Government of South Australia

State Records
of South Australia

Records Management Disaster Planning

Guideline

June 2007

Version **1.2**

Table of Contents

Acknowledgments

State Records would like to acknowledge that this guideline has been developed thanks to a significant contribution from the State Records Authority of New South Wales, and their publication *Guidelines on Counter Disaster Strategies for Records and Recordkeeping Systems*, June 2002.

Foreword

State Records has issued this guideline in accordance with section 7(g) of the *State Records Act 1997*. Disaster planning is an important component of an adequate records management program. Planning for disasters is a benchmark for Outcome 7 in *Adequate Records Management: Meeting the Standard* (2002) and is also identified as part of a high quality recordkeeping system in the national Australian Standard *AS ISO 15489 – 2002: Records Management*.

The purpose of the guideline is to assist agencies within South Australia as defined in section 3 of the *State Records Act 1997* which includes state government agencies, local government authorities and universities, in developing and maintaining a disaster plan for records and recordkeeping systems. Agencies are encouraged to use this guideline in conjunction with the *Records Management Disaster Planning Toolkit*.

Introduction

Background

One of the major threats to the safety and preservation of official records is the risk of disaster. Disasters can at best be an annoying and expensive diversion for a government agency. At worst, a disaster may impede the operations of the agency and may cause severe financial loss, embarrassment and a loss of credibility and good will. Disasters have the potential to impact negatively on staff, clients, suppliers, taxpayers, the Government and the public.[1]

Counter disaster management strategies yield many benefits for records and recordkeeping systems. They are also essential for achieving adequate records management practices. Implementing risk management techniques, impact analysis, good recordkeeping practices, establishing vital records programs and prevention and preparedness plans can reduce the likelihood of disaster or minimise their impact. Business continuity planning and response and recovery planning will ensure that government agencies can react quickly to disasters, thereby increasing the chances of controlling the impact of disasters and promptly restoring resources and operations. Such actions can promote continued profitability or revenue flow and minimise costly disruptions to business services. In addition, counter disaster management planning can be a significant catalyst to improving a records management program.

Scope of this guideline

Records Management Disaster Planning Guideline provides a generic plan for the development of a Disaster Plan for records and recordkeeping systems. The guideline applies to agencies within South Australia as defined in section 3 of the *State Records Act 1997*. This guideline is issued in accordance with section 7(g) of the *State Records Act 1997* to assist agencies in achieving adequate records management practices with regards to Outcome 7 – The management of official records is planned (including the development of disaster plans ad the identification of vital records). Section 16 of the *State Records Act 1997* states that "If the manager [of State Records] is of the opinion that the records management practices of an agency are inadequate, the manager is required to report the matter to the Minister."

Related Documents

This document forms part of an overarching framework for adequate records management. Other documents in the framework include:

* *Records Management Disaster Planning Toolkit* – a series of templates, checklists and sample sheets relevant to the development of a records management disaster plan

* *Adequate Records Management: Meeting the Standard* – a standard that outlines the outcomes for an adequate records management regime, and provides associated policy

---

[1] Emergency Management Australia, *Non-Stop Service: Continuity Management Guidelines for Public Sector Agencies*, Commonwealth of Australia, Canberra, 1997, p.8.

statements, explanations and benchmarks that agencies need to satisfy if their records management programs are to be considered adequate in accordance with section 16 of the *State Records Act 1997*

- *Adequate Records Management: Implementation Plan* – a guideline that provides a generic plan for implementing an adequate records management program
- Recordkeeping Advices – these provide further advice and detail about each of the adequate outcomes and benchmarks, including disaster management.

All of these documents may be retrieved from the State Records of South Australia web site at www.archives.sa.gov.au.

Reference to the Adequate Records Management Standard

By ensuring that it takes all adequate steps to prevent a disaster, and by developing and maintaining a disaster plan, an agency will satisfy key elements of Outcome 7 of *Adequate Records Management: Meeting the Standard* (2002). Outcome 7 relates to "Planning – Records management shall be managed and planned in s strategic and corporate manner". One of the benchmarks for achieving adequacy for this outcome includes the identification of vital records and the development of a disaster recovery plan for official records, including recordkeeping systems.

Variation to this guideline

State Records may update or alter the *Records Management Disaster Planning Guideline* from time to time. All such updates or alterations shall be authorised by the director of State Records in consultation with the State Records Council. All South Australian agencies shall be informed of any such alterations or updates.

Records and Disasters

There are a number of definitions for 'disasters'. Some sources define them as unexpected events with destructive consequences, including small and large-scale events. Others distinguish disasters from emergencies, seeing emergencies as adverse events that require action, but not significant expenditure of effort to control, and disasters as emergency events that require resources beyond the organisation's means.

Perhaps the most realistic interpretation of 'disasters' is to view them as dependent, not on the *scale* of damage, but on the *effect* that the incidents create. For example, a water leak affecting one shelf of an agency's records may only be a small-scale emergency, but can be considered a disaster if the material affected is of significant value and will result in financial loss or legal action. Whether damage is considered a disaster will also depend on who values that material. For example, if there were no copies kept of the material on the shelf, it is vital to the production of a product and cannot be salvaged, it is disastrous *for that agency* but perhaps not for the general community. [2]

Disasters affecting records

Records are always potentially at risk of disaster. Due to the importance of records, their loss in a disaster can be crippling for the responsible government agency. Disasters affecting records may include:

- natural events or hazards including earthquakes, cyclones, bushfires, floods, vermin, lightning strikes, windstorms
- structural or building failure such as malfunctioning sprinklers, heating or air conditioning systems, leaks in roofs, poor wiring, sewer/ stormwater/ drainage failure, energy failure
- industrial accidents such as nuclear or chemical spills, fire, explosions, gas leaks, falling object damage
- technological disasters such as viruses and computer equipment failures
- criminal behaviour such as theft, arson, espionage, vandalism, riots, bombing, demonstrations, terrorism and war
- accidental loss through human error.

Disasters may also be caused by storage conditions that are unsuitable for the media stored, and by the natural decay of materials.

Disasters affecting Australian organisations

Thousands of records facilities worldwide have suffered damage in disasters. Organisations in Australia have been relatively lucky in comparison, although many disasters have not been reported. Some of the disasters that have affected records in Local, State and Commonwealth agencies since 1974 include: [3]

- Floods, Brisbane (1974) – many government departments suffered damage. For example, the Children's Services Department had files submerged in two metres of water for two days, including vital and unduplicated records relating to adoptions. Staff at the Queensland State Archives headed recovery efforts.
- Cyclone Tracy, Darwin (1974) – in the cyclone many government departments suffered losses. Boxed files and those in filing cabinets fared well, but exposed files were mouldy and in a deplorable condition. The Australian Archives set up a reclamation centre in Brisbane to treat them.
- Floods, Perth (1988) – water seeped in the basement of the Supreme Court of Western Australia. LISWA (Library and Information Service of Western Australia) was called in to assist and their plan was adapted as a model.

---

[2] J. Doig. Disaster Recovery for Archives, *Libraries and Records Management Systems in Australia and New Zealand*, Centre for Information Studies, Wagga Wagga, 1997, p.35.

[3] *Ibid*., pp.5-24.

- Fire, Perth (1994) – a fire in the Architectural Division of the West Australian Building Management Authority caused damage to a large collection of active files including charring to edges and water saturation. As they only had short-term value, they were microfilmed and originals destroyed.

- Fire, Melbourne (1994) – a fire gutted the ground floor of the Knox Civic Centre in Victoria. A commercial company was called in to carry out the salvage and restoration of municipal records. The council leased a nearby building and restored services fairly quickly.

- Fire, Fremantle (1994) – there was a fire following a break-in at the Law Courts. There was no sprinkler system and the majority of paper-based records were destroyed. Paper materials, that survived, were badly damaged.

- Flooding, Hobart (1994) – over Christmas water from a heavy rainstorm partially flooded the strong room of a government agency. Some material was air dried successfully but other records were lost.

- Fire, Melbourne (1994) – there was an explosion in the transformer at an SEC substation, that caused fires in tanks.   Melbourne City Archives was located on the floor above. While the fire did not spread to the Archives, soot and smoke did.   A commercial company was contracted to clean, involving the removal of soot from 25,000 rolled plans, and plans in 139 plan cabinets.

- Another more recent disaster was the fire at Bankstown City Council Civic Centre on 1 July 1997. [4] The fire destroyed much of the building and damages exceeded $30 million. Luckily many of the paper-based records were not destroyed in the fire, although water damage was extensive. The mainframe system's on-site storage tape was not destroyed in the fire either, allowing access to the data (even though it had to be sent to France to read). The Bankstown Council fire was not as disastrous as it could have been and business continuity was soon restored on a limited capacity at another site.

