchmarks and guidance on digital records security within Australian Government agencies.

Security practices should be periodically reviewed and system log files interrogated to identify any potential attempts to breach systems security – as well as any previously undetected breaches. The relevant agency manager should develop incident reporting systems and be familiar with the appropriate Defence Signals Directorate security contact personnel so that breaches of security can be reported in a timely manner and appropriate action taken to prevent further breaches.

8.4 Authentication of digital records

Digital records provide evidence of agency business activity. For digital records to retain their evidential value, and be admissible as evidence in court, systems and practices must prevent the unauthorised alteration of digital records, and so ensure their continued authenticity.

To guarantee the authenticity of digital records, systems and procedures should be capable of establishing:

- if digital records have been altered
- the reliability of software applications creating digital records
- the time and date of creation and alteration of digital records
- the identity of the author of a digital record
- the safe custody and handling of records.[5]

Version control is a useful tool for preserving the authenticity of digital records. Digital source records should be clearly distinguished from any subsequent copies. Identification may be achieved through labelling of records or by time and date stamps.

To provide evidence of business activities or action taken, agencies must be able to clearly demonstrate the provenance of digital records. This includes establishing the original conditions for the creation of the record, such as date and time of creation, software application integrity and the author or sender of a record. The ability to track when the record was last altered, by whom, and the 'chain of custody' (who was responsible for the record) will also support a record's evidential value.

Clearly implemented policies and procedures demonstrate that an agency has protected the provenance of its digital records.

In some instances, authenticity may be demonstrated if access to digital records is restricted to authorised persons or applications. In such cases, there must be security mechanisms to prevent unauthorised persons or applications accessing the digital record. Audit trails should be able to verify that digital records have not been accessed inappropriately or illegally.

Alternatively, agencies may make use of standards-based cryptographic techniques to authenticate authorship, enable secure transmission and provide strong evidence that a particular digital record has not been altered, or that a copy of the record is identical to the original (see 13.3 – Records subject to online security processes). Digital records should be decrypted before being captured into secure recordkeeping systems.

8.5 Long-term digital records

Australian Government agencies should take additional care to ensure that their security and authentication mechanisms do not inadvertently make digital records inaccessible in the long term and that the evidential value of the records does not diminish over time. This is particularly important for records of archival value.

[5] Adapted from Standards Australia, 2003, *Guidelines for the Management of IT Evidence*, HB 171 – 2003.

Agencies should address the following considerations when applying security and authentication practices and protocols to digital records.

- If manipulation of data is required (eg encrypting a file to send via email), the process should be applied to a copy of the source record. The source record should be maintained separately in a secure recordkeeping system. This will safeguard records of long-term or archival value in the event that data loss occurs during manipulation or the file becomes inaccessible.
- Access controls should be applied and maintained within a recordkeeping system. Staff should be discouraged from using software functions to create passwords or limit access to business records. This includes specifying who can read or alter a document, preventing copying or printing, or setting an expiration date (see 13.1.3 – Messaging system management tools).

  Documents that have been password-protected or otherwise restricted should not be captured into a recordkeeping system while the restrictions are still in place. There is a considerable risk that records will become inaccessible as staff changes occur and passwords are forgotten over time. Unrestricted records should be captured into recordkeeping systems. Authorised users can then apply access controls, in accordance with business rules.
- Metadata attesting to the validity of a digital signature, where a digital record has been authenticated using such technology, should be captured and maintained for as long as required. If such information is not kept, the evidential value of the record may be undermined (see 13.3 – Records subject to online security processes).
- Digital records that have been encrypted should be decrypted prior to capture in a secure recordkeeping system. Metadata relating to the encryption and authentication process should be captured and maintained for as long as required. If encrypted records are captured and kept there is a considerable risk they will become inaccessible (see 13.3 – Records subject to online security processes).

Where to from here?

Evaluate your agency's security of digital records using the Digital Recordkeeping Checklist, section 8.

Improve your agency's security of digital records according to the advice in this section. The following products will assist:

- *Australian Government Information Technology Security Manual* (ACSI 33)
- *Commonwealth Protective Security Manual*
- *DIRKS: A Strategic Approach to Managing Business Information* (see below for relevant pathway)

Pathway through DIRKS

- Use Step D to conduct a survey of current systems and practices. This can be used to evaluate compliance with security requirements and other recordkeeping obligations.

- Use Step F and Step G to incorporate security and authentication controls in the design and implementation of new systems.
- Use Step H to verify that a recently implemented system is protecting records from malicious damage or unauthorised tampering.

9. BUSINESS CONTINUITY PLANNING FOR DIGITAL RECORDS

Key points

- Loss of digital records can be crippling for an agency (9.1).
- Business continuity plans comprise measures to prevent, prepare for and recover from a disaster (9.2).
- Australian Government agencies should prepare to counteract the effects of a disaster (9.3).
- Australian Government agencies should take particular care that preparations are made to restore records vital to the re-establishment of their business, and digital records of archival value, in the event of a disaster (9.4).
- Recovery of digital records should be accorded a high priority in an agency's business continuity plan as delays can result in substantial loss of data (9.5).

9.1 Why plan for business continuity?

Loss of digital records in a disaster can be crippling for an agency. Information is the lifeblood of modern business – communications, contracts, research data, strategic plans, policy advice, customer records, payments and receipts. Without records, business grinds to a halt, corporate memory is lost and agencies are vulnerable to a multitude of risks.

Data on digital storage devices can be more susceptible to damage through disaster than other record formats, such as paper or microforms. Relatively minor damage to digital storage devices can easily render all information contained on a storage device inaccessible.

Disasters that can affect digital records include:

- natural events such as earthquakes, cyclones, bushfires, floods and vermin plagues;
- structural or building failure such as malfunctioning sprinklers, leaks in roofs, poor wiring and power surges;
- industrial accidents such as nuclear or chemical spills;
- technological disasters such as viruses and computer equipment failures;
- criminal behaviour such as theft, arson, espionage, malicious computer hacking, vandalism, riots, terrorism and war; and
- accidental loss through human error, unsuitable storage conditions (eg storage of magnetic media near electronic equipment generating strong magnetic fields) or by the natural decay of materials (eg corrosion of poor quality compact disks).[6]

All digital records and systems for which an Australian Government agency is responsible should be incorporated into a business continuity plan. Appropriate disaster management arrangements for records created, and systems used, by

[6] State Records Authority of New South Wales, *Guidelines on Counter Disaster Strategies for Records and Recordkeeping Systems*, June 2002, published online at www.records.nsw.gov.au/publicsector/rk/guidelines/counterdisaster/toc.htm).

outsource providers on behalf of the agency should also be provided for in contractual obligations.

9.2 Establishing a business continuity plan

The National Archives encourages all Australian Government agencies to develop, implement and maintain an effective business continuity plan to cover their digital records and recordkeeping and business information systems. It is critical to plan and protect digital records and business information systems from the risk of disaster, and to ensure the continuation of business in the event of a disaster.

Typically, a business continuity plan will comprise measures to prevent or minimise the impact of a disaster (see 9.3), protection strategies for vital records (see 9.4) and disaster recovery and restoration procedures to be followed if a disaster occurs (see 9.5).

The key components of such a plan include:

- a general policy statement;
- assignment of staff responsibilities, including contact details for emergency services staff and the agency disaster recovery team;
- threat analysis identifying the most likely potential disasters;
- steps for preparedness, response and recovery;
- procedures for identification and declaration of a disaster situation;
- list of vital records, noting significant or vulnerable holdings, and associated location and control documentation (see 9.4);
- clearly identified priorities for salvage;
- details of equipment and materials available for use in disaster salvage and recovery;
- building plans identifying and addressing any potential site risks;
- provisions for staff training and current awareness; and
- emergency funding and insurance arrangements.

Periodic monitoring and review of an agency's business continuity plan should be undertaken to ensure its continued viability and effectiveness.

9.3 Counter disaster strategies

Australian Government agencies should be proactive in matters of business continuity and ensure that appropriate procedures and practices are in place to minimise the risk of digital records being lost or damaged as a result of disaster.

Before establishing a business continuity plan, agencies should undertake a risk analysis to determine the types of threats faced, the likelihood of disasters occurring and the potential impact of the resulting loss of records. All reasonable risks affecting digital records and business information systems should be identified, prioritised and assessed as part of the risk analysis, so that steps can be taken to determine appropriate counter disaster strategies.

Counter disaster strategies are measures devised and implemented to improve an agency's capacity to prevent, prepare for and respond to disasters. Implementation of these strategies is central to any business continuity plan.

The following represent the core counter disaster strategies for the protection of digital records:

- duplication and dispersal of vital digital records (see 9.4.1);
- transfer records of archival value to the National Archives as soon as they are no longer required for business needs (see 9.4.2);
- regular and comprehensive system backups (see 9.3.1);
- preservation of systems and application documentation and passwords;
- secure storage facilities for digital devices, including fire and water resistant housings and appropriate environmental controls;
- high standards of systems security to prevent digital records from being unlawfully altered or destroyed and to safeguard against computer viruses (see 8 – Securing digital records); and
- procedures for managing critical work in progress which may not be backed up or which is located outside storage facilities.

