Australian Capital Territory

Territory Records (Standard for Records Management Number 8: Business Continuity and Records Management) Approval 2008 (No 1)

Notifiable instrument NI2008—438

made under the

Territory Records Act 2002, s 18 (Approved standards and codes for records management)

---

1. Name of Instrument

This instrument is the Territory Records (Standard for Records Management Number 8: Business Continuity and Records Management) Approval 2008 (No 1).

2. Approval

I approve the Standard for Records Management Number 8: Business Continuity and Records Management.

3. Commencement

This instrument commences on the day after notification.

David Wardle
Director of Territory Records
18 September 2008

September 2008

Standard for Records Management
Number 8 – Business continuity and records management

PURPOSE

To set principles and minimum standards for business continuity in relation to records management across the ACT Government.

AUTHORITY

This Standard is produced in accordance with section 18 of the *Territory Records Act 2002* (the Act), which allows the Director of Territory Records to approve Standards or Codes for agency records management.

Under section 17 of the Act, an agency's Principal Officer may approve a Records Management Program only if it complies with the Standards and Codes set by the Director of Territory Records.

Section 17(2) allows a Principal Officer to approve a Records Management Program that does not comply with an approved Standard or Code only if the Director of Territory Records agrees in writing that non-compliance is necessary for the operational needs of the agency.

Section 14 of the Act requires agencies to "make and keep full and accurate records" of their activities. Section 15 requires agencies to take steps necessary to ensure that the information in their records continues to be accessible.

This Standard must be reviewed as soon as practicable five years after its commencement.

INTRODUCTION

The *Territory Records Act 2002* (the Act) requires all ACT agencies to make and keep records of their business activities:

- for use in ongoing business activities,
- to allow public access to them consistent with the principles of the *Freedom of Information Act 1989*, and
- for the benefit of future generations.

Recordkeeping practitioners in the ACT Government recognise the importance of the records in their jurisdiction, and they are generally aware of a range of events that could pose a threat

to continued access to these records. However formal recordkeeping practices frequently give only nominal attention to records-related threats to business continuity.

This Standard addresses the need for proper assessment and mitigation of threats to business continuity. Risk assessment has to be undertaken on an agency basis as the business context and some of the risks are agency-specific. Business continuity planning for records should be part of an agency's broader business continuity program. (Standards Australia, HB 292-2006)

This Standard addresses only records-specific aspects of risk assessment, business continuity, disaster recovery and risk management planning. This is because it is assumed that all agency business continuity plans will meet relevant Australian Standards as well as Government requirements. This Standard does not limit the range of legitimate approaches to business continuity planning that agencies may pursue. This Standard seeks to ensure that records management related aspects of risk management and business continuity planning are adequately addressed.

BACKGROUND

Lost or damaged records (in any form) can cause problems. All records need whole-of-life management, including counter-disaster planning. Business continuity management helps an agency prepare for, and recover from a major disruption. Records management identifies which records are vital to the conduct of the business, so it supports business continuity planning and assists in maintaining an operational, accountable agency in the event of a disaster.

Business continuity planning for records requires recognition of the important role that records play in enabling an agency to carry out its essential or core responsibilities. An agency's full compliance with all Standards for Records Management is evidence of its recognition of the importance of records to the Government, the community, its staff, and to the delivery of its ongoing business functions including its accountability responsibilities. Successful implementation of its approved Records Management Program demonstrates the agency's compliance.

The key elements of business continuity management in relation to records management include:

- Understanding the importance of records management (Standards 1 to 7);
- Understanding the overall context within which the agency operates and manages records including the agency's critical objectives (Principle 1);
- Understanding the risk management and security context within which an agency's records management operates (Principle 1);
- Understanding the triggers for implementing disaster management, business continuity response and recovery procedures in relation to records management (Principle 2);
- Ensuring that all those with delegated or outsourced responsibility for records management play their part in ensuring business continuity (Principle 2); and

- Ensuring all staff understand their roles and responsibilities when a major disruption occurs (Principle 2).

PRINCIPLES

Two principles define the high-level requirements to be met by agencies when determining and implementing business continuity programs relating to their records management.