- In 2001 two separate fires occurred at Pennant Hills High School, Sydney, over one weekend. Initial losses included the labours of the school's Higher School Certificate students involving major Art, Design and Technology, and Wood Technics projects that represent more than a year's work for some students. The second blaze destroyed 12 classrooms, all school records, and the principal's office.

These examples are by no means comprehensive. There are likely to be many more unreported disasters. However, they illustrate that Australian Government records facilities are not immune to disasters. Records are corporate assets and as such need to be protected by a number of measures, including counter disaster strategies.

Counter disaster management for records

Counter disaster management is the term given to strategies for the prevention, preparedness and response to disasters, and the recovery of operations following disasters.

Counter disaster management for records should take place in the framework of a government agency's business continuity plan. Within that framework there are 4 stages:

---

[4] *Image and Data Manager*, January/February 1998, pp.12-13.

- assessment of risks affecting records and recordkeeping systems, and the subsequent activities to reduce the probability of a disaster and reducing the probability of loss should a disaster occur
- planning activities to establish a counter disaster plan to assist the government agency to respond to an emergency event
- the activities to identify and protect vital records of the agency
- response and recovery from a disaster: the activities involved in implementing the plan and initiating resources to protect or secure the organisation from loss, and restoring records and operations, so that normal business operations can resume.

These guidelines give practical guidance on how to undertake risk assessment, planning, vital records protection, and response and recovery activities in order to avoid disasters and to minimise the impact and damage of a disaster on records and recordkeeping systems.

Disaster review of your agency

Agencies are encouraged to undertake a disaster review of their organisation. This review should highlight the history of disasters within your agency and is intended to familiarise staff with risks to their records and recordkeeping systems and their potential impact. This review should also include an assessment of disasters experienced by agencies serving similar functions and agencies located within a close proximity of your agency. For example, an agency situated close to a chemical plant will need to prepare for possible disasters that could occur at that site as any disaster may have a huge impact on your agency and your records.

The disaster review should begin by a brain storming session with staff responsible for the development of the Records Management Disaster Recovery Plan. Long-term employees within an agency may be able to provide useful information regarding past disasters, accidents or emergencies previously experienced by the agency. You may also consider a walk through your premises with staff and record anything that may be a potential hazard or danger to your organisation (also refer to *Records Management Disaster Planning Toolkit –* **Disaster Review Form**)[5].

Risk Assessment

Risks affecting records and recordkeeping systems should be identified and assessed.[6]

Risk management is recognised as an integral part of good management practice within the South Australian Government. The risk management process involves:

---

[5] Heritage Council Collection, Department of Communications, Information Technology and the Arts, Be Prepared: *Guidelines for small museums for writing a disaster preparedness plan*, 2000, pg 16 & 17.

[6] State Records NSW, Standard on Counter Disaster Strategies for Records and Recordkeeping Systems (Standard no: 6), 2002, p.2.

> *"the systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk."* [7]

This section of the guideline is designed to assist records managers to contribute to the agency's broad risk management programs. In addition, the scope of this section has been intentionally widened so that if risks to records have been neglected in the initial broad risk assessment of the organisation, records project teams can address them as part of the counter disaster strategies project. Ideally, of course, risk management programs should include assessments of risks to records and recordkeeping systems as part of the risk management program.

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

- establish the context
- identify the risks to records and recordkeeping systems
- analyse the risks in terms of probability and effect
- assess the risks in terms of acceptability and priorities for treatment
- treat the risks by identifying, evaluating and implementing options (this involves developing and implementing a counter disaster plan)
- monitor and review.

Establish the context

The risk management process needs to occur within the framework of the agency's strategic, organisational and risk management context. This context defines 'the basic parameters within which risks must be managed and to provide guidance for decisions within more detailed risk management studies' [8], for example, the counter disaster plan.

In order to understand the agency's context, staff will need to identify and document the role of the organisation, its structure, the business, regulatory and socio-political environments in which it operates, and major factors affecting its recordkeeping practices. One of the key outcomes of the preliminary investigation will be a general appreciation of the organisation's recordkeeping strengths and weaknesses.

Identify the risks

The next step in the process is to identify all potential risks to records and recordkeeping systems, their possible causes and consequences. Risks can be identified by:

- brainstorming with key employees who have a knowledge of the building/s and agency processes
- using established checklists to find inadequacies

---

[7] Australian/New Zealand Standard AS 4360-1999, *Risk Management*, Definitions, 1.3.26, p.4.

[8] Australian/New Zealand Standard AS 4360-1999, *Risk Management*, Chapter 4, *Risk Management Process*, p.9.

- discussing risks with professionals like risk managers, emergency services and auditors
- making judgments based on experience
- employing systems analysis, scenario analysis, or systems engineering techniques.

Remember that risks to records and recordkeeping systems can come from:
- natural perils: such as earthquakes, cyclones, bushfires, floods, vermin
- structural or building failure: such as malfunctioning sprinklers, heating or air conditioning systems, leaks in roofs, poor wiring
- industrial accidents: such as nuclear or chemical spills
- technological disasters: such as viruses and computer equipment failures
- criminal behaviour: such as theft, arson, espionage, vandalism, rioting, terrorism and war
- accidental loss through human error.

Refer to *Records Management Disaster Planning Toolkit* – **Hazard Checklist** to assist in identifying potential hazards in your organisation.

Destruction may also result from:
- unstable records, such as combustible nitrate film,
  or
- chemical degradation of records caused by natural deterioration, hot, polluted environments, improper shelving, and inadequate precautions in transit or careless handling or work procedures.

One of the most important ways to identify potential disasters is to conduct regular risk audits of the building and its surroundings, and records storage locations. A risk audit involves examining the following to detect risks:
- building locations: for example, are they close to rivers? Airports? Chemical factories?
- building structure and fabric: for example, wire and pipe positioning and state of repair
- existing fire and water detection systems
- existing fire suppression systems
- existing maintenance regimes: for example, cleaning, servicing of heating ventilation and air conditioning systems, and electricity
- storage areas and containers for types of records
- storage areas for flammable materials
- electronic recordkeeping systems and existing security and protection measures
- security control mechanisms
- relevant procedures: for example, smoking restrictions, records handling procedures.

Risk audits should be applied to the agency's vital records to see whether they are adequately protected and accessible to staff that require them. Risk audits for vital records should also identify the impact on business activities, such as service delivery functions, legal liability and financial functions, if such records were lost or unrecoverable. Further guidance on identifying and protecting vital records is provided below.

Risk audits should also be applied to electronic records and their locations. Usage conditions and patterns that may increase the vulnerability of electronic records should be studied, as should the existing security procedures. Additional risks inherent in electronic formats, such as the risks of disk crashes, system failures, organisational threats, hardware failure, programming errors, viruses and hackers should also be examined. Risks inherent in the use of Local Area Networks (LAN), Wide Area Networks (WAN) and the Internet/Intranet also require identification. Many data processing functions can be deferred and thus do not become critical when outages or interruptions are of a short duration. However, as the length of the outage span increases due to a disaster, more and more data processing tasks and functions become critical to the organisation.

Government agencies should consult the Security Adviser within Government Information and Communication Technology Services for South Australian Government (Government ICTS). Government ICTS has developed the Information Security Management Framework (ISMF) version 1, April 2003. This Framework presents a set of policies, standards, guidelines and control mechanisms for South Australian Government agencies to use in developing their information security capabilities. The standard AS/NZS ISO/IEC 17799:2001 *Information technology – Code of Practice for Information Security Management* should also be consulted.

There are a number of possible risk management models. Included in the *Records Management Disaster Planning Toolkit* are tools that may assist an agency with applying the risk management framework and document the process for evidential purposes. Refer to the **Risk Management section of the Toolkit** for further information.

Critical needs determination

Agencies may have also determined their critical needs for information (often located in records and recordkeeping systems) and equipment that would be required in order to continue operations should the agency be damaged, destroyed or become inaccessible. Critical needs determinations are usually undertaken as part of business continuity planning processes. Knowledge gained during these processes should be assessed and incorporated into risk assessments and vital records identification.

Critical needs determination is based on data gathered from within and outside the organisation involving a set of inventories and checklists. If the recovery lead-time for replacing any item is unacceptable then a backup alternative is usually considered. Whilst the determination generally focuses on equipment, IT and contact information, it is important to incorporate requirements for records storage facilities and recordkeeping systems.

A series of critical needs questions are listed in the *Records Management Disaster Planning Toolkit* – **Critical Needs Questionnaire Checklist**.

Analyse the risks

The next step in risk management is to analyse risks in terms of probability and effect. This involves looking at the risks identified and estimating the likelihood of their occurrence in the context of existing control measures. The consequences of particular risks also need to be considered. The aim of this assessment is to separate the minor acceptable risks from the major risks and to provide data to assist in the assessment and treatment of risks.

A simple qualitative method of analysing risks is to chart risks on a matrix like the one illustrated below.