9.3.1 System backups

Agencies should perform system-wide backups of all corporate data on a regular basis as a matter of routine operating procedure – with emphasis given to identifying and duplicating vital digital records and those of archival value.

If it is not possible to separate vital records within a system (for example, in an electronic document and records management application), a backup should be made of the whole system. Metadata connected with these records should also be duplicated and maintained offsite with the copied records.

In order that system backups capture as much of an agency's business information as possible, counter disaster strategies should influence agency work processes (ie by encouraging the creation of policies to centralise business information).

Employees should be encouraged to work from network drives rather than their workstation hard drives, and discouraged from storing files on removable digital media. Where applicable, records should be captured into recordkeeping or business information systems as soon as practical. The digital recordkeeping framework should include guidelines discouraging the use of auto-archiving of emails and other user-controlled backup facilities (see 3 – Digital recordkeeping framework).

The frequency of backups, and the period they are retained, will be determined by the results of the agency's risk management assessment and organisational requirements. System backups should be as comprehensive as possible and include information from all corporate directories and networked drives. In organisations where staff are permitted to store corporate records to workstation hard drives, this data should be uploaded for backup. Backup procedures should also be established for digital records stored offline on digital storage media.

9.4 Vital and archival value digital records

9.4.1 Vital records

Vital records are records that are essential for the ongoing business of an organisation, without which it could not continue to function effectively. These can include daily invoices through to the minutes of meetings of executive bodies.[7] Vital records should be proactively identified. *DIRKS: A Strategic Approach to Managing Business Information* assists agencies to do this (see the pathway through DIRKS at the end of this section).

Business continuity plans, including counter disaster and disaster recovery strategies, should give vital digital records high priority.

The most effective method of protecting vital digital records, is to duplicate the records and maintain the duplicates in secure offsite storage. The relative ease with which digital records can be duplicated and the low cost of digital storage makes this strategy both effective and affordable.

Duplicate vital records and system backups should always be stored offsite at a sufficient distance from the originating office to be relatively secure from the effects of the same disaster. Storage facilities should be secure, have appropriate environmental controls and meet the requirements set out in the National Archives' best practice *Standard for the Physical Storage of Commonwealth Records* and the supporting guidelines (see 7 – Storing digital records).

In addition to storing duplicates of digital records offsite, agencies will need to maintain duplicates of systems and application software and documentation, access codes, passwords, serial numbers and other information relevant for the re-establishment of the agency's computer systems. Ideally, the equipment necessary to access the records should also be stored offsite, or alternative sources of the equipment should be identified in the business continuity plan. It is not enough to preserve the digital records. The capacity for the agency to access the records must also be preserved.

9.4.2 Digital records of archival value

Every care should be taken to ensure that digital records of archival value receive maximum protection. Counter disaster strategies should indicate that loss of archival value digital records is not acceptable, based on risk analysis.

The best way to safeguard digital records of archival value is to transfer them into the custody of the National Archives as soon as they are no longer required for immediate business needs (see 12 – Disposing of digital records).

9.5 Disaster recovery

Business continuity plans should include disaster recovery and restoration procedures to enable an agency to swiftly re-establish its business operations after a disaster.

Disaster recovery procedures should:

- provide advice on recommended handling procedures and preservation techniques for damaged digital media;

[7] Australian National Audit Office, *Recordkeeping in Large Commonwealth Organisations*, published online at www.anao.gov.au/WebSite.nsf/Publications/478B4A27724E193BCA256DA50074796C

- enable the timely re-establishment of vital computer systems and critical data;
- make arrangements for data integrity checking to ensure salvaged digital records are intact;
- ensure access to specialised data recovery services; and
- ensure that vital digital records are restored as quickly as possible.

Recovery of digital records should be given an appropriately high priority within an agency's business continuity plan, as delays in attending to the recovery of digital records can result in substantial loss of data. It is a good idea to identify requirements for point-in-time recovery (ie recovery of records as they existed at a particular point in time – eg just before the disaster), because reverting to an earlier backup will result in the loss of any records that were created in the interim period. While there are methods of recovering data from damaged or corrupted digital storage media, these processes can be very expensive and in many cases cannot retrieve all data lost (see 7.5 – Recovering lost digital records).

One reason for major delays in re-establishing systems is the ready availability of replacement servers. Mission-critical applications should have failover servers (ie servers that automatically come online in the event of a problem with the primary server) and offsite standby servers to enable restoration as soon as possible. Disaster recovery procedures should be tested regularly.

For more information on disaster preparedness and recovery, see the *Standard for the Physical Storage of Commonwealth Records* and *Disaster Preparedness Manual for Commonwealth Agencies*.

Where to from here?

Evaluate your agency's business continuity plan for digital records using the Digital Recordkeeping Checklist, section 9.

Improve your agency's business continuity plan for digital records according to the advice in this section. The following *e-permanence* products will assist:

- *DIRKS: A Strategic Approach to Managing Business Information* (see below for relevant pathway)
- *Standard for the Physical Storage of Commonwealth Records*
- *Storing to the Standard: Guidelines for Implementing the Standard for the Physical Storage of Commonwealth Records*
- *Disaster Preparedness Manual for Commonwealth Agencies.*

Pathway through DIRKS

- Use Step C and Step D to gain an appreciation of your organisation's level of exposure to risk due to such events as failures of accountability, legal action and loss of vital records.
- Use Step C to identify records vital to the performance of your organisation's business.

- Use Step E to identify strategies to remedy weaknesses, protect against system failures and recover vital records in the event of a disaster.
- Use Appendix 11 to assist in the application of risk management principles to recordkeeping.

10 PRESERVING DIGITAL RECORDS FOR THE LONG TERM

Key points

- Digital records must be preserved and accessible to meet the requirements of legislation and support the efficient conduct of business (10.1).
- Given the rapid obsolescence of digital technology, Australian Government agencies must plan for the preservation of digital records (10.2).
- Australian Government agencies must be proactive to ensure the preservation, and continued accessibility, of digital records over time (10.3).
- The most common techniques for preserving digital records can be divided into three broad categories – migration, encapsulation and emulation (10.4).
- The National Archives' preferred approach involves converting, or 'normalising' digital records into archival data formats (10.5).
- Implementing a successful preservation strategy involves a number of requirements (10.6).

10.1 Why preserve digital records?

Considering the problems of technological change, and the potential instability of digital storage media, 'long term' may not be very long. When applied to the preservation of digital records, 'long term' usually means 'greater than one generation of technology'.

Many records have retention periods greater than one generation of technology. It is important that these records are preserved and accessible for use in daily business. Long-term records support strategic planning and decision-making. They act as corporate memory, reducing duplication of work and improving business efficiency.

There may also be evidentiary reasons to keep digital records for extended periods, as part of a risk minimisation strategy. Inaccessible records may expose agencies to accountability failures and potentially costly consequences, such as legal action. The Australian National Audit Office's *Recordkeeping* report (2002) recommends agencies develop strategies to preserve/migrate electronic records, and to ensure that all digital records are captured into a corporate recordkeeping system.

Australian Government agencies have legal responsibilities under the *Privacy Act 1988*, the *Freedom of Information Act 1982*, and the *Archives Act 1983* to ensure the ongoing maintenance and accessibility of their records. Long-term maintenance is particularly significant for digital records of archival value. Inadequate preservation strategies can render digital records inaccessible and unusable. Allowing digital records to become inaccessible may be considered a breach of the Archives Act.

Accessibility requirements apply to all digital records, not just those of archival value. Digital records must remain accessible for as long as they are required (see 6 – Determining how long to keep digital records).

10.2 Planning for technological obsolescence

Digital records are dependent on various combinations of hardware, software and media to retain their content, context and structure. Agencies must ensure that the technology required to render a digital record usable and accessible is available. It is not sufficient to simply retain records in digital format; the records and associated metadata must be in a format that is viewable with current technology.

Computer technology is subject to ongoing technological obsolescence, with both hardware and software quickly becoming outdated as new upgrades and versions come onto the market. This can result in digital records created using older hardware and software becoming inaccessible in their original form after a relatively short period of time.

Agencies that need to retain digital records for the long term should plan for technological obsolescence by ensuring that records can be copied, reformatted, converted or migrated across successive generations of computer technology (see 10.4). Such planning involves considering hardware, software, operating systems and storage devices.

Agencies need to consider a number of interrelated software and hardware issues when preserving digital records, including:

- the proprietary, platform-specific nature of many software applications and the likelihood of their continued availability;
- the cost of maintaining access to obsolete formats (including operating system software and licensing fees) for a system no longer in active use;
- the estimated physical and/or commercial life of the media on which digital records and related metadata are stored; and
- the long-term availability of the hardware and operating system platforms needed to access records stored on different types of media.

