

State Records Authority of New South Wales

Standard: No. 6

**Standard on counter disaster
strategies for records and
recordkeeping systems**

issued under the State Records Act 1998

Approved June 2002

© State of New South Wales through the State Records Authority of New South Wales 2002.

First published 2002

This work may be freely reproduced for personal, educational or government purposes. Permission must be received from State Records Authority for all other uses.

ISBN 0-7313-5383-8

Standard for Records Management

Standard no 6

SR file no 00/0174

Title of Standard Standard on counter disaster strategies for records and recordkeeping systems

Scope The standard sets out principles to ensure that records in all formats, recordkeeping systems, and critical data required to reconstitute electronic records are protected by counter-disaster measures.

Application The standard applies to all public offices as defined in section 3 of the *State Records Act 1998*, to which Part 2 of the Act applies. The standard covers all State records on any topic and in any format.

Authority This standard is issued under section 13(1) of the State Records Act. It has been approved by the Board of the State Records Authority in accordance with section 13(2) of the State Records Act.

Authorised This standard was approved by David Roberts, Director, State Records Authority of New South Wales, on 19 June 2002.

Standard on counter disaster strategies for records and recordkeeping systems

Executive summary

The need to plan and protect records and recordkeeping systems from the risk of a disaster and to ensure the continuation of business in the event of a disaster has become critical in recent years. The implementation of Government policy in relation to the Year 2000 Millennium Strategy, its legacy of business continuity planning, and the *Standard on Physical Storage of State Records* have been key drivers behind the development of the standard on counter disaster strategies for records and recordkeeping systems.

This standard forms part of the framework of rules and guidance issued by State Records to help public offices meet their obligations under the *State Records Act 1998*. In particular, it aims to help each public office to '*ensure the safe custody and proper preservation of the State's records that it has control of*' (s.11).

The purpose of this standard is to ensure that records in all formats, recordkeeping systems and data critical to the reconstitution of a public office's electronic records are protected by counter disaster measures.

The standard comprises three principles, drawn from national and international best practice, that should be followed by public offices when working to protect records and recordkeeping systems from disaster events through counter disaster measures. Each principle is explained and followed by minimum compliance requirements. Sources of further guidance and a compliance checklist are also provided.

The principles are:

1. **Risk assessment:** Risks affecting records and recordkeeping systems should be identified and assessed.
2. **Planning:** An effective counter disaster plan for records and recordkeeping systems should be developed, implemented and maintained.
3. **Vital records protection:** Vital records should be identified and protected.

This standard is issued under the terms of s.13 of the State Records Act and applies to public offices, as defined in s.3 of the Act, except for those public offices to which Part 2 of the Act does not apply.

Definitions

Critical data

Data critical to an organisation's service delivery. Critical data includes information in all formats, including all information files that provide inputs to, and in some cases, outputs from critical business applications identified in the risk analysis. Also includes information entities such as data dictionaries, definitions of relationships, and codes used in computer applications.

Disaster

Any event that creates an inability on an organization's part to provide critical business functions for some predetermined period of time. (*Disaster Recovery Journal - Disaster Recovery Glossary*, www.drj.com/glossary/glossleft.htm)

Record

Any document or other source of information compiled, recorded or stored in written form or on film, or by electronic process, or in any other manner or by any other means. (*State Records Act 1998*, s.3(1))

Recordkeeping systems

Information systems which capture, maintain and provide access to records over time. (Australian Standard AS 4390-1996, *Records Management*, Part 1, *General*, Clause 4.20)

Risk assessment

The process of identifying and minimizing the exposures to certain threats which an organisation may experience. (*Disaster Recovery Journal – Disaster Recovery Glossary* www.drj.com/glossary/glossleft.htm)

State record

Any record, made and kept, or received and kept, by any person in the course of the exercise of official functions in a public office, or for any purpose of a public office, or for the use of a public office. (*State Records Act 1998*, s.3(1)).

Vital records

Those records that are essential for the ongoing business of an agency, and without which the agency could not continue to function effectively. The identification and protection of such records is a primary object of records management and disaster planning. (Judith Ellis, ed., *Keeping Archives*, 2nd edition, Melbourne, 1993, p. 481)

Introduction

Background

It is critical to plan and protect records and recordkeeping systems from risk and to allow for the continuation of business during a disaster event. State Records issued guidelines in 1999 to help agencies implement disaster management strategies for their records. The *2001 NSW Government Records Management Survey*, however, reveals that few agencies have disaster management plans for paper or electronic records.