PRINCIPLE 1 – AN AGENCY IS TO ASSESS ITS RECORDS FOR BUSINESS CONTINUITY RISKS

Issues of risk management, corporate governance, security and customer service are high priorities for agency governance (see *Public Sector Management Act 1994*). Records and document management are one aspect of governance, which is recognised by the existence of the *Territory Records Act 2002*.

It is necessary to ensure continued access to vital records and archival records if core business functions are to continue to be delivered when and after disaster strikes. The term "disaster" is used here to cover a wide range of major and minor disruptions to records, records management and recordkeeping systems.

It is essential for each agency to undertake an assessment of the risks facing its records, records management and recordkeeping systems. The methods for vulnerability ratings, consequence measurement criteria, likelihood ratings, risk rating matrices and so on are covered in documents by Standards Australia and are not repeated here.

Business risk impact assessment for records

A business impact assessment is a management-level analysis which identifies the impacts of losing agency resources or capability. Such an assessment measures the effect of the loss of access to records, and escalating losses over time. This measurement provides senior management with reliable data upon which to base decisions on risk mitigation and continuity planning.

An agency's risk assessment for records informs business continuity planning for records management and is part of a broader business impact assessment for that agency.

An agency's risk assessment for records will include:

- Identification of vital records.
- Identification of archival records.
- Valuation of records, particularly vital records and archival records.
- Calculation of full insurance replacement value of all its records
- Identification of possible risks to an agency's business continuity, its vital records and archival legacy arising from emergencies or disasters affecting its records; and

- Evaluation of the risks associated with disasters of selected orders of likelihood and consequence. The evaluation includes cost estimates of recovery processes required to ensure business continuity and maintenance of its vital records and archival legacy.

Vital records and archival records

The first step in assessing risks from a records management viewpoint is to identify vital records and archival records. Identification of vital records provides an agency with information that it needs to conduct its business when and after any disruptions occur to normal operating conditions. It also enables staff members to protect the records required for ongoing core business.

Vital records are those records that, if destroyed, must be recreated to resume essential business functions, including the agency's legal and accountability responsibilities. If a vital record is lost, damaged, destroyed or otherwise unavailable, the loss *is* a disaster, affecting critical operations. Vital records are records, in any format, which contain information essential to the survival or continuity of an agency. Records that protect the legal and financial interests of the agency and its customers are vital records. Vital records are not necessarily, in themselves, valuable in monetary terms.

The ongoing availability of information held in vital records can be ensured by one of three strategies: duplication and dispersal; use of secure fireproof, waterproof and vermin-proof storage; or remote storage.

Archival records are records that are preserved for the benefit of present and future generations and therefore have longer term access and preservation requirements. Some records that are identified as vital records may also be archival.

Vital and archival records become the main priorities for recovery and salvage efforts when a disaster occurs. Records are to be recovered in accordance with the disaster response arrangements established for the agency.

An agency may choose to create a priority ranking between its vital records. For example, a record may be considered a vital record for only part of its life; so an agency may conduct periodic reviews of the status of its records. Or, a record may not be vital if it is inaccessible for one day, but may become vital if inaccessible for two days.

Valuation and insurance

It is important that an agency understands the value of the records for which it is responsible. Their value is broader than simply monetary, and many provide insights into our community's cultural heritage. In addition, records need to be valued as assets – especially historic archival material retained as Territory Archives. Identifying the value of an agency's records is an important part of the risk assessment.

An agency's records are regarded as a Territory asset. ACT Government agencies are required to declare the full replacement value of assets to the ACT Insurance Authority for insurance

purposes. The insurance value of paper records should reflect the costs of replacement and potentially, conservation and recovery. This can be established at a $ rate per linear shelf metre as provided by the Director of Territory Records.

There is no option for an Agency to decide not to insure or only partially insure such assets.

Risk identification and analysis

The identification and analysis of records-related risks must at least equal the rigour of, or comply with relevant Australian Standards of risk identification and analysis. (AS/NZS 4360-2004, *Risk Management;* HB 143:1999, *Guidelines for Managing Risk;* HB 292-2006, *A Practitioners Guide to Business Continuity Management* and HB 167:2006, *Security Risk Management.*)

It is likely that scenarios will be developed for a range of disasters, which will include a selected range of likelihoods and a selected range of consequences. ACT's records regime is media-independent, however the risks considered will sometimes be media-specific. For instance, paper and digital records face some very different risks as well as some risks that are similar.