The need to plan for technological obsolescence and provide for the preservation of digital records should be incorporated, through a formal digital records preservation strategy, within the digital recordkeeping framework (see Figure 1 in section 3). The preservation strategy should outline the approach adopted by the agency for the preservation of its digital records. There are several common techniques (see 10.4).

10.3 Creating a digital records preservation strategy

In order to adequately manage the preservation of digital records over time, and ensure their continued accessibility, Australian Government agencies must be proactive. They should develop and implement organisation-wide strategies targeted at identifying, managing, preserving, and ensuring continued access to digital records.

An effective digital records preservation strategy should incorporate formal policies and procedures governing the agency's approach to the long-term management of its digital records and establish processes to ensure their ongoing maintenance.

An agency's digital records preservation strategy must reflect its legislative obligations, industry standards and best practice (see 2.2.2 – Accountability, community expectations and best practice). The tools listed at the end of this chapter will be especially helpful to agencies formulating a digital records preservation strategy.

A digital records preservation strategy should be supported by a plan for its implementation that is promulgated to relevant staff. This can be achieved by:

- formulating policies, procedures and guidelines to provide a formal framework within the organisation for the implementation of the strategy; and
- providing manuals, information and reference sheets, and training for staff to ensure the preservation strategy is correctly implemented. Depending on the

approach adopted, this may require training for all operational areas, not simply for records and IT staff.

Agencies should assign responsibility for the management of long-term digital records to an appropriate area within the organisation where staff have relevant skills and qualifications. This will generally be a specialised information or knowledge management unit headed by a senior information officer (see 3.5 – Roles and responsibilities). Responsibility for policy and procedure formulation, implementation of strategies to preserve digital records, evaluation, monitoring and review of processes, and delivery of training should rest with this area.

Agencies should ensure that their digital records preservation strategy takes into account digital records that may be created and managed by outsource providers and that these contractors are also required to actively comply with the agency's long-term digital records preservation strategy (see 3.8 – Records created outside agency systems).

10.4 Techniques for digital records preservation

Some early approaches to digital records preservation relied on storing records in their original format on physical media – much like boxes are used for the storage and protection of paper records. However, magnetic tapes and disks, and optical storage disks (eg CDs and DVDs) are manufactured for short-term storage of digital objects, not long-term archival retention. The greatest concern for this method of preservation, in addition to the relatively short life span of digital media, is the obsolescence of the hardware and software used to access the records. Rapid change in the IT industry and the move from science-based development to commercial development of software and hardware systems, has meant that media rapidly become inaccessible. Consequently, this approach to digital preservation has proven to be wholly inadequate and the National Archives strongly advises against this preservation strategy.

The most common techniques for digital preservation can be grouped into three broad categories. Any one or a combination of these may form the basis for an agency's digital records preservation strategy.

10.4.1 Migration

Migration relies on a program of constant transferral (migration) of digital records from older or obsolete hardware and software configurations or generations, to current configurations or generations in order to maintain accessibility. This strategy avoids the obsolescence issues of the physical media solution, preserving the functionality of the digital records and enabling users to retain access to the records – but requires a substantial investment in resources to undertake the repetitive migration work involved. Furthermore, some characteristics of the original data format may not be retained through the migration process and, as a result, users will lose access to characteristics of the source record that may be important to its meaning.

Conversion

Conversion is the process of transferring digital records from their original data format to a standardised, long-term preservation format (also known as an archival data format). Conversion is also referred to as 'normalisation', 'stabilisation' and 'standardisation'.

The conversion process is a form of migration. However, instead of migrating from an outmoded data format to a current data format, the original data format is migrated to an archival data format. Generally, archival data formats are open source, non-proprietary formats that provide greater potential longevity and are less restrictive than proprietary formats. Conversion reduces the need for repeated migrations.

10.4.2 Encapsulation

Encapsulation requires metadata to be bundled with, or embedded into, the digital object. The metadata allows the record to be intellectually understood and technologically accessed in the future.[8] A viewer is then required to display the records. This packaging of contextual information ensures the integrity and authenticity of records over time. However, there is some risk that important metadata may be overlooked during encapsulation.

On its own, encapsulation cannot preserve digital records. This technique should be used in conjunction with migration or emulation to ensure the ongoing accessibility of the records.

10.4.3 Emulation

Emulation uses software to recreate the digital record's original operating environment to enable the original performance of the software to be recreated on current computer systems. The result is that the original data format is preserved and may be accessed in an environment that allows for the recreation of the original 'look and feel' of the record. The downside to the emulation approach is that the creation of the underlying emulator software is costly, requiring highly skilled computer programmers to write the necessary code. Furthermore, the intellectual property and copyright issues associated with the emulation of proprietary software may undermine the effectiveness and sustainability of the approach.

The National Archives approach to digital preservation uses a combination of these techniques (see 10.6).

10.4.4 Further information

Further information on the advantages and disadvantages of the techniques described above can be found in the National Archives green paper, *An Approach to the Preservation of Digital Records*, the National Archives *Digital Records Bibliography* and the National Library's *Preserving Access to Digital Information*.

10.5 Implementing a digital records preservation strategy

Whatever strategy an agency adopts to keep digital records accessible, it must address a number of common issues.

10.5.1 Choosing an approach to digital records preservation

Australian Government agencies should consider the following factors when choosing an approach to digital records preservation:

- cost of implementation, including cyclical costs for ongoing preservation treatments;

[8] Justine Heazlewood, 'Management of electronic records over time', *Selected Essays in Electronic Recordkeeping in Australia*, Australian Society of Archivists, 2000.

- technical complexity of the selected approach and the capacity of the agency to support the approach over time (both technically and financially);
- compatibility with existing hardware and software;
- impact on business operations (eg whether the approach requires changing corporate work practices); and
- overall effectiveness and robustness of the approach in protecting the integrity, accessibility and functionality of the agency's digital records over time.

10.5.2 When should a digital preservation treatment be applied?

To maximise the long-term preservation prospects for digital records, preservation techniques must be applied as soon as practical, preferably while the records are still accessible. Most data formats have a limited window of opportunity during which preservation treatments can be applied before the format becomes outmoded and inaccessible. The sooner an agency addresses preservation issues and determines and implements an appropriate preservation approach, the higher the probability that the digital records will be successfully preserved.

Agencies are therefore encouraged to be proactive in pursuing their digital preservation strategies and to determine and implement appropriate digital preservation techniques before their digital records become outmoded and inaccessible.

Preservation treatments are often undertaken reactively in response to the immediate business needs of an organisation, rather than as part of a considered solution to long-term digital records retention requirements. Such processes may be technology-driven exercises, initiated in response to changes in IT infrastructure or as a consequence of adopting new or upgraded software. In such cases, preservation treatments are undertaken primarily to ensure that existing digital records, particularly active core business records, are transferred from their original format into a new format capable of functioning within the upgraded IT environment.

10.5.3 Planning to implement a preservation strategy

Periodic preservation treatments (such as migration) are often applied to digital records without necessarily considering the long-term implications for the integrity of the records. If sufficient care is not taken to protect the integrity and authenticity of the records, migrating software and hardware systems can jeopardise their evidential value.

Agencies that apply preservation treatments to data formats without properly assessing the processes, risk the loss or limitation of the functionality, format, structure and content of their digital records and the potential loss of metadata relating to the records.

Planning for the preservation of digital records will allow agencies to retain the functionality and integrity of digital records after successive upgrades of hardware and software.

Development of preservation strategies, and the selection of an appropriate approach, should be the result of a collaborative effort between the records and IT sections within an agency (see 3.5 – Roles and responsibilities). Best practice recordkeeping issues need to be carefully considered, and the input of agency records and information personnel taken into account, before any preservation processes are applied to an agency's digital records.

10.5.4 Implementing the preservation strategy

Although the three main preservation techniques – migration, encapsulation and emulation – differ substantially in their method of preserving digital records, they share common ground in the process of implementation. The following steps outline the implementation process.

1. **Identify records requiring preservation** – Identify and select digital records that require the application of preservation treatments in order to ensure their continued accessibility.

2. **Research technical solutions** – Investigate the hardware and software technologies required to successfully implement the agency's preferred preservation approach. In the case of emulation, this may involve the development of specialised software capable of re-creating the source records within a new computer environment. In the case of migration, this may involve identifying suitable migration paths (ie software applications with sufficient backward compatibility to transfer source records from an outmoded data format to a current data format). In the case of encapsulation, this may involve software with the ability to embed metadata or 'package' it with the record.

3. **Test proposed solution** – Before a preservation approach is fully implemented, agency staff must conduct comprehensive testing of the technical processes. Testing should be performed on duplicates of source records.

4. **Back up records identified for preservation** – Prior to implementation, all digital records identified for preservation treatment should be backed up. The integrity of the duplicates should be verified before they are removed to a secure storage area. These duplicate source records should not be subjected to a preservation process and will serve as master copies should the selected preservation treatment be unsuccessful.