Probability	**high**	2	1
	low	4	3

low >> high

Effect >>

In this diagram, 1 = greatest risk and 4 = least risk. Examples of 1 ratings may include fire, cyclone, flood, burst water main; examples of 2 may be a leaking tap or vandalism; examples of 3, nuclear war; and examples of 4, shelving collapse. Threats may vary in intensity depending on the government agency. [9]

Considerations in analysing risk also include:
- investigating the frequency of particular types of disasters (often versus seldom)
- determining the degree of predictability of the disaster
- analysing the speed of onset of the disaster (sudden versus gradual)
- determining the amount of forewarning associated with the disaster
- estimating the duration of the disaster
- considering the impact of a disaster on two scenarios:
    - vital records are destroyed
    - vital records are not destroyed.

Government agencies should also draw on their past work and methodologies used in analysing risks to their records and recordkeeping systems, for example South Australian Government agencies may have used particular methodologies as part of their preparation for dealing with Y2K risks.

There are also other, more complex risk management methodologies, such as semi-quantitative and quantitative rating. The methodology chosen will depend on the needs and the expertise available to the agency. See the bibliography for more information.

Assess the risks

Risk assessment involves assessing the acceptability of the risk and priorities for treatment. In the diagram above, low probability and low effect risks might be assessed and accepted, monitored and periodically reviewed. Higher risks should be prioritised and treated. A risk assessment Template can be located in the *Records Management Disaster Planning Toolkit*

---

[9] Doig, *op cit*., pp.2-3.

– **Risk Assessment Template** to assist agencies in assessing risks and potential hazards to your agency.

Treat the risks

Once risks have been assessed, to determine which require treatment, the agency needs to look at treating risks.

This phase of risk management involves:

- identifying the range of options for treating risks
- evaluating options on the basis of the extent of risk reduction and the extent of benefits or opportunities created at what cost
- implementing the options.

For the major risks identified, agencies should document in a Risk Reduction Plan how the chosen options will be implemented, responsibilities, schedules, expected outcomes, budgets, performance measures and a review process. A risk reduction template is located in the *Records Management Disaster Planning Toolkit* – as **Action Plan to Reduce or Remove Risks Template**.

Treatment for risks may involve:

- choosing a new building on a low risk site
- modifying an existing building to ensure risks are removed or minimised
- modifying existing services and practices, for example, not storing records on the floor, changing security and access arrangements
- implementing protective mechanisms such as:
  - detection and suppression systems, security systems (see bibliography)
  - boxes or secure packaging for all records and fire proof safes for vital records
  - copying programs for vital records.
- writing policies and procedures to address risks in practices or service provision
- developing and implementing a counter disaster plan for records and recordkeeping systems.

Treatment for electronic records should include:

- general controls that affect all computer systems, like organisation controls, systems development, maintenance, documentation controls, access controls, data and procedural controls, physical security, password systems and communication security
- application controls unique to specific applications, like input controls, processing controls and output controls.

For more information on control measures, consult the Australian/New Zealand Standard AS/NZS ISO/IEC 17799:2001 4444-1996, *Information Technology – Code of practice for information security management.*

Monitor and review

Monitoring and review of risk management programs should be continuous and should cover seasonal, short and long term risks, the implementation of treatment plans and the effectiveness of control mechanisms to ensure changing circumstances do not alter risk priorities.

The Australian/New Zealand Standard AS/NZS 4360:1999 *Risk Management* notes:

> *"Few risks remain static. Ongoing review is essential to ensure that the [risk] management plan remains relevant... it is therefore necessary to regularly repeat the risk management cycle."* [10]

Planning

Outcome 7 of *Adequate Records Management: Meeting the Standard* (2002) requires records management to be managed and planned in a strategic and corporate manner. One of the benchmarks for meeting adequacy for Outcome 7 is the development of a disaster recovery plan for official records. This section covers the process of preparing a counter disaster plan to respond to identified risks to records and recordkeeping systems.

Many government agencies will have different approaches to the planning phases of counter disaster management for records and recordkeeping systems. For example, some may wish to include prevention plans and preparedness, response and recovery plans together in the one document. Others will separate them to facilitate updating and ease of response and recovery in an emergency. If the plans are separated, it is important that the vital records schedule and listings of other significant or vulnerable holdings are attached to the response and recovery plans so that priorities are clear. Other related information like emergency evacuation procedures should be linked to the response and recovery plans. Security plans meet many of the preparedness needs for electronic records and should also be linked.

Writers on counter disaster planning usually advocate one of two approaches for response and recovery plans:

- minimalist planning - so that the plans are easily updateable and less resource intensive, and so that response is facilitated
- long written plans containing details on how to respond to the major disasters for each of the record formats.

The level of detail will depend on the resources and time available for the development of the plan and the cost-benefit analyses conducted. It is important to plan for the most likely disasters identified in the risk assessment. For example, organisations can reasonably expect to treat the effects of fire and water. However, in a disaster, staff will be under pressure so the plans should be as concise and easy to follow as possible.

Alternatively, detailed plans can be prepared for those coordinating response and recovery. Make these *as simple as possible* and include indexes, tables of contents, flow charts and

---

[10] Australian/New Zealand Standard AS 4360-1999, *Risk Management*, Chapter 4, *Risk Management process*, p.20.

graphics so they can be implemented easily. Single page extractable response and recovery information can also be provided in the form of steps or illustrations that can be circulated to all staff and kept for reference at strategic points on and off the premises.

If government agencies wish to reduce the time and effort expended in preparing response and recovery plans, they may use generic plans. They could also draw on existing plans from similar institutions, or from other branches of their own organisation. Remember, if generic or other plans are used as a basis they need to be adapted to the specific needs of the agency's records.

Where a generic package is used, the package should only be seen as the first step in developing a comprehensive plan. Identification and consideration of specific risks to the agency is still required. Whether the plan is developed completely in-house or based on a generic package, the need for specialist advice, such as conservators and disaster recovery specialists, should be considered.

Project Planning

Developing a counter disaster plan for records and recordkeeping systems should be managed as a project. It is possible that this counter disaster plan will form part of a larger project to safeguard corporate assets.

Like all projects, someone should be assigned the responsibility to coordinate the project. They would be responsible for:

- project planning
- developing policy for endorsement by the chief executive officer
- defining the scope, objectives and limits of the project
- selecting a team to work on the project
- allocating appropriate resources
- determining requirements for professional assistance, training and/or outsourcing.

A reporting structure should be established so that senior management can supervise and monitor the project.

Project team responsibilities

The size and responsibilities of the team can vary according to the agency and the risks that need to be addressed in the counter disaster plan. Representatives should include the chief information officer, as well as the occupational health and safety director, and the building/facilities manager.

Teams and team leaders should receive training commensurate with their duties. For example, the project teams may need training in how to conduct risk assessments, the identification of vital records and project management methodologies.

One of the vital components of the counter disaster management project is the need to communicate the objectives and progress of the project to staff, management and other stakeholders in order to gain their support and assistance; a communication plan would assist in this process.

This is a useful step in preparing staff for training activities to be conducted once the counter disaster plan is prepared.

Content of the plan

The basic components of the plan may vary according to organisational needs, but should include the following:

- a list of vital records, particularly significant or vulnerable holdings, and location and control documentation
- a list of equipment and materials available for use in disaster salvage and recovery
- the function, composition and chain of command of the salvage and recovery team and their contact information
- procedures for identification and declaration of a disaster situation and initiation of the disaster response chain of command by the normal business operation
- provisions for the training and current awareness of the team
- a list of sources of back-up resources, including expertise, trades people, materials, equipment, vehicles and accommodation
- procedures for updating and testing plan
- simple technical information on the handling of damaged material, directed towards establishing priorities for early action.

The counter disaster plan should be supported by:

- a clear policy statement that mandates the plan and defines responsibilities
- vital records and risk management procedures
- results of the risk assessment and analysis
- copies of current ongoing contracts (like vital records storage, pest control, emergency equipment and supplies) and contact details
- arrangements for reviewing risks and contracts, and revising procedures. [11]

A model counter disaster plan is provided in the *Records Management Disaster Planning Toolkit* – **Contents of Disaster Preparedness Plan Checklist**. The checklist may be used to check that all aspects of counter disaster management have been covered through the planning process.

A clearly written counter disaster plan is much easier to maintain, implement and use. Tips in writing the detailed procedures include:

- write the plan with the assumption it may be implemented by personnel unfamiliar with the operations of the organisation
- use direct language
- use short paragraphs
- present one idea at a time

---

[11] Jones and Keyes, *Emergency Management for Records and Information Programs*, ARMA International, Kansas, 1997, pp.35-38.