The analysis must include an assessment of the vulnerability of the agency to records-related risks associated with records, records management and recordkeeping systems. Although the greatest emphasis must be on vital records and archival records, all records and recordkeeping systems of an agency must be considered including those records that derive from a function that has been outsourced (see *Standard for Records Management No.5 – Recordkeeping and Outsourced Government Business*).

Compliance with Principle 1

A compliant agency can demonstrate that it has completed an adequate and explicit business risk impact assessment for records, which includes the following components:

- Assessment of all records for which an agency is responsible, including those derived from any function that has been outsourced;
- Identification of vital records;
- Identification of archival records
- Valuation of vital records
- Valuation of archival records
- Calculation of full insurance replacement value of all its records
- Identification of possible risks to an agency's business continuity and its archival legacy arising from emergencies or disasters affecting its records, records management and recordkeeping systems;
- Evaluation of the risks associated with disasters of selected orders of likelihood and consequence; and
- A program demonstrating that regular reviews are undertaken to ensure that the impact assessment of the risks facing an agency's records, records management and recordkeeping systems is current.

PRINCIPLE 2 – AN AGENCY IS TO UNDERTAKE BUSINESS CONTINUITY PLANNING FOR ITS RECORDS

It is critical to plan for and protect all records and recordkeeping systems of an agency from the risk of disruption and to ensure the continuation of business in the event of a disaster. This includes all records for which an agency is responsible, including those associated with a function that has been outsourced.

As used in this Standard, business continuity planning for records encompasses four related activities that may be characterised as occurring before, during, after and looking back on a disaster:

- *Disaster mitigation*: minimising the likelihood of the occurrence of anticipated disasters by having preventive measures in place
- *Disaster response*: work undertaken to lessen the impact of a disaster after it has occurred
- *Business continuity*: measures that are necessary for the swift and efficient resumption of daily operations after a disaster
- *Periodic review*: periodically reviewing and adapting the business continuity plan to reflect current conditions.

Disaster mitigation

In determining actions to minimize the likelihood or impact of an identified threat, agencies are to be guided by their business risk impact assessment for records. Any easy, cost-effective measures that can be undertaken in the normal course of business should be the first focus of activity. Records managers are to liaise with agency officers responsible for risk management, security, buildings and property.

Mitigation measures are to be detailed in the contractual obligations of service providers of outsourced functions.

Disaster response

To be effective, disaster response arrangements must be documented actions that are specific to the agency. They will be clearer if grouped in meaningful headings, such as “Take immediate action to:…” and “Stabilise the situation by:…”, and so on. Sequential “action checklists” of required actions for identified individuals or groups of individuals’ will be useful. Responsibilities during a disaster must be known in advance. The actions required during a disaster are best anticipated in advance by the individuals’, and, prior to the disaster, must have been rehearsed as far as possible.

The *ACT Protective Security Policy and Guidelines*, (P.38) points out that “[i]f a person’s duties require access to security classified information or areas he or she should have an appropriate clearance”. Therefore, to perform their roles adequately, all Records Managers will require security clearances, as they require access to the whole of an agency’s records management system, including electronic records.

Disaster response measures are to be detailed in the contractual obligations of service providers of outsourced functions.

Business continuity

Getting normal functions back into operation is likely to be a staged process, depending on the scale and nature of the disaster. Stages need to be sensible for the functions of the agency and the impact of the disaster, but may include stages like "Immediate recovery procedures", "Stabilising the situation", "Recovery materials and equipment", and "Returning to normal". An agency's business continuity planning for records should determine likely stages for disasters of different impacts, and the recovery teams that may be required for each stage.

Priorities for the recovery of records and recordkeeping systems are to be derived from the agency's business risk impact assessment for records. Recovery teams will need to be established using identified procedures. Action checklists may be useful during the re-establishment of business continuity.

To be ready for a disaster when it occurs, the disaster response and business continuity instructions must be produced as separate, widely distributed documents. Business continuity measures are also to be detailed in the contractual obligations of service providers of outsourced functions.

Periodic review

An agency's business continuity plan for records must be reviewed from time-to-time to ensure it meets current requirements. A review is sensible after a disaster of any significant size. A review of risks is to occur at least annually.