5. **Apply the preservation treatment** – After successful testing, the treatment should be applied to all digital records identified for preservation treatment. For migration and encapsulation techniques, this would entail applying preservation treatments to the source records, thereby altering their format. For an emulation-based technique, the records identified for preservation would be transferred to the new environment – without altering the records themselves.

6. **Audit the integrity of preserved records** – Following implementation of the preservation process, the preserved records should be subjected to rigorous testing to ensure that any reduction in functionality, or loss of content, structure or format, is within previously set limits of acceptability. The integrity of all relevant metadata associated with the preserved records should be verified. Metadata should also be updated to record the preservation treatment.

If the records cannot be verified, the preservation process will need to be repeated on new duplicates of the source records (steps 4 to 6). In some instances, the preservation strategy itself may require re-evaluation.

7. **Destroy source records where appropriate** – Once the preservation process has been completed and the integrity of the preserved records has been verified, agencies may destroy the duplicate source records as long as they meet the requirements set out within the *General Disposal Authority for Source Records that have been Copied, Converted or Migrated* or specific disposal authorisation obtained from the Archives.

8. **Establish monitoring regimes** – The integrity of the preserved records, their functionality, structure, content and context, and associated metadata, should be monitored periodically following preservation to ensure the stability of the preserved records and to identify when subsequent preservation treatments are required.

Please note that, if it appears likely at any stage during the application of a preservation treatment that digital records of archival value may be lost or significantly altered as a result of the preservation process, the Archives should be consulted immediately so that alternative arrangements may be considered.

The National Archives' *Recordkeeping Metadata Standard for Commonwealth Agencies* specifies the metadata that should be kept to document the preservation actions that have been applied to digital records.

Agencies experiencing significant difficulty in ensuring the continued accessibility of their digital records should contact the National Archives for advice.

10.5.5 Requirements for a successful preservation strategy

A successful preservation strategy ensures the continued integrity of the digital records, as well as their continued accessibility and functionality. The preservation of integrity requires that the records, and their associated metadata, remain reliable, complete and authentic.

The following steps will ensure successful preservation of digital records.

- Care is taken in selecting and testing software applications and hardware required for preservation processes.
- Where possible, non-proprietary, fully documented, open source data formats are used – particularly when implementing migration-based preservation techniques. Proprietary data formats are not recommended for long-term storage of records.
- Preservation processes are applied systematically to all digital records, both current and non-current, retained by an agency. Failure to include non-current digital records can result in their inaccessibility.
- All relevant metadata (for the records and the preservation process) is captured at the time of preservation.
- Preservation processes are fully documented and the documentation retained to help inform future preservation efforts. Any copying or reformatting of data for migration or conversion should be documented in the recordkeeping metadata.
- Preservation processes are carried out in accordance with relevant recognised recordkeeping, information and data management standards.
- Guidelines and procedures are issued and staff are encouraged to adopt common usage rules to help standardise the application of the selected techniques across all agency systems.

- Where records are migrated, converted, copied or reformatted, the success of the process must be verified and data integrity confirmed before the duplicate source records are destroyed (see also *General Disposal Authority for Source Records that have been Copied, Converted or Migrated*).
- Any alteration or loss of functionality, structure, content or appearance that occurs as a result of preservation is fully documented in the recordkeeping metadata.
- Thorough checking regimes are put in place following preservation to monitor record integrity and identify when further preservation treatments are required.

10.6 The National Archives approach to digital preservation

Preservation strategies involving migration, encapsulation and emulation of digital records are all effective and reasonable paths to maintain records that are active and regularly required for business and administrative purposes. These processes can maintain the integrity and accessibility of digital records to ensure that developments in technology do not render digital records inaccessible. Digital records requiring long-term maintenance need to be actively managed in a planned, systematic and documented strategy.

The National Archives approach to the preservation of digital records is based on a combination of these techniques – conversion, encapsulation and emulation.

Digital records are converted or 'normalised' using archival data formats. The archival data formats use XML (eXtensible Markup Language) standard schemas. XML provides a standard syntax to identify parts of a document (known as elements), and a standard way (known as a schema) to describe the rules for how those elements can be linked together in a document.

Metadata is encapsulated within the preserved data object, and the whole package is stored in a digital repository. A special viewing tool makes the packages accessible using a form of emulation.

This approach allows the 'essence' of the record to be captured in a format that can be re-created as required and preserved over time.

The concept of 'essence' is central to the National Archives digital preservation approach. 'Essence' refers to the essential characteristics that give a record its meaning. These characteristics include the format, structure, content and context, as well as the overall 'look and feel' of a record.

This approach can be implemented regardless of the system from which the digital records were derived. It works for records in any format for which an archival data format has been developed (referred to as XML normalisers). Current formats include email, proprietary word-processed documents, datasets, images and plain text.

The National Archives approach is compatible with migrating records across platforms – records do not need to be in their native formats (ie their original pre-migration data formats) in order to be converted to an archival data format. However, digital records of archival value need to be converted to accessible data structures before their native formats become obsolete. Once original data formats are outmoded, there is a substantially increased risk that it may not be possible to normalise the records into archival data formats.

The process of emulating digital records is also compatible with the National Archives digital preservation approach, since the emulation process retains the digital records in their original data format. As long as the records remain accessible in their original format, conversion to archival data formats should be possible.

For more information on maintaining and preserving digital records, and advice on developing digital records preservation strategies, see the National Archives Digital Preservation web page. For more information about the National Archives approach to digital preservation, refer to the green paper on digital preservation.

Where to from here?

Evaluate your agency's preservation of digital records using the Digital Recordkeeping Checklist, section 10.

Improve your agency's preservation of digital records according to the advice in this section. The following products will assist:

- *Australian Standard for Records Management*, AS ISO 15489
- *DIRKS: A Strategic Approach to Managing Business Information* (see below for relevant pathway)
- *Recordkeeping Metadata Standard for Commonwealth Agencies*
- *An Approach to the Preservation of Digital Records*
- *Preserving Access to Digital Information*

Pathway through DIRKS

- Use Step C to determine how long records are required. This is the basis for developing a preservation strategy.
- Use Step D to determine whether existing systems have the capacity to preserve digital records for as long as they are required.
- Use Step E to develop a planned, systematic approach to the preservation of records and management of technological obsolescence. This step can help identify tactics to satisfy recordkeeping requirements and meet organisational constraints.
- Use Appendixes 10 and Appendix 12 to develop a preservation strategy using cost-benefit and feasibility analysis. These appendixes explain how these forms of analysis can be applied to recordkeeping.

11. PROVIDING ACCESS TO DIGITAL RECORDS

Key points

- The National Archives will provide access to digital records of archival value in its custody (11.1).
- Australian Government agencies must provide secure access to digital records in their custody, in accordance with legislative requirements (11.2).

11.1 Access to digital records in Archives custody

11.1.1 Public access to records in Archives custody

In accordance with section 31 of the *Archives Act 1983*, the public has a general right of access to Commonwealth records that are more than 30 years old, regardless of their location or format. Subject to certain exemptions, members of the public are entitled to access open period records (records older than 30 years), whether they are in the custody of the Archives, an agency or an outsource provider.

Digital Commonwealth records in the National Archives custody will be accessible in a variety of ways. They may be accessible via online computer terminals in reading rooms, and via the website. Accessing digital records in our holdings will be similar to the current method of accessing digitised copies of paper-based records.

11.1.2 Agency and official access to records in Archives custody

The Archives will continue to facilitate access by agencies to records that have been transferred into its custody. Agencies may authorise staff or other people (eg consultants) to view such records.

11.2 Providing access to digital records in agency custody

Records retained by agencies for more than 30 years to meet business, legal or evidentiary purposes are subject to the access provisions of the Archives Act. Requests for access to records under the Archives Act should be referred to the National Archives in the first instance.

Further information on access to Commonwealth records is available from Fact Sheet 10 – Access to records under the Archives Act.

Digital records held by Australian Government agencies are also subject to the *Freedom of Information Act 1982* and *Privacy Act 1988*.

To meet these legislative requirements, Australian Government agencies should ensure that they are able, at any time, to provide access to digital records in a usable form.

11.2.1 Responsibilities of Australian Government agencies

For agencies to meet their legislative obligations, their digital records must remain accessible and usable, with the necessary infrastructure to meet public and official access demands. For long-term digital records, it will be necessary to apply appropriate preservation strategies to enable continued access to the records (see 10 – Preserving digital records for the long term). Agencies are also required to identify and retain appropriate metadata for digital records.

To meet their access obligations, Australian Government agencies need to:

- understand the access provisions of the *Archives Act 1983*, *Freedom of Information Act 1982* and the *Privacy Act 1988*;
- identify which records are 30 years old and document how the age of records is calculated;
- nominate staff able to liaise with the Archives, as well as officials and the public;
- provide copies of, or electronic access to, digital records; and
- keep a record of the access process.