- use active voice verbs

- use the imperative style where a sentence starts with a verb

- use a standard format

- avoid jargon

- use position titles (rather than personal names) to reduce maintenance and revision requirements

- develop uniformity in procedures to simplify the training process and minimise exceptions to conditions and actions

- identify events that occur in parallel, and events that must occur sequentially

- interlink with supporting documentation and inventories.

How to prepare the response and recovery plan

The response and recovery plan forms an important part of the counter disaster plan. Consultants can be hired to develop the response and recovery aspects of the plan or an internal team can be appointed. If internal staff members are allocated the responsibility, they should represent employees from all areas of the organisation. The response and recovery team need to:

Determine the preparedness strategy

By employing methods like research, brainstorming and simulations, the team can determine what the agency has to do to prepare for the most likely disasters. For example, if bushfires have been identified as a risk, the team needs to brainstorm the steps necessary to prepare for and control the emergency. These steps may cover:

- what to do at the beginning of bushfire season

- what to do when the public office has been alerted to the presence of a bushfire in the area

- what to do when a bushfire threatens the premises.

Determine a response strategy

The team should also consider what initial action the organisation should take when a disaster occurs, who should be called and in what order, and what further action is required. Response strategies may be determined by function if that is useful. Remember that there will be priorities in responding and recovering records affected by the disaster.

Determine a recovery strategy

Simulations and brainstorming sessions should also be used to consider the action needed to ensure that recovery is facilitated. These include, for example, damage assessment strategies, alternative sites for resuming business operations, vendor assistance, alternative sites for recovery operations, and the use of vital record duplicates.

Collect data

The other major task for the team is to collect information that relates to all the phases of counter disaster management. This involves utilising the supporting documentation and inventories that will interlink with the counter disaster plan. These include user manuals,

technical documents, job descriptions, floor plans, hardware and applications inventories, vendor contacts, emergency contacts, etc. These lists are described below under Lists and Supplies.

This process may also be done through a critical needs determination with data gathered from within and outside of the organisation involving a set of inventories and checklists. This method could be chosen if an agency has not continually maintained or updated its counter disaster plan with the consequent rise in vulnerability or it is has just been established. A critical needs checklist is available in the *Records Management Disaster Planning Toolkit* – **Critical Needs Questionnaire Checklist**.

Teams should meet for regular briefings and should regularly report to staff and senior management about progress.

Components of the response and recovery plan

Response and recovery plans are a component of the counter disaster plan and should describe the specific procedures for personnel to follow from the time a disaster is discovered until the preparation of the final report. Information necessary for implementation should also be included.

Plans should include:

Policy statement

This should define the main terms: outline the purpose of the plan, goals and objectives, benefits, scope and impacts, the plan components and statements of policy and legal authority. Senior management should sign it.

The planning process needs to be approved of and supported by the CEO.

Responsibilities, authority and task organisation

The broad responsibilities and duties of personnel should be outlined, including those responsible for plan maintenance and distribution. In some agencies it may also be advisable to establish clear lines of authority in the succession hierarchy if the leaders designated in the plan are incapacitated or unavailable.

Senior officers and managers need to be given the time and authority to be accountable for this plan. Once a manager is given the role of disaster coordinator they should be supported and assisted.

Information distribution procedures

The major communication methods required in an emergency should be described. For example, the plan should nominate staff to deal with the media in times of crisis to ensure that accurate and authoritative information is given.

Preparedness steps

Preparedness steps for each emergency scenario, based on risk assessment, should be described. For example, if the organisation is at risk of flooding, steps should be described as to how to prepare for the likelihood of such an emergency.

Response and recovery steps

Response and recovery steps for each emergency scenario, based on risk assessment, should be described. Checklists, steps or illustrations can be used to promote clarity. Priorities for salvage and recovery, such as vital records, should be clearly identified in this section of the plan.

These sections should provide all the information needed to activate the plan, assess damage and stabilise and secure the situation and environment and initiate contingency and recovery activities. Immediate action procedures for responding to the major types of disasters should be provided. Refer to sections below on Response and Recovery for further information.

The *Primer on Disaster Preparedness, Management and Response: Paper-Based Materials* (see bibliography) provides general examples of immediate action to be taken in case of fire, severe storms, hurricanes, tornadoes, winter storms, utility failure, flood, hazardous material accidents, civil disorder and demonstrations, terrorism, bomb threat, explosion, major transport accident or earthquake.

Simple technical information on the handling and salvage of damaged material and priorities, that covers the major record formats and their treatment requirements, should also be given or provided as appendices to response and recovery information. See *Records Management Disaster Planning Toolkit* – **Packing records in recovery operation** and the bibliography for further information.

Some records may carry access restrictions and only staff with the proper clearance should be allowed to handle those records in an emergency.

Another issue to be considered and documented is arrangements for helping staff during a disaster. While the response and recovery plan describes procedures to be undertaken, it is important to remember that staff will need regular breaks, food and drink and variation of duties in the response and recovery process. Continuous and effective communication is necessary to ensure effective recovery operations. Staff may also need to be provided with safety clothing and briefed to avoid dangers. Organisations may consider it useful to include an overtime policy in the counter disaster plan so staff expectations are clear (see the bibliography for more information on staff needs).

In terms of professional and volunteer disaster managers the *Australian National Emergency Management Competency Standards* (EMA 1995) identify the need for them to be competent in the use of information. This concept is outlined in two specific competency units – Unit 10 Manage Information and Unit 11 Process Information – covering the processes of collection, recording, verification, interpretation, structuring, collation and dissemination of emergency management information. By carrying out all of these processes a disaster manager should be able to deliver effective and sustainable decisions for emergency response personnel, at disaster sites, and across the organisation.

Goals and objectives for training, testing and review

The counter disaster plan may also include goals and objectives, and program information for training employees, conducting exercises, and reviewing and updating the plan. If desired, these may be documented separately to the response and recovery plans.

Putting plans to the test are also an excellent way to train coordinators and members of recovery teams in specific techniques and improve their confidence and knowledge. Weaknesses in the plan may be revealed and corrected, and coordination and communication improved. Tests should occur during the plan development and then on an annual basis.

Lists and supplies

A vital part of planning involves compiling and frequently updating lists of materials and contacts that can be used in a disaster. Having these lists available both on and offsite enables the fast and efficient procurement of services and equipment. The lists to include will depend on the needs of the agency and the resources available to them. An ideal set of lists may include:

- contact details for the nearest fire brigade, emergency services, police, hospitals and WorkCover officials
- contact details of the disaster response coordinator and team
- staff resources including blood donors, first aid officers, and those with experience in emergency relief, the military or police force
- details of alternative sites, including operating sites and treatment sites nearby
- lists of equipment and materials available and where additional emergency supplies/services might be obtained
- inventories of computer and communication equipment and details of arrangements for their replacement in a disaster
- inventories of computer software and programs and details of arrangements for their replacement in a disaster
- details of storage sites for vital records
- contact details for insurance agents
- contact details for records disaster recovery specialists and conservators (lists should note their areas of expertise)
- vital record/priority schedules
- building plans showing storage areas, exits, extinguishers, alarms, master switches and the location of vital records
- location details for master keys**
- a list of pertinent customers that will need to be informed quickly
- details of trauma counselling services
- television, radio and newspaper contacts in case statements need to be released
- 'action sheets' describing procedures for each recovery team
- other proforma and recording sheets for disaster activities
- reading lists on disaster management.

**Some information (like the location of master keys) may need to be restricted to a few senior people as, in the wrong hands, they may *cause* a disaster.

Insurance and emergency funding arrangements

Details of insurance arrangements can be included in the plan, attached as an appendix, or kept as a separate but related document. When planning for insurance, check with experts to ensure the right types and limits of policy coverage are selected for specific exposures. The following costs need to be taken into account:

- salvage and repair of items
- the replacement of items irretrievably damaged, or more economically replaced than restored
- freezing and storage of records
- business interruption
- employing disaster recovery companies
- supplies
- software
- restoring the site, for example, cleaning carpets and walls, replacing furniture
- temporary alternate sites for air drying and for business continuity
- staff overtime and hiring of temporary staff.

Note that permission from the insurance agent to commence response and recovery action should be pre-arranged. It is also vital that insurance is upgraded each year to cover changes in the agency.

The following details should also be included in plans: how emergency funds might be obtained during business hours and during weekends and evenings; who can authorise them, and how much can be obtained.

On-site equipment

Project teams should consider maintaining on-site equipment to help mitigate water damage. The common practice is to have disaster 'bins' at strategic points around the building containing paper towels, plastic sheeting, torches and similar supplies. Refer to the *Records Management Disaster Planning Toolkit* – **Disaster Bin Checklist** and **Disaster Store Checklist** for details of the contents of disaster recovery bins and storerooms.

Agencies may decide to keep additional materials that are too large for the 'bins' such as dehumidifiers or large fans, or items that are likely to be 'souvenired' in lockable rooms. These can be held on-site, or several organisations can arrange to share a resource room.