Roles and responsibilities of an agency's Records Manager

It is important that everyone involved in dealing with a potential disaster clearly understands their roles and responsibilities and in advance of a disaster occurring. In times of crisis, the capacity for quick decision-making is essential. This requires that everyone involved, including each decision-maker, knows who holds which responsibilities.

The roles of many staff members will derive from the business continuity planning of the agency to which they belong. However, there are some roles and responsibilities that can be identified for all agencies. This applies particularly to each agency's nominated Records Manager who has responsibility for the implementation of the agency Records Management Program.

The agency Records Manager is responsible for ensuring that:

- A current business risk impact assessment for records exists for the agency
- A current business continuity plan for records is created and adequately rehearsed
- Instructions about disaster response and business continuity are widely distributed so that instructions during a time of crisis are sufficient, clear, understood and accessible
- As far as possible, the integrity of records will be maintained in event of a disaster

- An agency's business risk impact assessment for records is used as the basis of a security and access classification scheme for records of the agency, so that it is clear who has access to which records
- Records managers have access to all relevant parts of an agency's records management system, including electronic records. This is likely to mean that key staff dealing with records and information will require security clearances (see the *ACT Protective Security Policy and Guidelines* (p.38).
- Outsourced providers are meeting the agency's obligations regarding records, records management, recordkeeping systems and business continuity planning
- All relevant staff are trained and adequately rehearsed in emergency procedures to protect and salvage records and
- Disaster mitigation measures are incorporated in the design and management of all of that agency's records storage facilities and workplaces.

Compliance with Principle 2

A compliant agency will have undertaken business continuity planning for records incorporating four phases of planning for business continuity:

- *Disaster mitigation*: a system of preventative measures to minimise the likelihood of the occurrence of anticipated disasters
- *Disaster response*: instructions that will lessen the impact of a disaster after it has already occurred
- *Business continuity*: measures that are necessary for the swift and efficient resumption of operations after a disaster
- *Periodic review*: adaptation of the business continuity plan for records to reflect current conditions.

A compliant agency can demonstrate that its Records Manager meets the responsibilities, as listed above, placed on him or her.

DEFINITIONS

Agency
The Executive, an ACT Court, the Legislative Assembly Secretariat, an administrative unit, a Board of Inquiry, a Judicial or Royal Commission, any other prescribed authority, or an entity declared under the regulations of the *Territory Records Act 2002* to be an agency.

Archival records
See Territory Archives.

Business continuity
The uninterrupted availability of all key resources supporting essential business functions. In relation to records, business continuity is the uninterrupted availability of records in all formats, recordkeeping systems and data critical to the reconstitution of an agency's vital records and archival records.

Business continuity planning for records
A process which seeks to enable business continuity, and contains procedures, information and resource identification that are ready to use in the event of an emergency or disaster affecting an agency's records, records management or recordkeeping systems. It is the process of preparing for, mitigating, responding to and recovering from a disaster.

Business risk impact assessment for records
A management level analysis that identifies the impacts of losing access to an agency's records. It provides senior management with reliable data upon which to base decisions on risk mitigation and continuity planning, and it includes an agency's records, records management and recordkeeping systems.

Disaster
A wide range of major and minor upsets to records, records management and recordkeeping systems.

Disaster recovery planning for records
See Business continuity planning for records.

Outsourcing
A contractual arrangement whereby services to or on behalf of an agency that would otherwise be carried out internally are provided by an external organisation. The outsourcing or controlling agency remains ultimately responsible for a function that has been outsourced.

Principal Officer
The Chief Executive of an administrative unit, or its equivalent in other types of agencies.

Records
Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. This recorded information must be maintained or managed by the agency to provide evidence of their business activities. Records can be in written, electronic or any other form.

Records of an agency
Records in written, electronic or any other form, under the control of an agency or to which it is entitled to control, kept as a record of its activities, whether it was created or received by the agency.

Recordkeeping Systems
Information systems that capture, maintain and provide access to records over time. While the term is often associated with computer software, Recordkeeping systems also encompass policies, procedures, practices and resources which are applied within an agency to ensure that full and accurate records of business activity are made and kept.

Records management
The managing of the records of an agency to meet its operational needs and, if appropriate, to allow public access to the records consistent with the *Freedom of Information Act 1989* and for the benefit of future generations. Records management includes but is not limited to the creation, keeping, protection, preservation, storage and disposal of, and access to records of the agency.