11.2.2 Provision of secure access to digital records

When providing access to digital records, agencies should take appropriate precautions to ensure their security, integrity and authenticity. Like records on paper or any other medium, digital records need to be protected from unauthorised alteration. As such, procedures should be established to supervise access to digital records.

To avoid any compromise of the security, integrity and functioning of an agency's digital recordkeeping system, the Archives recommends that access is not given to the live system, but rather to a clone or parallel system, or to copies of the records. Any sensitive or classified records should be appropriately expunged or made unavailable for access, in accordance with legislative requirements.

If agencies are unable to provide properly supervised access to digital records, they should seek further advice from the National Archives.

11.2.3 Determining when a digital record can be open for access

Agencies need to be able to determine the age of a record to determine which access regime applies – the *Freedom of Information Act 1982* or the *Archives Act 1983*. Commonwealth records are subject to the Archives Act once they are more than 30 years old.

For the purposes of determining the age of a particular digital record, the date of creation is the date from which to measure the age of the record. Updating a digital record (eg saving, refreshing or migrating) does not impact on the 30-year countdown. In cases where the original transactions occurred on earlier electronic or manual systems, the date of first creation should be used rather than the date of transfer onto the current system.

Full and accurate metadata documenting dates for the creation, modification and preservation (eg migration or conversion) of digital records will assist in determining the age and integrity of long-term digital records.

Where there is doubt over the appropriate age determination of digital records for access purposes, agencies should seek National Archives advice.

Where to from here?

Evaluate your agency's arrangements for providing access to digital records using the Digital Recordkeeping Checklist, section 11.

Improve your agency's arrangements for providing access to digital records according to the advice in this section. The following products will assist:

- Fact Sheet 10 – Access to records under the Archives Act
- *DIRKS: A Strategic Approach to Managing Business Information* (see below for relevant pathway)

Pathway through DIRKS

- Use Step C to identify requirements for access to records to meet business needs, legal and regulatory obligations, and community expectations.
- Use Step D to measure a system's ability to support retrieval tools (such as a thesaurus). Agencies can also evaluate whether systems can maintain the accessibility of digital records for as long as they are required.
- Use Step E to develop strategies for providing access to digital records to staff, the public, other interested parties, such as auditors, and to meet the requirements of legal discovery.
- Use Step F and Step G to produce specifications for systems that provide access to digital records, in accordance with legislative obligations.
- Use Step H to provide objective proof that a system meets requirements for ongoing public access to government records.

12. DISPOSING OF DIGITAL RECORDS

Key points

- In addition to destruction, disposing of digital records can involve transferring records to the Archives or another organisation (12.1).
- Disposal of Commonwealth records is authorised by the National Archives (12.1).
- There are requirements for transferring digital records of archival value to the National Archives (12.2).
- When digital records are transferred between agencies, the receiving agency assumes responsibility for their ongoing preservation and accessibility (12.3).
- Digital records of temporary value should be destroyed securely and in such a way that they cannot be reconstructed (12.4).
- Digital records to be retained indefinitely by the agency should be preserved and their ongoing accessibility ensured (12.5).

12.1 Methods of disposing of digital records

There are three lawful ways to dispose of digital records:

- transfer digital records of archival value to the National Archives once they are no longer required for agency business purposes (see 12.2);
- transfer digital records to another organisation as a result of a change in government administrative arrangements, such as the privatisation or redistribution of business functions (see 12.3); and
- destroy digital records of temporary value once their minimum retention period has expired (most digital records are of temporary value) (see 12.4).

Some digital records may need to be retained by the agency permanently. These records are not of archival value and, therefore, cannot be transferred to the National Archives. However, they must be preserved and remain accessible (see 12.5).

Disposal of Commonwealth records and associated metadata is approved by the National Archives under section 24 of the *Archives Act 1983* in a disposal authority (see 6 – Determining how long to keep digital records).

Metadata should be retained for digital records that have been destroyed or transferred (see 6 – Determining how long to keep digital records). More advice can be found in the *Recordkeeping Metadata Standard for Commonwealth Agencies*.

12.1.1 Disposal in digital systems

Recordkeeping systems should be able to manage disposal with some degree of automation. Achieving this requires some forethought in relation to system design and the development of the agency's records disposal authority.

Automation is only possible when a disposal action is linked to an event that takes place within the system. For example, disposal may be triggered 10 years after a file is closed. The system has access to metadata about date of closure, and can dispose of the file automatically. Business rules can ensure that files are closed on a certain date (such as end of financial year), or when they reach a certain capacity.

In some cases, the system relies on the manual entry of metadata to trigger disposal. For example, if a superseded policy is to be disposed of ten years after the date on which it was superseded, then staff must mark it as superseded as soon as the new policy is developed. Such tasks may be easily overlooked, resulting in a backlog of records past their disposal date.

Coordination between records managers and systems designers will allow disposal of digital records to be managed efficiently and with minimal intervention. Automating this process in systems with full recordkeeping functionality is the most effective way to demonstrate accountable disposal. Such systems will generate audit trails and metadata as evidence that records are managed in accordance with relevant disposal authorities.

12.2 Transferring digital records to the National Archives

The National Archives is currently developing processes for the transfer of archival digital records to its custody. These will be based on existing procedures for the transfer of non-digital records. More information can be found on the Transfer page of the website at www.naa.gov.au/recordkeeping/disposal/transfer/transfer.html

12.3 Transferring digital records between agencies

Periodic changes to the administrative arrangements of the Australian Government, such as the privatisation of Australian Government agencies or the redistribution of government functions between agencies, often create circumstances where Commonwealth records are transferred from the controlling agency to another organisation.

Transferring the custody or ownership of Commonwealth records to an organisation outside the Australian Government is authorised by the National Archives in accordance with section 24 of the *Archives Act 1983.*

Advice on transferring records between Australian Government agencies can be found in Archives Advice 27 – Handling administrative change.

When digital records are transferred from one agency to another, the relinquishing agency should transfer the digital records, and their associated metadata, in data formats that are accessible and functional for the receiving agency.

The receiving agency inherits the responsibility of managing, preserving, and providing access to the digital records. The agency, therefore, needs to ensure that it receives adequate system documentation and metadata along with the digital records.

If the relinquishing agency retains any copies of transferred records, the metadata for those copies should reflect the details of their transfer. Transferred files or containers should be closed, so that no more records can be added.

12.4 Destruction of digital records

Most digital records created and maintained by Australian Government agencies are of temporary value and may be destroyed when they reach the minimum retention period specified within the agency's approved records disposal authority. Some records can be routinely destroyed in the normal course of business (see 6.4 – Normal administrative practice).

Destruction of digital records involves ensuring that the record cannot be reconstructed.

Most temporary digital records will be required for relatively short retention periods and will not require preservation treatments – such as migration – to ensure their continued accessibility. Temporary digital records that need to be retained for longer periods of time may need preservation treatments to ensure their accessibility until they can be destroyed. Given the vulnerability of digital records, preservation treatments should usually be applied to records more than five years old.

12.4.1 Deletion is not destruction

In electronic systems, records are not destroyed when they are 'deleted'. What is destroyed is the pointer to the record (eg the file name and directory path) that tells the operating system where a particular piece of data is held on the medium.

The actual data objects are gradually overwritten in time by new data. However, until the data is completely overwritten there remains a possibility that the information can be retrieved.

'Deletion' does not meet the requirements for destruction of Commonwealth records.

12.4.2 Methods of destroying digital records

Disposal mechanisms should ensure the effective destruction of data. Such mechanisms include digital file shredding, degaussing (ie the process of demagnetising magnetic media to erase recorded data) and physical destruction of storage media (eg pulverisation, incineration or shredding). Reformatting may also be used as a method of destruction if it can be guaranteed that the process cannot be reversed.

To ensure the complete destruction of a digital record, all extant copies should be located and destroyed. This includes removing and destroying copies contained in system backups and offsite storage.

More information on appropriate methods of destruction for digital records and associated media formats can be obtained from the *Commonwealth Protective Security Manual* and *Australian Government Information Technology Security Manual* (ACSI 33).

12.5 Retaining digital records permanently within agencies

Some digital records are identified for permanent retention within the agency. Maintaining these records indefinitely and accessibly is the responsibility of the agency.

Agencies will determine their own approach to the long-term preservation of these digital records, although the Archives recommends its own digital preservation approach (see 10.6 – The National Archives approach to digital preservation).

12.5.1 Retaining archival value digital records in agency custody

In some circumstances, the Archives may ask agencies to retain archival value digital records rather than transfer them to the Archives. This will usually occur in cases where Archives staff believe that the best prospect for preserving access to those records is to retain them within their original technological environment.

Digital records of archival value to be retained in the physical possession of agencies remain subject to the *Archives Act 1983* (see 11 – Providing access to digital records). The National Archives will still be responsible for registering and describing the records in its control systems.

Where to from here?