In addition, Principle 4 of the *Standard on the Physical Storage of State Records* (issued in April 2000) requires that 'Disaster management programs should be established and maintained to ensure that risks to records are either removed or managed appropriately'. Compliance with this requirement will be mandatory from 1 January 2003. While important in establishing protection for records, this requirement only covers the different types of physical storage media (for example, paper, tapes, disks) but excludes the storage of electronic records on networks or on hard drives. The need to protect all records, regardless of their format or storage location has become an imperative.

Ministerial Memorandum No. 2001-04, issued in March 2001, required agencies to ensure that '...agency business continuity plans [developed for the Year 2000 Millennium Strategy] are maintained and updated as a normal part of agency operations. Each plan should ensure that agency services to the community are maintained in the event of any impact, including environmental hazards, loss of utilities supply or failure of technology.'

This standard builds on this legacy of business continuity planning and the protection of records, by extending the focus to all records and recordkeeping systems for which a public office is responsible. By setting minimum compliance requirements in relation to disaster management for all records and recordkeeping systems, the standard is intended in part to ensure that records and recordkeeping systems are addressed in business continuity planning.

The standard also builds on earlier guidance on disaster response and recovery. Rather than emphasise a reactive approach to disasters, the standard takes a proactive approach and seeks to 'counter' the possible effects of a disaster through the establishment of counter disaster plans based on an analysis of risks affecting records and recordkeeping systems.

This standard forms part of the framework of standards and codes of best practice, supported by guidelines, training and other forms of advice and assistance, provided by State Records to help public offices meet their obligations under Part 2 (*Records Management responsibilities of public offices*) of the State Records Act. In particular, it aims to assist each public office to '*... ensure the safe custody and proper preservation of the State's records that it has control of*' (s. 11).

Purpose

The purpose of this standard is to ensure that records in all formats, recordkeeping systems and data critical to the reconstitution of a public office's electronic records are protected by counter disaster measures.

Mandate

This standard is issued under s.13(1) of the *State Records Act 1998*, which empowers State Records to approve standards and codes of best practice for records management by public offices.

Application

This standard applies to public offices as defined in s.3 of the State Records Act, except for those public offices to which Part 2 of the Act does not apply.

Scope

This standard covers records of all formats, recordkeeping systems, and critical data required to reconstitute electronic records in the face of a disaster event.

The standard covers both disaster prevention (measures to prevent, or minimise the risk or impact of a disaster on records and recordkeeping systems) and disaster response and recovery.

Structure

This standard outlines three principles that should be taken into account by NSW public offices when they seek to protect records and recordkeeping systems through counter disaster measures. The principles are concerned with:

1. Risk assessment
2. Planning, and
3. Vital records protection.

Monitoring and compliance

A compliance checklist has been included as an attachment to this standard. It will help public offices to assess their own performance against the minimum compliance requirements.

State Records will monitor the implementation of this standard by examining responses to Records Management Surveys. State Records also has the power under s. 15 of the State Records Act to inspect public offices and third party storage facilities to ensure that minimum compliance requirements are met.

Reference to the Australian Standard AS 4390-1996, Records Management

Reference is made in this standard to the Australian Standard AS 4390, which is endorsed as a code of best practice under the *State Records Act, 1998*. The new international standard on records management, ISO 15489, has recently been endorsed as the new Australian standard on records management. This means that from the perspective of Standards Australia, the official body that issues Australian standards, AS 4390 has been replaced by the standard known as AS ISO 15489.

From State Records' perspective, however, both these standards provide excellent advice concerning records management. We fully endorse the new Australian standard, but we think that AS 4390 has much still to offer. Specifically, AS 4390 contains a number of definitions and some practical guidance that were not incorporated into AS ISO 15489 (eg. because they were Australian specific advice and terminology). The references in this standard are made to specific information in AS4390 not replicated or replaced by AS ISO 15489.

AS ISO 15489 has also been endorsed as a code of best practice under the State Records Act. This means that the standard is a model of best practice in NSW. AS 4390 was endorsed as a code of best practice under the Act some years ago. AS 4390 will not be removed as a code of best practice, rather both AS 4390 and ISO 15489 are endorsed as best practice models for NSW public offices.

For more information

For further information about this and other recordkeeping standards and codes of best practice and associated guidance, contact State Records.

Principles

Principle 1: Risk Assessment

Risks affecting records and recordkeeping systems should be identified and assessed

The identification and assessment of risk are the first important steps in developing effective counter disaster management strategies for a public office's records and recordkeeping systems.