Records Management Program (RMP)
A document that complies with section 16 of the *Territory Records Act 2002* by setting out the means by which an agency will manage its records, and is approved by the agency's Principal Officer.

Records Manager
The person nominated in an agency's Records Management Program to be responsible for Records Management in the agency. Such a nomination is required under *Standard for Records Management No.1 – Records Management Programs*.

Risk
Risk is the chance of something happening that will have an impact upon objectives. It is measured in terms of consequences and likelihood.

Risk management
Risk management refers to the culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects.

Territory archives
Territory records preserved for the benefit of present and future generations.

Vital records
Records without which an organisation could not continue to operate, that is, those containing information needed to re-establish the organisation in the event of a disaster. If destroyed, vital records must be recreated to resume essential business functions, which include the legal and accountability responsibilities of an agency and its customers.

REFERENCES AND FURTHER READING

Dorge, Valerie and Sharon L Jones (1999) *Building an Emergency Plan: A Guide for Museums and Other Cultural Institutions. The Getty Conservation Institute,* http://www.getty.edu/conservation/publications/pdf_publications/emergency_plan.pdf

Heritage Collections Council (2000) *Be prepared: guidelines for small museums for writing a disaster preparedness plan.* Available 23 April 2007, from http://sector.amol.org.au/publications_archive/collections_management/be_prepared

National Archives. *Records management standards business recovery plans: Standards for the management of Government records RMS 3.2.* http://www.nationalarchives.gov.uk/documents/stan_business_recovery.pdf

National Archives of Australia (2004). *Digital Recordkeeping Guidelines: Part 9. Business continuity planning for digital records* http://www.naa.gov.au/Images/Digital-recordkeeping-guidelines_tcm2-920.pdf

Petersen, Katherine M (2006) *Disaster Preparedness and Recovery for Museums: A Business Recovery Model. Texas State University* http://ecommons.txstate.edu/cgi/viewcontent.cgi?article=1118&context=arp

Public Record Office of Victoria, *Advices on Electronic Records: 7. Preserving Records in Databases, 2003;* Available at: http://www.prov.vic.gov.au/publications/publns/PROVRMadvice7.pdf

Public Sector Management Act 1994

Standards Australia (1999). *HB 143:199: Guidelines for managing risk in the Australian and New Zealand public sector.* Strathfield, NSW, Standards Association of Australia

Standards Australia (2004). *AS/NZS 4360:2004: Risk Management.* Strathfield, NSW, Standards Association of Australia

Standards Australia (2006). *HB 292-2006: A Practitioners guide to business continuity management*. Sydney, NSW, Standards Australia International Ltd

Standards Australia (2006*). HB 167: 2006 Security risk management*. Sydney, NSW, Standards Australia International Ltd

State Records New South Wales. (2002). *Standard on counter disaster strategies for records and recordkeeping systems.* http://www.records.nsw.gov.au/recordkeeping/standard_4438.asp

Territory Records Act 2002

Territory Records Office (2003). Standard for *Records Management No.1 – Records Management Programs.* Territory Records Office, Canberra. Available at: http://www.territoryrecords.act.gov.au/

Territory Records Office (2003) *Standard for Records Management No. 2 – Appraisal*. Territory Records Office, Canberra. Available at: http://www.territoryrecords.act.gov.au/

Territory Records Office (2003), *Standard for Records Management No. 3 – Records Description and Control*. Canberra http://www.territoryrecords.act.gov.au/

Territory Records Office (2003). *Standard for Records Management No.4 – Access*. Territory Records Office, Canberra. Available at: http://www.territoryrecords.act.gov.au/

Territory Records Office (2003) *Standard for Records Management No.5 – Recordkeeping and Outsourced Government Business*. Territory Records Office, Canberra. Available at: http://www.territoryrecords.act.gov.au/

Territory Records Office (2007). *Standard for Records Management No.6 – Digital Records*. Territory Records Office, Canberra. Available at: http://www.territoryrecords.act.gov.au/

Territory Records Office (2008), *Standard for Records Management No.7 – Physical Storage of Records*. Canberra. http://www.territoryrecords.act.gov.au/

US National Archives and Records Administration. (1999). *Vital records and records disaster mitigation and recovery: an instructional guide*. Available at http://www.archives.gov/records-mgmt/vital-records/