Evaluate your agency's disposal of digital records using the Digital Recordkeeping Checklist, section 12.

Improve your agency's disposal of digital records according to the advice in this section. The following products will assist:

- *DIRKS: A Strategic Approach to Managing Business Information* (see below for relevant pathway)
- Archives Advice 27 – Handling administrative change
- *Australian Government Information Technology Security Manual* (ACSI 33).
- *Commonwealth Protective Security Manual*

Pathway through DIRKS

- Use Step A, Step B, Step C and Appendix 8 to develop a records disposal authority based on identified requirements for records.
- Use Step D to measure a system's ability to dispose of records in accordance with legal requirements.
- Use Step E to develop strategies for disposing of, and transferring, records.

13. MANAGING SOME COMMON TYPES OF DIGITAL RECORDS

Key points

- Electronic messages are communications made using electronic systems. They can occur in a variety of forms (13.1.1).
- Electronic messages can be digital records (13.1.2).
- Messaging system management tools should be used appropriately to ensure digital records are not affected (13.1.3).
- New formats of electronic messages, and new software, are emerging rapidly. Australian Government agencies should be aware of the recordkeeping implications (13.1.4).
- National Archives has produced a policy and guidelines to assist Australian Government agencies to manage web-based digital records (13.2).
- National Archives has produced guidelines to assist Australian Government agencies to manage records subject to online security processes (13.3).
- Agencies should seek National Archives advice on managing records in business systems that are outside the scope of these guidelines (13.4).

13.1 Electronic messages

Capturing electronic messages into agency recordkeeping systems, and managing them as records over time, presents a series of challenges that are unique to this particular type of digital record.

Please note that storing electronic messages in email folders does not constitute 'capture' into a corporate recordkeeping system (see 4 – Creating digital records).

This section provides advice only on issues specific to electronic messages and should be read in conjunction with the general principles provided in these guidelines.

13.1.1 What are electronic messages?

An electronic message is any communication made using an electronic system. Electronic messages can occur in a range of forms, including:

- electronic mail (email)
- electronic document exchange (electronic fax)
- electronic data interchange (EDI)
- voice mail
- instant messaging
- short messaging services (SMS)
- enhanced messaging services (EMS)
- multimedia messaging services (MMS)
- multimedia communications, eg teleconferencing and video-conferencing.

13.1.2 Which electronic messages are records?

Electronic messages sent or received in the performance of an agency's business are records. Examples of electronic messages that are records include a directive or an approval for a particular course of action, an interchange of messages about a case or policy issue, or data interchange with another agency.

Agency staff will also receive information messages with a business context – eg unsolicited advertising material for training courses – and private messages unrelated to the agency's business. These messages are not records.

For further information, see Archives Advice 20 – Email is a record!

13.1.3 Messaging system management tools

There are many systems management tools designed to deal with problems such as storage limitations, nuisance and unsolicited messages and the ever present threat of computer viruses. These administrative tools may either be built into electronic messaging system software or provided through third party applications. Most electronic messaging systems software allows a degree of configuration, allowing agency staff to control and limit how the system operates.

The following are examples of common practices employed for managing electronic messaging systems that may impact on compliance with recordkeeping requirements.

Blind carbon copies (BCC)

Electronic messaging systems are often configured to hide blind carbon copy (BCC) address information. As a result, BCCs may not be included when a message is captured into a recordkeeping system or displayed when a message is printed. The sender of a message needs to ensure that all recipient details, including BCC recipients, are captured into the recordkeeping system.

All relevant metadata for digital records needs to be captured into the recordkeeping system. This includes BCC information for emails sent by the agency. Therefore, special care should be taken to configure both recordkeeping and electronic messaging systems to allow this.

Message recall

The Archives does not encourage the use of email recall functionality. However, if agencies opt to implement this functionality, a record must be kept of the original message, the recall notification, and the reason for recalling the email.

Systems should be configured so that when emails are retrieved an automatic notification of recall is sent to the recipient to advise of the recall. Agencies should configure systems so that emails received from external sources cannot be recalled by the sender.

Mailbox size limitations

Many agencies impose limitations on the message capacity of user mailboxes, thereby forcing staff to delete older messages in order to be able to send new messages. This practice limits the use of storage space in the message system and encourages staff to keep only relevant messages. However, it can also encourage the deletion of messages that should be kept as records of business activity. This may constitute unauthorised disposal (see 6 – Determining how long to keep digital records).

The imposition of mailbox size limits should always be accompanied by sound message management policies and an emphasis on user training to ensure that messages providing evidence of business activity are captured into a corporate recordkeeping system and not simply deleted. Staff should be encouraged to file emails into the recordkeeping system as a routine practice and not simply do so when reaching their mailbox size limit.

Message size limitations

Another common limitation placed on messaging systems is the capping of the maximum size for messages that may be sent or received. The implementation of message size limitations varies between systems. In some cases, messages may simply be rejected by the agency messaging system and returned to the sender. In other cases, messages may be held on the agency's system and a special arrangement made with the intended recipient for receipt of the message.

If agencies document their policies and procedures for message size limitations, they can dispose of these messages under the provisions for normal administrative practice (see 6.4 – Normal administrative practice). Comprehensive audit logs that detail all messages automatically rejected by the system should also be maintained. Ideally, systems that automatically prevent the delivery of over-sized messages should incorporate processes to notify both the sender and the intended recipient that the message was unable to be accepted.

The practice of automatically rejecting and deleting oversized messages from messaging systems is not encouraged as there is a risk that business related messages may be inadvertently lost.

Messaging system maintenance

In order to clear storage space within messaging systems and improve system performance, the maintenance of messaging systems may be automated. It is possible to delete all messages that have been on the system for a specified period of time, or to move older messages to offline or nearline storage. But it is important to consider the content of the messages being moved or deleted, and whether the records have been captured.

Automatically deleting messages is not sound recordkeeping practice. There is considerable risk of losing valid business messages, ie records. At the least, a check should be performed, prior to deletion, to ensure that the affected messages have been captured into the agency's recordkeeping system.

Improved staff training and tighter controls and policies for filing of messages are preferable strategies for reducing strain on messaging systems.

Gateway filter software

Gateway filter software provides essential security for messaging systems and preserves systems integrity and efficiency. The software analyses the header and content of messages upon receipt and filters out unsolicited and virus-infected messages, thus preventing their entry into the agency network and protecting against potential denial of service attacks. Messages identified as unwanted are then deleted automatically. This function may be performed by dedicated third party software applications, such as virus scanners and 'spam' filter programs or may be incorporated into the agency's messaging system.

The parameters of all filters should be carefully documented with measures to guarantee delivery of valid business related messages. Thorough documentation should be retained for accountability and audit purposes, to demonstrate the types of messages that may be blocked.

Digital rights management software

Some electronic messaging applications offer a level of server-client integration that allows the sender to place restrictions on who can view, print, forward, copy or edit messages. These restrictions can include the automated self-deletion of email – ie the sender of an email can stipulate the lifespan of a message and force the deletion of the message from the system at a predetermined time. Automatic deletion of messages in this manner may constitute unauthorised disposal (see 6 – Determining how long to keep digital records).

Only staff within an agency that have responsibility for, and expertise in, the management of records should restrict access to, or delete, records from within a recordkeeping system (see 8.5 – Long-term digital records). In this way, agencies can ensure compliance with all relevant legislation and recordkeeping requirements.

The National Archives does not endorse the use of digital rights management systems to enable the automatic deletion of electronic messages, or to place any other restrictions on messages that may impede corporate recordkeeping practices. Australian Government agencies are advised not to use this functionality.

Appropriate use of messaging system management tools

Agency staff should carefully review any software that may block, delete or otherwise alter business related messages received by the agency's messaging system. Procedures and policies for such software should be well documented.

In order to meet accountability and audit expectations, system log files should be kept. They should record information about all messages deleted from a messaging system, particularly where messages are not delivered to the recipient. These log files should be managed according to the general advice in these guidelines.

Before they can be legally deleted from a messaging system, messages must be captured into a recordkeeping system, or meet the requirements of normal administrative practice or a disposal authority (see 6 – Determining how long to keep digital records).

13.1.4 Emerging technologies

Email currently represents the dominant electronic message format used in business. But agencies should note the emergence of alternative electronic message formats, such as instant messaging, SMS and MMS. These new messaging systems are often more flexible than email and tend to be more ephemeral in nature. Yet they are still electronic messages and as such have the potential to be Commonwealth records (see 13.1.2).

Personnel with responsibility for digital recordkeeping are advised to be aware of the uptake and usage of new electronic message formats by their agency's staff and to take steps, as necessary, to develop and implement policies, procedures and practices to ensure that any resulting digital records are treated appropriately.

13.2 Web-based digital records

Australian Government agencies are generating an increasing proportion of business records through web-based resources and online activities. A number of standards and best practice requirements apply to web-based records.

The National Archives has produced the *Archiving Web Resources* policy and guidelines to assist Australian Government agencies.