The location of disaster bins and rooms should be listed in the plan along with information on where to obtain keys if rooms are locked. Sources of additional supplies should also be listed in the plan.

Implementing the plan

Implementation of the plan involves:
- employee training to prevent unsafe practices or carelessness
- regular building and equipment inspections and maintenance to avoid building and equipment malfunctions

- installation of fire, water and movement alarms
- establishment of an information security program to protect information
- establishment of prevention, response and recovery contracts so that vendors can be on hand in an emergency.[12]

For the plan to be implemented successfully, agencies will also need to:

- assign responsibility for the implementation and ongoing maintenance of the plan
- involve staff in the process of implementing the plan
- place a priority on vital records and critical data recovery
- regularly practice and test the plan through training exercises.

Maintaining the plan

The counter disaster plan needs to be regularly tested and maintained in order to be relevant. It should be reviewed and improved regularly to reflect current operating environment and functions, for example when there are:

- changes to personnel assigned responsibilities within the plan
- changes in procedures
- new vital records
- new equipment or systems
- new building locations or changes to building structures
- changes to standards or best practice.

The plan should be tested periodically to maintain awareness of the plan, and to reveal any flaws in the plan. Supplies in disaster bins and rooms also need to be checked regularly to ensure that they have not been tampered with or depleted. Formal responsibility for the review should be assigned.

Reviews should be conducted after testing and after emergency situations to consider successes and failures and how implementation procedures might be changed to work more effectively. Refer to the section below on post-disaster analysis for further details. Internal audits of the counter disaster plan may also be conducted on at least a yearly basis. Changes to the plan should be documented to show the history of plan development. Agencies may also consider having their plan externally audited by a disaster management service provider.

Distribution issues

It is advisable that the counter disaster plan is widely distributed in paper form, as well as placed on the organisation's intranet. Having paper copies of the counter disaster plan is important, as intranets may be inaccessible during an emergency.

To facilitate plan maintenance, it is important to monitor and track each copy of the plan. A distribution log can be used as a record and control all copies of the counter disaster plan issued to various officers. A master distribution list can also be maintained for backup

---

[12] *Ibid*., pp.35-38.

purposes. Each authorised copy of the plan should contain a version identification number and the recipient should be recorded on the distribution list. Each officer with a copy of the plan is responsible for the security and control of the document in accordance with organisational policies.

Plan maintenance responsibilities

Plan maintenance responsibilities should be clearly defined in both the plan and in the individual position descriptions for those with maintenance responsibilities. Responsibilities may be divided among the counter disaster planner, team members, branch/section heads, senior management, and internal audit.

Training and testing

A plan is not a plan until it has been tested. Plans need to be maintained to accommodate change. If these two principles are not acted upon then the value of the human and financial investment by the organisation in its counter disaster plan (no matter how large) will dwindle as time passes. If an organisation has been fortunate enough not to experience a disaster event for a prolonged time then there is often an unwillingness to renew the disaster plan.

The objectives of counter disaster plan testing include:
* revealing any flaws in the plan
* gaining feedback on any problems while implementing the plan
* gauging organisational responses to the suggested recovery procedures
* training the disaster management team
* practicing debriefing of staff
* preparing for post disaster analysis.

Once plans are in place, senior officers and managers need to ensure that all staff learn the necessary skills and practice their response or recovery tasks. Training can use a sequence of learning and rehearsal approaches, involving:
* background reading of books, publishes articles, the Internet
* lectures
* videos
* case studies of past disasters
* computer based exercises
* computer simulations
* tabletop exercises
* field exercises
* full scale field exercises (scenario based exercises).

Training allows participants to become acquainted with the counter disaster plan and their designated roles within it. Through rehearsal, respondents can interact with each other and determine task requirements while mobilisation, assembly, and deployment measures can also be tested. The training outcome should be an increased awareness of potential disaster situations and increased experience of managing a disaster. The central theme is for the

organisation's approach to disaster management to move towards coordinated activities across the organisation.

Initial training should include walk-throughs of the counter disaster plan with the emphasis on familiarisation plus the checking of its accuracy and workability. This can then be followed by small unit practice of specific response tasks. This should focus on checking whether staff can perform the required tasks, along with checks of the equipment and resources. Following on from this staff deployment and communications can be tested in field or 'hands on' exercises. Scenario training can then be used through three approaches:

- case study or conference room analysis
- tabletop exercise of the management team
- field based exercises.

Building upon these measures a full-scale scenario exercise can be developed where many or all of the elements and roles in the disaster response plan are tested.

Disaster management training is available through State Records Business Recordkeeping Certificate 4 and Diploma courses. Doig (see bibliography) gives practical advice about developing simulations and training sites and evaluating and reviewing participants, if agencies wish to compile and run their own.

A counter disaster plan needs to be checked for its relevance and accuracy over time otherwise post planning changes may hinder or halt the plan from working. Existing counter disaster and recovery plans should be changed to incorporate:

- alterations to interior design (including blocked off or removed emergency exit paths, new positioning of emergency equipment and disaster bins)
- alterations to building access measures including loading bay space, new entrances, and transport zones)
- new equipment
- changes in the storage of hazardous goods
- changes in work practices (shift times, core resources and skills)
- changes in organisational structures (expansion, contraction, resizing, downsizing that removes, replaces or makes redundant the persons and positions that would have contributed to response and recovery action)
- changes in software, hardware, work tools and organisational records that will affect designated warm or hot site resources and equipment
- changes in personnel.

Post disaster analysis

The analysis of the disaster needs to be carried out by impartial reviewers either by outside consultants or a senior management team made up of officers not involved in the disaster event. If this is not possible due to the organisation's size then some of the reviewers should be from other organisations. An assessment from the actual disaster response team is neither desirable nor appropriate.

It needs to be emphasised that each disaster and subsequent response is unique and requires a thorough investigation. The post disaster analysis should include:

- a narrative of the actual disaster event – what happened, why and how and what caused the event?
- a summary of the order and events of the disaster response
- any effects on records or recordkeeping systems
- the loss of any records and their subsequent replacement or restoration
- the damage to information infrastructure or interruption to services
- the follow up activities leading to the resumption of service
- the levels of cooperation that occurred between different sections of the organisation during the disaster
- the precautions that were taken for the safety of employees, volunteers and visitors present at the disaster area and how successfully were these measures carried out
- an assessment of any barriers to communication among the disaster respondents
- the handling of equipment during the disaster
- ability of staff to follow procedures in recovery plan
- the ability of local officers to deviate from the detailed plan in emergencies arising during disaster response operations
- an analysis of leadership shown by local officers
- an analysis of leadership and support shown by senior management
- an analysis of organisational support given to the CEO during the disaster response and recovery period
- the role of outside agencies
- a review of disaster response recordkeeping
- the effectiveness of information management (including data collection, validation, and exchange and communications interactions with people outside the disaster situation and media representatives).

The resulting information should be assembled into a report on the disaster event, including its consequences and the organisation's response, the loss of any records and their subsequent replacement and/or the restoration of any recordkeeping systems.

Vital Records Protection

Outcome 7 of *Adequate Records Management: Meeting the Standard* (2002) requires records management to be managed and planned in a strategic and corporate manner. One of the benchmarks for meeting adequacy for this outcome is the identification of vital records. This section covers this essential component of the counter disaster plan, the identification and protection of vital records.

Vital records are records, in any format, that contain information essential to the survival of an organisation. If a vital record is lost, damaged, destroyed or otherwise unavailable, the loss is a disaster, affecting critical operations. Vital records should be the main priorities for recovery and salvage efforts when a disaster occurs.

Vital records include records that are needed to:
- operate the organisation during a disaster

- re-establish the organisation's functions after a disaster

- establish and protect the rights and interests of the organisation and its clients.

Vital records usually constitute a small percentage of records created by an organisation, normally 5%, however the range can vary from 3% to 10%. Depending on the business of the organisation, vital records might include:

- contracts/agreements that prove ownership of property, equipment, vehicles, products

- records about the operation of the agency, such as current or un-audited accounting and tax records, current personnel and payroll records

- current client files

- standard operating procedures

- control documentation (registers, indexes, metadata repositories) for the agency's records and recordkeeping systems

- data critical to the reconstitution of the agency's electronic records

- permanent value records in the agency's custody.

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

A vital records program should be established within each agency's counter disaster plan. The program includes the policies, plans and procedures developed and implemented and the resources needed to identify, use, and protect vital records. The aims of the program are to:

> "provide an agency with the information it needs to conduct its business under other than normal operating conditions and to resume normal business afterward….the program enables [an] agency … to identify and protect the most important records dealing with the legal and financial rights both of the agency and of persons directly affected by the agency's actions."[13]

Identifying vital records

The first phase in protecting vital records is to identify what is 'vital' to the organisation. Remember to assess all records, including electronic records.