The recommended methodology, based on that in Australian/New Zealand Standard AS 4360—1999, *Risk Management*, involves the following steps:

1. **Establish the context**
2. **Identify the risks** to records and recordkeeping systems
3. **Analyse the risks** in terms of probability and effect
4. **Assess the risks** in terms of acceptability and priorities for treatment
5. **Treat the risks** by identifying, evaluating and implementing options. Under this standard, this involves developing and implementing a counter disaster plan (see Principle 2: *Planning*)
6. **Monitoring and review.**

The methodology is discussed in more detail in the *Guidelines on Counter Disaster Strategies for Records and Recordkeeping Systems*.

Risks to vital records should be identified and assessed specifically in addition to risks to records in general (see Principle 3: *Vital records protection*).

The assessment should include the impact of potential disaster events on business functions, operations and services that depend on records in any format and on recordkeeping systems of all types, including business systems that keep records as part of their functionality.

The Business Risk Analysis, and subsequent updates (as required by Ministerial Memorandum No. 2001-04) that many NSW Government agencies prepared as part of their Year 2000 Millennium Strategy, provide a useful source for identifying and assessing risks to records and recordkeeping systems from disasters.

Minimum compliance requirement

1. A risk assessment of potential disaster events identifying threats to records and recordkeeping systems has been performed.

For further guidance

Australian/New Zealand Standard, AS 4360—1999, *Risk Management*

Office of Information and Communications Technology, *Information Security Guidelines for New South Wales Government Agencies Part 1 – Information Security Risk Management*, January 2001, <http://www.gcio.nsw.gov.au/library/guidelines>

Office of Information and Communications Technology, *Information Security Guidelines for New South Wales Government Agencies Part 2 - Examples of Threats and Vulnerabilities*, January 2001, <http://www.gcio.nsw.gov.au/library/guidelines>

Principle 2: Planning

An effective counter disaster plan for records and recordkeeping systems should be developed, implemented and maintained

Once risks to its records and recordkeeping systems have been identified and assessed, a public office should prepare a counter disaster plan to respond to those risks.

Content of the plan

The plan should cover the full range of counter disaster considerations including disaster prevention, disaster response and recovery and vital records protection.

As noted in the Australian Standard on records management (AS 4390—1996, Part 6, *Storage*, Appendix B), the plan should contain the following components:

- a. List of vital records, particularly significant or vulnerable holdings, and location and control documentation.
- b. List of equipment and materials available for use in disaster salvage and recovery.
- c. The function, composition and chain of command of the salvage and recovery team and their contact information.
- d. Procedures for identification and declaration of a disaster situation and initiation of the disaster response chain of command by the normal business operation.
- e. Provisions for the training and current awareness of the team.
- f. List of sources of back-up resources, including expertise, tradespeople, materials, equipment, vehicles and accommodation.
- g. Procedures for updating and testing plan.
- h. Simple technical information on the handling of damaged material, directed towards establishing priorities for early action.

The plan should be specific to the public office, its records and recordkeeping systems. The guidelines supporting this standard include a generic model that a public office can use to help develop its counter disaster plan.

The plan should be written in a clear and concise language that non-technical staff can understand.

Implementing the plan

For a counter disaster plan to be successfully implemented, the public office will need to:

- assign responsibility for the management and implementation of the counter disaster plan (either an individual officer or a group)
- build consensus about plans and their implementation
- place a high priority on the vital records program and critical data recovery
- encourage staff to take part in preparedness procedures such as information gathering and planning
- ensure staff are educated about the counter disaster plan and are aware of their roles
- understand that, in the event of a major disaster event requiring a sustained salvage operation, an organisation may have to restructure operations during and after disasters, and
- regularly practice and test the counter disaster plan through training exercises.

Maintaining the plan

A counter disaster plan should be regularly tested and revised in order to maintain its relevance. Untested plans present a danger to a public office's information infrastructure and business processes as they have not been evaluated through trial or simulation. Because the risks will change over time, counter disaster plans must accommodate that change. Without testing and revising the plan, the value of the investment in the counter disaster plan is wasted.

Post disaster analysis

Should a disaster affecting records and recordkeeping systems occur, an impartial review should be conducted, preferably by a senior management team, who were not involved in the disaster recovery. This team should report on the disaster event, including the nature of the disaster event, its consequences and the public office's response. Any effects of the disaster event on records or recordkeeping systems, the loss of any records and their subsequent replacement or restoration, the damage to information infrastructures or interruption to services, and follow up activities leading to the resumption of service should be documented.

The results of the analysis should be used to modify the counter disaster plan and/or the tasks of the disaster response team.

Minimum compliance requirements

1. A counter disaster plan for records and recordkeeping systems has been developed and implemented.
2. The plan is tested regularly and modified over time to reflect organisational, technological and other changes.