13.3 Records subject to online security processes

With an increasing use of computer-based commerce, there is a need to ensure that records transmitted across insecure networks such as the Internet are authentic, reliable and accessible. Online security processes, such as authentication and encryption, provide those guarantees.

The National Archives has produced *Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received using Authentication and Encryption* to assist agencies to effectively manage these records.

13.4 Records in business information systems

Records created or stored in business information systems are subject to the same legal requirements as other government records. They should be managed in accordance with the general advice contained in these guidelines.

Business information systems include (but are not limited to):

- databases
- geospatial data systems
- human resources systems
- financial systems
- client management systems
- customer relationship management systems
- workflow systems
- systems developed in-house

These systems may not have recordkeeping capability (see 4.4 – Business information systems not designed to keep records).

Agencies should seek National Archives advice on managing records in business information systems that are outside the scope of these guidelines.

Where to from here?

Evaluate your agency's management of some common types of digital records using the Digital Recordkeeping Checklist, section 13.

Improve your agency's management of some common types of digital records according to the advice in this section. The following *e-permanence* products will assist:

- Archives Advice 20 – Email is a record!
- *Archiving Web Resources Policy*
- *Archiving Web Resources Guidelines*
- *Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received using Authentication and Encryption*

APPENDIXES

Glossary

The following are some key definitions for terms used in these guidelines. Please note that certain words are used differently in the information technology (IT) and archives/records management fields. Terminology used in this document refers to the archives/records management sense of the words.

Archives – Records that are appraised as having archival value.[9] Note: This definition of the term differs to the IT sphere where it refers to 'a copy of one or more files or a copy of a database that is saved for future reference or for recovery purposes in case the original data is damaged or lost.'[10]

Archival data format – A format into which digital data objects are converted for long-term preservation.

Archival value records – Records appraised as satisfying the Archives criteria for indefinite preservation. These records are also referred to as 'retain as national archives' (RNA).

Business information system – Organised collection of hardware, software, supplies, policies, procedures and people, which stores, processes and provides access to an organisation's business information.[11]

Capture – The process of lodging a document into a recordkeeping system and assigning metadata to describe the record and place it in context, thus allowing the appropriate management of the record over time.

Checksum – An algorithm-based method of determining the integrity and authenticity of a digital data object. Used to check whether errors or alterations have occurred during the transmission or storage of a data object.

Commonwealth record – A record that is the property of the Commonwealth or a Commonwealth institution.

Content – That which conveys information, eg text, data, symbols, numerals, images, sound and vision.

Context – The background information that enhances understanding of technical and business environments to which the records relate, eg metadata, application software, logical business models, and the provenance (ie address, title, link to function or activity, agency, program or section).

[9] J Ellis (ed.), *Keeping Archives*, 2nd edition, Australian Society of Archivists, Thorpe, Melbourne, 1993, p. 463.

[10] *IBM Dictionary of Computing*, McGraw Hill, New York, 1994, p. 30.

[11] Adapted from Standards Australia, *Records Management Standard*, AS 4390 – 1996, Part 1, 4.17.

Conversion – Process of changing records from one medium to another or from one format to another. Conversion involves a change of the format of the record but ensures that the record retains the identical primary information (content).[12]

Data – Facts or instructions represented in a formalised manner, suitable for transmission, interpretation or processing manually or automatically.[13]

Digital record – A record created and/or maintained by means of digital computer technology. Digital records are a subset of electronic records.

Digital signature – A security mechanism included within a digital object that enables the identification of the creator of the digital object, and that can also be used to detect and track any changes that have been made to the digital object.[14]

Document – Recorded information or object which can be treated as a unit.[15]

Electronic document management system (EDMS) – An automated system used to support the creation, use and maintenance of electronically created documents for the purposes of improving an organisation's workflow. These systems do not necessarily incorporate recordkeeping functionality and the documents may be of informational rather than evidential value (ie the documents may not be records).

Electronic messages – Any communication using an electronic system for the conduct of official business internally, between Australian Government agencies, or with the outside world.

Electronic messaging systems – Applications used by agencies or individuals for sending and receiving, as well as storing and retrieving, electronic messages. These systems generally do not possess recordkeeping functionality.

Electronic record – a record created and/or maintained by means of electronic equipment. Includes analogue formats (see also Digital record).

Electronic records management system (ERMS) – An automated system used to manage the creation, use, maintenance and disposal of electronically created records for the purposes of providing evidence of business activities. These systems maintain appropriate contextual information (metadata) and links between records to support their value as evidence.

[12] Standards Australia, *Australian Standard for Records Management*, AS ISO 15489 – 2002, Part 1, Clause 3.7 and Part 2, Clause 4.3.9.2.

[13] International Council on Archives, *Dictionary of Archival Terminology*, KG Saur, Munich, 1988, p. 48.

[14] Australian Government Information Management Office, *Trusting the Internet – A Small Business Guide to E-security*, July 2002, p. 43

[15] Standards Australia, *Australian Standard for Records Management*, AS ISO 15489 – 2002, Part 1, Clause 3.10.

Emulation – A digital record preservation approach which involves keeping digital records in their original format and recreating the operating environment to enable the original performance of the software to be recreated on current computers. The result is that the original data format is preserved and may be accessed in an environment that allows for the recreation of the original 'look and feel' of the record.

Encapsulation – The process of 'packaging' records with enough metadata to preserve their content and context, and to support their reconstruction at some time in the future.

Encryption – Encryption is the process of converting data into a secure code, through the use of an encryption algorithm, for transmission over a public network. The mathematical key to the encryption algorithm is encoded and transmitted with the data, thus providing the means by which the data can be decrypted at the receiving end, and the original data restored.[16]

Exempt information – Sensitive information defined in section 33 of the Archives Act (eg personal or security related information) which may be withheld from public access beyond 30 years.

Expunge – To delete exempt information from a copy of a record in order to make the remainder of the record available for public access.

Hybrid recordkeeping system – A system containing a combination of paper, electronic or other formats.

Metadata – Structured information that describes and/or allows users to find, manage, control, understand or preserve other information over time.[17]

Migration – The act of moving records from one system to another, while maintaining the records' authenticity, integrity, reliability and usability. Migration involves a set of organised tasks designed to periodically transfer digital material from one hardware or software configuration to another, or from one generation of technology to another.[18]

Normalisation – Process of changing records from one data format to an archival data format.

[16] Australian Government Information Management Office*, Trusting the Internet – A Small Business Guide to E-Security*, July 2002, p. 43

[17] Adrian Cunningham, 'Six degrees of separation: Australian metadata initiatives and their relationships with international standards', *Archival Science*, vol. 1, no. 3, 2001, p. 274.

[18] Standards Australia, *Australian Standard for Records Management*, AS ISO 15489 – 2002, Part 1, Clause 3.13 and Part 2, Clause 4.3.9.2.

Record – Information in any format created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.[19]

Recordkeeping – Making and maintaining complete, accurate and reliable evidence of business transactions in the form of recorded information. Recordkeeping includes:

- creating records in the course of business activity and the means to ensure the creation of adequate records;
- the design, establishment and operation of recordkeeping systems; and
- managing records used in business (traditionally regarded as the domain of records management) and as archives (traditionally regarded as the domain of archives administration).[20]

Recordkeeping system – Framework to capture, maintain and provide access to evidence over time, as required by the jurisdiction in which it is implemented and in accordance with common business practices. Recordkeeping systems include:

1. both records practitioners and records users;
2. a set of authorised policies, assigned responsibilities, delegations of authority, procedures and practices; policy statements, procedures manuals, user guidelines and other documents which are used to authorise and promulgate the policies, procedures and practices;
3. the records themselves;
4. specialised information and records systems used to control the records; and
5. software, hardware and other equipment, and stationery.[21]

Records management – Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.[22]

Structure – The appearance and arrangement of a record's content (eg the relationships between fields, entities, language, style, fonts, page and paragraph breaks, links and other editorial devices).

[19] Standards Australia, *Australian Standard for Records Management*, AS ISO 15489 – 2002, Part 1, Clause 3.15.

[20] Standards Australia, *Australian Standard for Records Management*, AS ISO 15489 – 2002, Part 1, Clause 4.19 and Part 3, Foreword.

[21] Standards Australia, *Australian Standard for Records Management*, AS ISO 15489 – 2002, Part 3, Clause 6.21.

[22] Standards Australia, *Australian Standard for Records Management*, AS ISO 15489 – 2002, Part 1, Clause 3.16.

Vital records – Records without which an organisation could not continue to operate – ie those containing information needed to re-establish the organisation in the event of a disaster. Vital records are those that protect the assets and interests of the organisation as well as those of its clients and shareholders.[23]

Web-based records – A generic term that refers to all types of web-based information that meets the criteria of a record, including public websites, virtual private networks, extranets and intranets.