There are a number of strategies that can be used to identify vital records:

- assessing business continuity and resumption planning strategies, as some records will have been identified as essential in restoring critical functions

- assessing risk assessments, as some records will have been identified as essential or critical

- assessing organisational charts and related documentation to identify functions that are vital to the organisation

- assessing functions and records as part of the process of preparing disposal authorities or coordinating retention-oriented management actions for records in any format

---

[13] National Archives and Records Administration, *Vital Records and Records Disaster Mitigation and Recovery: An Instructional Guide.* 1999.

- reviewing organisational documentation.

Once functions are identified, each needs to be analysed by the project teams to determine what records are:

- vital records: those records that are irreplaceable and mission-critical
- important records: those records that are not irreplaceable but could be reproduced only at considerable expense, time and labour
- useful records: those records that, if lost, will cause some inconvenience but could be readily replaced
- non-essential records: those records that are listed in disposal authorities for routine destruction.

To validate the classifications, personnel responsible for the vital records program should interview program managers and personnel who create records. It is important to remember, however, that most program managers think that most of their records are vital. It is also important to apply good risk management principles when determining what records should be classified as vital by the agency.

Vital records may also be identified by reviewing:

- existing emergency plans and priority lists
- documentation created for contingency planning and risk assessment
- agency statutory and regulatory responsibilities
- functional/organisation charts
- records disposal authorities
- current file plans.

Another approach to identifying vital records may be to take 'a layered approach', particularly for larger government agencies. Such an approach allows project teams to consider the organisation as a corporate entity, and then to consider recordkeeping systems in other branches or divisions of the organisation. It is quite possible that such an approach will reveal the records vital to operate and re-establish the organisation after a disaster, and those records that are vital to a particular section of the organisation.

Once identified, vital records need to be listed. Lists should include the following:

- an identification number for each type of record
- the name of the area responsible for record series or the electronic recordkeeping system containing vital records
- the title of the series or electronic recordkeeping system
- an indication as to why it is considered vital
- the record format (is it paper or electronic, or another format?)
- all physical locations of originals and duplicates
- the frequency of update.

Refer to *Records Management Disaster Planning Toolkit* – **Vital Records List Template**.

Other information may include:

- the amount of reference activity and frequency
- existing records protection, such as the storage equipment used
- the cost of records protection (this may be initial, annual maintenance and total costs)
- the consequences of loss to the organisation
- how vital records are transported between the agency's locations
- when records are to be transferred to secondary storage or destroyed.

Taking a university as an example, there could be two basic categories of records regarded as vital:

- those that allow the protection of the rights of individuals
- those that allow the protection of the university's rights, assets, and the execution of its educational obligations.

The first group of records may include current payroll records necessary to pay employees, master academic records that show the completion of work, and employee service records for the protection of tenure and retirement.

The second group of records may include drawings and specifications required to maintain and repair university facilities, records necessary to establish the university's ownership of buildings, equipment, land, patent license agreements, research contracts, legal records that prove the university's stand on a particular issue in dispute, along with fiscal records that support the university's financial standings (accounts receivable or general ledgers).

The above examples are meant as a guide only as the identification of vital records can only be established by the judgment of the university using the appropriate identification criteria and seeking the contributions of the 'owners' and users of the records. Also depending on the university and its activities, more records categories could be designated as vital. This will involve reviewing the many types of records that are of great importance, aid the conduct of business, or have historic meaning to assess whether they are of vital importance.

Protecting vital records

Once identified, vital records then need to be protected through the inclusion of strategies within the counter disaster plan. This planning:

- ensures that emergency operating records vital to the continuity of essential business activities during a disaster will be available at relocation sites in the event that those sites are activated during emergency event
- safeguards rights and interests through the preservation of records essential to the legal rights and interests of individual citizens and the South Australian Government
- ensures that vital records are evaluated on the basis of their adequacy in facilitating emergency operations or in protecting the rights and interests of citizens and the Government
- employs control techniques to ensure that needed records are available at relocation sites
- ensures that records will be easily retrievable and maintained in usable condition
- ensures that the necessary finding aids are available at the sites
- ensures that a current inventory of records located at the sites is readily accessible.

Protecting vital records should cover both:

- measures to prevent or minimise the impact of a disaster event
- recovery and restoration measures if a disaster does occur.

Preventative measures

There are a number of possible preventative strategies. Each preventative measure should be evaluated to ensure that it is viable and cost effective for the agency. Agencies may choose to use a range of strategies depending upon the types of records formats that they need to protect. For example, it may be feasible to store vital paper records in a fireproof safe within a storage facility that has high levels of fire and security protection. Alternatively, an agency that has official records of permanent retention in its custody and possession may choose to transfer these vital records to State Records' custody and protection when no longer required for business purposes in accordance with *State Records Act 1997*.

Specific protection strategies for vital records may include:

- duplication and dispersal
- ensuring high levels of fire and security protection in storage containers and spaces, i.e. on-site and off-site storage
- establishing procedures for managing critical work in progress that may not be backed up or is located outside of storage facilities.

Duplication and dispersal means creating duplicate copies of records and storing these in secondary locations. If the agency is duplicating records, such as Board papers, it may be economical to duplicate the original medium to the same medium (eg. paper to paper, microfilm to microfilm), but considerations like the stability of the media and the cost of reproduction need to be taken into account. To maximise the cost benefit, agencies may wish to reproduce to a medium, such as microfilm, that can be used for other purposes besides protection. The costs of duplication and whether duplicates have the same legal value as the original also need to be considered.

When storing duplicates at another location, such as a branch of the organisation or a commercial storage facility, the agency need to ensure that the duplicates are secure and accessible only to authorised persons. Dispersal should be regular, the storage location and conditions should afford adequate protection, and housings should be appropriate for the media. Special equipment required to read vital records should also be stored at the dispersal location or alternative sources of this equipment listed in the counter disaster plan.

On-site storage involves housing vital records in fire resistant housings or file rooms (vaults) with appropriate suppression systems and security. However, records may still be vulnerable if the site suffers damage.

Agencies choosing to store vital records off-site are required to use facilities approved by State Records. If records are of permanent value, then they must be transferred to State Records Archives. However, agencies may decide to store back-ups or copies off-site. In this case, agencies should utilise the Approved Service Providers for the storage of these records. Please refer to the *Records Management Disaster Planning Toolkit* – **Storage and Handling Requirements Checklist** and *Records of Temporary Value – Management & Storage Guideline, 2002*.

The publication by Ted Ling (see bibliography) gives advice regarding the essential elements of purpose built archival repositories.

Protective measures for electronic records involve similar measures. Specifically designed filing cabinets and vaults can be used to provide on-site protection for magnetic tapes and disks. For example, vital electronic records can be protected against theft and fire by storing them in fire resistant safes or vaults with combination locks. Remember, fire resistant cabinets for paper and microforms do not provide sufficient protection for magnetic tapes, disks and diskettes, since the ignition point of paper and microfilm is higher than magnetic media.

The most effective approach for electronic media, is to duplicate and store duplicates in secure off-site storage. The production of backup copies of essential files should be a routine operating procedure. There should be full backup, not just backups of files that have been modified. If necessary PCs should be backed up as well as networks and the duration of backup storage should be sufficient for organisational needs. Backup schedules should be established and rigidly enforced and audited and responsibilities should be assigned to appropriate employees. Backup procedures should not only apply to information on fixed magnetic drives, but also for magnetic tapes, optical media and other media, and backup media should satisfy the security and recoverability requirements for their applications.

There are various backup methods and these should be discussed with information technology specialists. For vital records protection, backups are typically made on media that can be removed and stored offsite. Those offsite storage facilities used should have storage suitable for electronic records.

Preventative measures should also extend to critical work in progress that may not be backed up every day or is sitting on desks, or placed in open shelving. All data is not always backed up or stored off-site. Which business units in the organisation have exposure in these areas? It is important to identify and prioritise critical work in progress and then establish procedures, such as 'clean desk policy' or additional safety measures to reduce exposure.

Recovery and restoration

To facilitate systematic vital records recovery, the vital records recovery plan, i.e. the list of all vital records, their locations, and the procedures for the recovery of these records, should be included in the counter disaster plan for records and recordkeeping systems. The listing of all vital records should include the location of buildings and room locations, and floor plans. The list should also include safe and vault combinations, location of keys to all cabinets or desks or containers that house vital records, all services (power, water etc) and where they can be shut off in an emergency, evacuation routes for staff (and for records if necessary), and the location of emergency equipment. The vital recovery procedures should be written in a clear and concise language, easily understandable by non-technical staff. Backup copies of the vital records recovery plan should be stored off-site.