For further guidance

Australian Standard AS 4390—1996, *Records Management, Part 6, Storage*

Principle 3: Vital records protection

Vital records should be identified and protected.

Vital records are records that are essential for the ongoing business of an organisation, and without which it could not continue to function effectively. They are needed to:

- operate the organisation during a disaster
- re-establish the organisation's functions and legal and financial position after a disaster, and/or
- establish and protect the rights and interest of the organisation and its employees, customers and stakeholders after a disaster. (adapted from AS 4390 - 1996, *Records Management*, Part 6, *Storage*, Clause 6.1.2)

Vital records require special attention in an organisation's counter disaster strategies. They should be addressed specifically in the identification and assessment of risks affecting records and recordkeeping systems (see Principle 1: *Risk assessment*) and in the counter disaster plan (see Principle 2: *Planning*).

Identifying vital records

The identification of vital records should be a collaborative process involving records staff and business units, in order to:

- determine the kinds of records required to meet the needs noted above, and
- identify the specific groups of records of each kind, and their quantity and location, that exist in corporate recordkeeping systems and elsewhere.

The guidelines supporting this standard discuss in more detail the kinds of records that should be identified as vital.

For the purposes of this standard, vital records include:

- control documentation (registers, indexes, metadata repositories) for the public office's records and recordkeeping systems
- data critical to the reconstitution of the public office's electronic records, and
- State archives in the public office's custody, along with classes of records that are required to be kept as State archives under a retention and disposal authority.

For State collecting institutions, vital records include registration and control documentation for their collections.

Once identified, vital records should be listed in, or as an appendix to, the counter disaster plan and prioritised for recovery and restoration operations. This documentation should be kept up to date along with the rest of the plan.

Protecting vital records

A public office's counter disaster plan should cover both:

- measures to prevent or minimise the impact of a disaster event on vital records preventive measures, and
- recovery and restoration procedures to be followed if a disaster occurs.

Preventive measures may include:

- duplication and dispersal of vital records
- high levels of fire and security protection in storage containers and spaces
- storing backup copies off-site, and
- identifying and prioritising critical work in progress that may not be backed up or is sitting out on desks, in drawers, or on open shelving, and establishing procedures such as a 'clean desk policy' or additional safety measures.

Recovery and restoration procedures may include:

- the relocation of vital records to a secure site in the event of a disaster, and
- recommended handling and preservation techniques based on the media involved.

Preventive measures and recovery and restoration procedures for vital records are discussed in more detail in the guidelines supporting this standard.

Critical data protection

As part of vital records protection and recovery, data critical to the reconstitution of a public office's electronic records should be identified and able to be restored easily. Without the recovery and restoration of this data, business processes involving electronic recordkeeping, such as electronic commerce, supply chain management, enterprise resource planning, multimedia products or telecommunication applications, may be impossible to recover and restore.

Measures for protecting and recovering data critical to the reconstitution of electronic records should be integrated with arrangements for protecting a public office's other critical data.

Critical data recovery planning ensures that copies of electronic datasets and their most current updates (whether in electronic form or as paper based input documents) are:

- available to the recovery effort
- not destroyed by the same disaster event that renders the workplace and business operations untenable
- stored in a safe location, preferably off-site, and
- able to be restored within a specific timeframe to an accessible form for processing by systems, networks, and end users.

The guidelines supporting this standard provide further information about protecting data critical to the reconstitution of electronic records.

Minimum compliance requirements

1. Vital records are identified and documented.
2. Vital records protection, including recovery and restoration procedures, forms part of the counter disaster plan for records and recordkeeping systems.
3. Preventive measures for protecting vital records have been implemented.

For further guidance

National Archives and Records Administration, *Vital Records and Records Disaster Mitigation and Recovery: An Instructional Guide*. An instructional guide. 1999. Available at http://www.archives.gov/records_management/publications/vital_records.html

Compliance checklist

1	Risk assessment	Yes	No
1.1	Has a risk assessment of potential disaster events identifying threats to records and recordkeeping systems been performed?		
2	Planning		
2.1	Has a counter disaster plan for records and recordkeeping systems been developed and implemented?		
2.2	Is the counter disaster plan for records and recordkeeping systems tested regularly and modified over time to reflect organisational, technological and recordkeeping changes?		
3	Vital records protection		
3.1	Are vital records identified and documented?		
3.2	Does vital records protection, including recovery and restoration procedures, form part of the counter disaster plan for records and recordkeeping systems?		
3.3	Have preventative measures for protecting vital records been implemented?		