XML (e**X**tensible **M**arkup **L**anguage) – A simple, flexible computer language developed by the World Wide Web Consortium as an open, non-proprietary technology that creates common information formats so that both the format and the data can be shared between organisations, regardless of their respective Internet computing platforms.[24]

[23] J Kennedy and C Schauder, *Records Management: A Guide for Students and Practitioners of Records and Information Management with Exercises and Case Studies*, Longman Cheshire, Melbourne, 1994, p. 302.

[24] Australian Government Information Management Office, *B2B E-Commerce: Capturing Value Online*, 2001, p. 90.

Further reading

National Archives publications

National Archives of Australia, 2000, *Administrative Functions Disposal Authority*, published online at www.naa.gov.au/recordkeeping/disposal/authorities/gda/afda/summary.html

National Archives of Australia, December 2002, 'An Approach to the preservation of digital records', published online at www.naa.gov.au/recordkeeping/er/digital_preservation/summary.html

National Archives of Australia, 2002, 'Archives Advice 5 – Protecting and handling magnetic media', published online at www.naa.gov.au/recordkeeping/rkpubs/advices/advice5.html

National Archives of Australia, 1999, 'Archives Advice 6 – Protecting and handling optical disks', published online at www.naa.gov.au/recordkeeping/rkpubs/advices/advice6.html

National Archives of Australia, September 2003, 'Archives Advice 20 – Email is a Record!', published online at www.naa.gov.au/recordkeeping/rkpubs/advices/advice20.html

National Archives of Australia, 2002, 'Archives Advice 27 – Handling Administrative Change', published online at www.naa.gov.au/recordkeeping/rkpubs/advices/advice27.html

National Archives of Australia, March 2001, *Archiving Web Resources: A Policy for Keeping Records of Web-based Activity in the Commonwealth Government*, published online at www.naa.gov.au/recordkeeping/er/web_records/policy_contents.html

National Archives of Australia, March 2001, *Archiving Web Resources: Guidelines for Keeping Records of Web-based Activity in the Commonwealth Government*, published online at www.naa.gov.au/recordkeeping/er/web_records/guide_contents.html

National Archives of Australia, December 2002, *Commonwealth Implementation Manual: AGLS Metadata*, published online at www.naa.gov.au/recordkeeping/gov_online/agls/cim/cim_manual.html

National Archives of Australia, July 2003, *Developing a Functions Thesaurus: Guidelines for Commonwealth Agencies,* published online at www.naa.gov.au/recordkeeping/control/functions_thesaur/intro.html

National Archives of Australia, 2002, *Developing a Policy: How to Develop a Recordkeeping Policy*, published online at www.naa.gov.au/recordkeeping/overview/policy/summary.html

National Archives of Australia, September 2001, *DIRKS: A Strategic Approach to Managing Business Information*, published online at www.naa.gov.au/recordkeeping/dirks/summary.html

National Archives of Australia, 2000, *Disaster Preparedness Manual for Commonwealth Agencies*, published online at www.naa.gov.au/recordkeeping/preservation/disaster/intro.html

National Archives of Australia, December 2002, 'Fact Sheet 10 – Access to records under the Archives Act', published online at www.naa.gov.au/Publications/fact_sheets/FS10.html

National Archives of Australia, May 2004, *General Disposal Authority for Encrypted Records Created in Online Security Processes*, published online at www.naa.gov.au/recordkeeping/disposal/authorities/GDA/summary.html

National Archives of Australia, February 2003, *General Disposal Authority for Source Records that have been Copied, Converted or Migrated*, published online at www.naa.gov.au/recordkeeping/disposal/authorities/GDA/summary.html

National Archives of Australia, 2003, *Keep the Knowledge – Make a Record!*, published online at www.naa.gov.au/recordkeeping/training/keep/package.html

National Archives of Australia, 2001, *Keyword AAA: A Thesaurus of General Terms* (Commonwealth version), see www.naa.gov.au/recordkeeping/control/keyaaa/summary.html

National Archives of Australia, July 2003, *Overview of Classification Tools for Records Management,* published online at www.naa.gov.au/recordkeeping/control/tools.html

National Archives of Australia, May 2004, *Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received using Authentication and Encryption*, published online at www.naa.gov.au/recordkeeping/er/security.html

National Archives of Australia, 1999, *Recordkeeping Metadata Standard for Commonwealth Agencies*, published online at www.naa.gov.au/recordkeeping/control/rkms/summary.htm

National Archives of Australia, 1998, *Records Issues for Outsourcing: General Disposal Authority 25*, published online at www.naa.gov.au/recordkeeping/disposal/authorities/GDA/summary.html

National Archives of Australia, 2002, *Standard for the Physical Storage of Commonwealth Records*, published online at www.naa.gov.au/recordkeeping/storage/standard.html

National Archives of Australia, 2002, *Storing to the Standard: Guidelines for Implementing the Standard for the Physical Storage of Commonwealth Records*, published online at www.naa.gov.au/recordkeeping/storage/standard.html

Other publications

The following are general sources of information on aspects of digital recordkeeping.

Australian National Audit Office, September 2003, *Recordkeeping in Large Commonwealth Organisations*, published online at www.anao.gov.au/WebSite.nsf/Publications/478B4A27724E193BCA256DA50074796C

Australian National Audit Office, May 2002, *Recordkeeping*, published online at www.anao.gov.au/WebSite.nsf/Publications/4A256AE90015F69BCA256BA5000C25D8

Australian Public Service Commission, October 2002, *State of the Service Report 2001–02*, published online at www.apsc.gov.au/stateoftheservice/2002/index.htm

Australian Public Service Commission, 2003, *APS Values and Code of Conduct in Practice*, published online at www.apsc.gov.au/values/conductguidelines.htm

Attorney General's Department, 2000, *Commonwealth Protective Security Manual,* Commonwealth of Australia, published online at www.ag.gov.au/www/protectivesecurityHome.nsf/AllDocs/3ABEF2858B90B6D3CA256BB3001AE07C?OpenDocument

Barrett PJ, Auditor-General for Australia, May 2002, 'External scrutiny of government decisions – trends and lessons learnt', Institute of Public Administration of Australia, ACT Division, half-day seminar, published online at www.anao.gov.au/WebSite.nsf/Publications/4A256AE90015F69B4A256BCD007C8E50

Barrett PJ, Auditor-General for Australia, June 2002, 'Achieving better practice corporate governance in the public sector', International Quality and Productivity Centre seminar, published online at www.anao.gov.au/WebSite.nsf/Publications/4A256AE90015F69BCA256BE4000827D3

Consultative Committee for Space Data Systems, 2003, *Reference Model for an Open Archival Information System,* ISO 14721, published online at ssdoo.gsfc.nasa.gov/nost/wwwclassic/documents/pdf/CCSDS-650.0-B-1.pdf

Defence Signals Directorate, 2004, *Australian Government Information Technology Security Manual* (ACSI 33), published online at www.dsd.gov.au/library/infosec/acsi33.html

Ellis, Judith (ed.), 2000, *Selected Essays in Electronic Recordkeeping in Australia,* Australian Society of Archivists Inc.

National Library of Australia, *Preserving Access to Digital Information (PADI)*, published online at www.nla.gov.au/padi/

National Office for the Information Economy (now the Australian Government Information Management Office), 2002, *Authentication: A Guide for Government Managers about Online Authentication,* published online at www.agimo.gov.au/publications/2002/07/online_auth/

National Office for the Information Economy (now the Australian Government Information Management Office), July 2002, *Better Services, Better Government: The*

Federal Government's e-Government Strategy, published online at www.agimo.gov.au/publications/2002/11/bsbg/

National Office for the Information Economy (now the Australian Government Information Management Office), April 2000, *Government Online: The Commonwealth Government's Strategy*, published online at www.agimo.gov.au/publications/2000/04/govonline

National Office for the Information Economy (now the Department of Communications, Information Technology and the Arts), 2002, *Trusting the Internet – A Small Business Guide to E-security*

National Office for the Information Economy (now the Department of Communications, Information Technology and the Arts), 2001, *B2B E-Commerce: Capturing Value Online*

Standards Australia, 2002, *Australian Standard for Records Management*, AS ISO 15489, available from Standards Australia's website www.standards.com.au

Standards Australia, 1996, *Australian Standard for Records Management*, AS 4390, (superseded by the AS ISO 15489 – 2002)

State Records Authority of New South Wales, April 2002, *Future Proof: Ensuring the Accessibility of Equipment/Technology Dependent Records*, published online at www.records.nsw.gov.au/publicsector/rk/guidelines/techdependent/TechDependentTOC.htm

State Records Authority of New South Wales, June 2002, *Guidelines on Counter Disaster Strategies for Records and Recordkeeping Systems*, published online at www.records.nsw.gov.au/publicsector/rk/guidelines/counterdisaster/toc.htm

State Records Office of Western Australia, , Electronic Records Handbook (working title), forthcoming, Perth, Western Australia.

World Wide Web Consortium (W3C), Extensible markup language (XML), www.w3.org/XML/