Another way of dealing with vital records would be to clearly mark them with highly visible signage, labels or insignia. There is, however, a risk involved in this, as special marking of records may allow intruders (potential thieves or vandals) the opportunity to identify and take or damage the organisation's most important records. This recommendation is meant in no way to contradict the use of the Blue Shield, the symbol specified in the 1954 Hague

Convention on the Protection of Cultural Property in the Event of Armed Conflict for marking cultural heritage sites, cultural heritage properties, including archives.[14]

The procedures for the removal of vital records in the event of a disaster would include a tracking method, relocation destination, transportation arrangements, conservation vendor's 24-hour contact information, necessary clearances and permits, and internal or external personal assigned to accompany the records. Recommended handling and preservation techniques based on the media involved needs to also be identified. The officer in charge of this operation, and their 24-hour contact, should be detailed as well.

The vital records recovery strategy is founded on a detailed knowledge of the organisation's records holdings including every storage area in use, and of its contents and their nature, the location of vital records, and the level of information contained in finding aids or indexes.

Vital records need to be prioritised for recovery and restoration purposes. Remember, there should be copies of the vital records recovery plan in the organisation's counter disaster plan!

Critical data protection

The recovery of data critical to an organisation's service delivery supports all the other logistics and strategies of the counter disaster plan. If data restoration does not occur then business processes involving electronic recordkeeping, electronic commerce, supply chain management, enterprise resource planning, multimedia products, or telecommunication applications, cannot be recovered.

Planning for critical data recovery 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
* able to be restored within a specific timeframe to an accessible form for processing by systems, networks, and end users,
* those electronic records, that are required for organisational survival, contract commitments, and the conduct of business, are available.

Critical data includes all information files that provide inputs to, and in some cases, outputs from critical business applications identified in the risk analysis. These may include source documents that are coded or otherwise rendered machine-readable by system users. Produced reports and summaries may also be critical if they are auditable documents, or are used in the analysis of business trends, or are used by staff to carry out vital work (such as client account histories and shipping delivery records). Licensed programs and systems software plus their source codes and custom developed applications software, should also be

---

[14] *Emergency Programme for the Protection of Vital Records in the Event of Armed Conflict* – Guidelines developed by the International Council on Archives for UNESCO.

earmarked for off-site storage. Software licenses and registration keys required to make software function and gain vendor support should also be included.

Data recovery planning needs to encompass all the areas where data is stored in the organisation such as the locations and usage characteristics of electronic files stored on PCs, server storage configurations, network storage measures, plus electronic and machine readable data. There may also be critical business information stored on paper, source documents or staff knowledge that make all data usable. This may extend the search of information storage repositories to safes, filing cabinets, microfiche and microfilm storage racks along with desk drawers. If the organisation has adopted electronic document management then these systems can be used to identify key documents for removal to off-site storage.

Developing a policy about data asset identification, classification, and backup requires a coordination of effort between the organisation's designated Disaster Management officer, IT Manager, business units, the Corporate Records Manager, and auditors. The Disaster Management officer may find that these other officers have already initiated data storage measures affording varying levels of records protection. These local strategies will have to be assessed in terms of their formal arrangements and documentation and then integrated into a consolidated off-site storage plan.

Response

This section includes the activities involved in putting the counter disaster plan into action and getting together those resources that can assist agencies to protect or secure their assets from loss. It includes:

- contacting the response and recovery team and relevant authorities
- securing areas
- issuing press releases
- contacting recovery resources.

If it is a significant, or community-wide disaster, then access to records may not be available to start immediate recovery. Staff will need to listen and heed the advice of emergency services personnel and WorkCover representatives. Remember, lives are always more important than records.

Recognising a disaster and contacting the right people

Employees should be trained in how to detect emergencies or disasters and how to respond to alarms. They should be aware of evacuation procedures and disabled egress in case the disaster is likely to affect their safety or the safety of others.

When someone recognises an emergency or disaster, employees should also be able to find response and recovery plans easily and use step-by-step lists and prioritised contact information to contact the Disaster Coordinator or, if they are unavailable, the next authorised disaster recovery team member. Communication should be face to face, by telephone, two-way radio or pager rather than by fax machines, voice mail or e-mail because of the time delay in transmission and retrieval.

The Australian Standard AS 3745-2002**:** *Emergency control organisation and procedures for buildings, structures and workplaces* (see bibliography) outlines procedures for organisations to respond to emergency events until the appropriate emergency services arrive. The standard recommends that organisations establish and implement an emergency plan, allocate responsibilities, conduct training, have evacuation exercises and review these. Such procedures should be developed and tested in association with the counter disaster plan.

In cases of minor damage where personal safety is not threatened, staff should also be confident to take initial action like turning off gas and water, electricity, removing excess water, covering affected shelves with plastic sheeting or raising records that are in danger.

Activating the plan

The coordinator of the response and recovery effort should decide whether it is prudent to notify the fire brigade, police, hazardous material team and others. The coordinator also needs to:

- notify all members of the disaster response team (or delegate this duty to someone reliable)
- brief the response team on the disaster, the response documented in the plan, and additional tasks to be undertaken.

Team members should then notify other personnel and seek expert opinion from conservators. The *Records Management Disaster Planning Toolkit* contains an **Emergency Services list** and the disaster response **telephone tree** that can serve as a starting point for agencies identifying the appropriate people to contact in the event of a disaster.

If required, agencies should set up a central area at the site or an alternate site, to be used by the coordinator and team to make and relay decisions. It may need to include computers and communications equipment, protective clothing, records required to respond to the emergency, backup power supply and fuel and presentation material and equipment[15]

If the disaster is attracting media coverage, the appointed representative may need to organise interviews and updates for the media.

Assessment of damage

The next step in response is to ensure that the site is safe to enter. In cases of minor damage, the disaster coordinator may be able to make this decision. In cases of major damage or instability, where emergency services have been brought in, it will be the decision of emergency services personnel and WorkCover authorities. The *Records Management Disaster Planning Toolkit* contains a **Safety Check Flowchart** that can be referred to and reviewed by agencies to assess the safety of a site before re-entering. If in doubt, wait for emergency services personnel to confirm that the site is safe prior to entering.

Once the site can be entered, the response team needs to carry out a damage assessment. The assessment is to estimate the damage in order to plan the salvage operation and to

---

[15] Jones and Keyes, *op.cit.*, p.64.

prepare a report for the insurance company. Training in how to conduct a thorough damage assessment should be provided as part of response and recovery planning measures. Staff (in association with insurance people) may be able to work from checklists to examine:

- what has caused the damage, for example, electrical fault, vandals etc
- what kind of damage has occurred, for example, structural damage, fire or water damage, sewerage contamination
- present conditions, like the presence of dirt, water, soot, smoke, gas, and whether electricity, water and air conditioning are still available
- what has been damaged, for example property, equipment, shelving, records, vehicles
- how much material or equipment is affected
- whether there are any injuries to people
- whether the agency can still continue to function at the site or needs to find alternative means. [16]

Other issues to consider after assessing the damage are the costs of the materials, supplies and personnel and repairs needed for recovery operations. From the damage assessment, teams can gather whether an alternate site or treatment site is needed and how many staff might be needed for recovery operations.

All information should be compiled into a report for the insurance company and senior management. Photographs of the site should be taken when the damage assessment is conducted to support insurance claims. Remember, recovery expenses such as travel, telephone calls, equipment or facility rentals need to be monitored for the insurance company.

Once security and contingency arrangements have been made (if they are necessary), teams will also need to stabilise the situation and conduct a more in depth assessment looking more closely at the damage that particular records series have sustained. Refer to the Recovery section below for further information.

Security activities

One of the basic rules in disaster recovery is to prevent the organisation suffering further loss wherever possible. One-way loss is commonly sustained after a disaster is to fail to secure the damaged site, leaving it vulnerable to unauthorised access, theft and vandalism and putting staff at risk. Agencies need to ensure that a designated person initiates and monitors security measures. Security measures should be introduced at the damaged site, alterative operating sites and treatment sites. Information security and disaster prevention provisions in the alternate worksite setting are also extremely important considerations in any recovery operation.

Disaster and recovery sites may be secured by methods like:
- creating a list of authorised personnel
- letting all employees know who are authorised leaders and decision makers

---

[16] State Library of NSW, *Counter Disaster Manual*, Sydney, 1992, p.84.

- issuing identification badges to authorised personnel
- locking doors and boarding up windows in unmonitored areas
- installing signs designating restricted areas
- organising a sign in and out sheet (this can record time worked as well)
- securing cash operations
- securing servers
- checking your firewall, virus protection, and intrusive detection systems (if necessary)
- hiring security patrols
- asking for police assistance.[17]

Contingency arrangements

When a disaster strikes, agencies may also need to implement contingency arrangements planned for in the counter disaster plan. For example, if the damage is affecting operations, teams will need to contact vendors under contract to arrange for use of alternative operating sites. Teams may also use the information in the plan's appendices to find office space and equipment for employees performing critical functions, and to obtain copies of vital records. If an alternative site is needed, officers should shutdown and secure the disaster-affected facility. Staff should be already trained in how to shutdown. All major decisions and actions should be documented to provide an audit trail.

Recovery

The final phase of managing a disaster, is recovery. These are the activities associated with restoring resources and operations following a disaster so that normal operations can resume. Response and recovery operations may overlap. For the purposes of this guideline, recovery includes treating damaged records, restoring information on computers, short-term recovery and resumption of critical functions and long-term restoration of secondary systems and processes. Records recovery can be labour intensive and costly.

Stabilising and protecting records

Once the initial response measures are in place, the organisation can work on stabilising the environment to ensure that records do not suffer further damage.

Recovery teams should organise for emergency repairs of structural damage and leaks, and initial clearing of entrances and aisles. The temperature and humidity can be reduced and air circulation increased by opening windows and doors and using fans and air conditioning if there is electricity (if not, portable generators may be required). These actions can help to prevent mould growth (that is likely to begin within 48 hours) and exhaust any soot. Temperature and humidity levels can be monitored by using equipment such as thermo hygrographs and sling psychrometers. Digital data loggers, if available, can be used with these instruments to achieve quick and easy readings.

---

[17] Jones and Keyes, *op.cit.*, p.67.

Treatment areas also need to be established. If the disaster is confined to part of a building, other parts of the same building may be used, providing the temperature and humidity is suitable. If the disaster involves the whole building then damaged material needs to be removed and relocated to another treatment site.

Records assessment

When security and contingency operations have been established and the environment stabilised, the damage that records have sustained can be examined. A **Damaged Records Documentation List** can be located in the *Records Management Disaster Planning Toolkit* as a starting point for agencies in developing their own to suit their situation.

Firstly, teams need to determine whether some records have been completely destroyed or are inaccessible. Then teams need to assess:

- the quantity and nature of damage
- which media has been affected
- if vital records are damaged
- if damage affects records storage containers
- what equipment, specialists and techniques are required.

Take into account those records directly affected (for example, by water or soot) and also those that might be indirectly threatened (for example, by exposure to the elements through structural failure). Teams need to document the assessment by taking photographs or making a videotape or digital recording for insurance and planning purposes.

In some cases it will be difficult to prioritise records for retrieval due to structural damage or other impediments such as mud obscuring box and file labels. If this is the case, records should be moved to another location where they can be cleaned and sorted and priorities established. The priorities for retrieval should be:

- records listed on the vital records schedule
- additional records and information identified on divisional and organisational priority lists
- records that are used to locate records, for example, indexes, classification schemes, accession registers, location registers and inventories
- records with high intrinsic value as originals
- items that have already developed mould.

In addition, particular record types that are more susceptible to damage should be given priority, including:

- items printed on parchment, vellum or coated paper that should be treated within 6 hours
- items with water soluble inks such as maps, drawings and manuscripts
- wet paper, including files, cards maps, plans and volumes that should be dried or frozen within 72 hours
- wet silver halide microfilm that should be immersed in clean water immediately
- wet diazo or vesicular microfilm that should be dried as soon as possible

- colour prints and slides that should be immersed in water and treated professionally to prevent separation of the layers within 48 hours
- black and white films that should be immersed in water immediately
- wet magnetic discs or tapes without backup copies that should be dried within 24 hours
- CD-ROMs and other optical disks.[18]

Commencing salvage operations

The Disaster Response Coordinator has a number of responsibilities in commencing the salvage process:

- to introduce the rest of the disaster recovery team
- to brief all those assisting in the recovery teams.

Discussions should cover: the way the recovery operation is to be organised, how many teams there will be and their responsibilities, the length of shifts, rotations between jobs, communication mechanisms to be used, emergency assembly points and emergency signals. The more mundane aspects also need to be covered: like the location of toilets and refreshment areas and times for breaks.

Workers should then be given operational instructions and taken to their respective areas by recovery team members. Step by step instructions for the different types of media can be copied from the appendices in the counter disaster plan. Teams should also be given basic instructions on safe lifting and handling so that injuries do not arise. Workers should be rotated every half hour to hour, given 10-minute breaks every hour and monitored by team leaders to ensure they are coping adequately with stress and their duties.[19]

The size and scope of the recovery effort will depend on the size and scope of the disaster. Doig (see bibliography) suggests that for small-scale disasters, teams may need to assess the damage, choose a treatment area, prepare the disaster bin and equipment and set up tables for evaluation, interleaving and treatment of particular formats, then retrieve the material and treat it. If the disaster is on a larger scale, Doig recommends that operating teams include:

- salvage team
- evaluation team
- packing team
- air drying team
- other staff.

The salvage team

This team is responsible for removing items from the damage site and taking them to the evaluation site. Remember, however, that records and information contaminated by chemicals or sewerage should not be handled by the untrained. If chemical contamination is

---

[18] National Archives of Australia, *Disaster Preparedness Manual for Commonwealth Government Agencies*, n.d., p.3.

[19] Doig, *op.cit*., p.92.

a possibility, the plan should include information on how to deal with it and experts should be on hand. Contaminated collections must be handled with gloves, protective clothing and masks to avoid health risks. With sewerage contamination, defence personnel and health organisations are a source for information in planning.

Gloves should be worn and material should be handled as little as possible. Generally, as a safety measure, material should be taken from top shelves first. An exception to this rule is if the damage is from fire and the worst charring is noticed on the higher shelves (the least damaged materials from the highest priority areas should be salvaged first).

When moving files, teams should move them as bundles, trying to retain the original order as much as possible. If records are fire affected and brittle, pieces of unprinted newspaper or paper towels can be placed underneath before moving the item to absorb moisture and provide support. Volumes and bundles can be passed by human chain to trolleys and taken to the evaluation team. Temporary conveyor belts may be built down stairways for removing materials if elevators are not operational, or pallets may be lifted out of windows by cranes.

If the evaluation area is close by, the salvaged material can be placed on grids in an evaluation room, and records kept of the location of the grid and item. If this method is followed, batches should never be piled on top of each other. In cases where the evaluation area is off-site, the items need to be packed for transport and accurate records kept. Labels and barcodes may be helpful in tracking the items. Refer to the section on **Packing records in recovery operation** in the *Records Management Disaster Planning Toolkit*.

The evaluation team

The evaluation team members are in charge of inspecting the records, and dividing them into categories for treatment. The evaluation team should document the records and their categories, including all unsalvageable records and information to protect the organisation in future litigation.

The categories should include:
- air drying for damp to wet items and coated papers (the latter must be interleaved)
- freezing for mouldy or priority wet papers
- replacement when copies of the records are readily available elsewhere and have no additional value in their original format
- discard those of no value (such as records authorised for destruction)
- no action.[20]

Information on the treatment of materials can be located in the sections on **Packing records in recovery operation** and **Stabilising and drying methods** in the *Records Management Disaster Planning Toolkit*.

---

[20] *ibid.*, p.83.

Packing team

Packing may occur before or after evaluation as teams may be packing to remove contents from a damaged site or packing on-site for treatment offsite. Refer to the section on **Packing records in recovery operation** in the *Records Management Disaster Planning Toolkit* for further information on how to pack materials.

Air drying team

Air-drying should be conducted in a large, secure area with good circulation, and there should be tables for those assigned to unpack and interleave so workers do not hurt themselves. Large fans, ventilators and dehumidifiers can assist air-drying. If external conditions are dry, windows may be opened.

When the material is received, the air drying team should do quick checks to make sure that it has not deteriorated (for example, mould may have developed). If the condition of some items has changed, they should be taken to the treatment team leader.

Refer to the section on **Stabilising and drying methods** in the *Records Management Disaster Planning Toolkit* for more information on air-drying.

Other staff

Other staff can be used to collect and distribute supplies, drive vehicles, serve refreshments and carry out other 'gopher' functions.

Remember that all teams need regular breaks, refreshments and encouragement.

When materials have been dried, by whatever method, they should be placed in an area away from the collection and separated according to the degree of additional repair or restoration they need. Guidelines for judging physical condition and sorting returned materials should be developed and work areas for sorting allocated. Some documents may be ready to shelve, while others may require cleaning, rebinding or minor repairs. Professional conservation staff should be consulted regarding the treatment of vital records and priority items. Once repaired, teams should monitor records for mould in a rehabilitation area (with temperature and humidity controls) for several weeks and gradually acclimatise them for return to the main records facility. Once returned, the material should be monitored at regular intervals for at least a year.

Restore procedures and resume operations

Dry and treated records need to be returned to clean facilities with appropriate temperature and humidity levels. This may be to an alternative operating site if the building is structurally damaged or destroyed. If the building is undamaged, there may be the need to clean internal areas to remove water, soot or other residues, and restore or replace furniture and furnishings prior to returning records to the original facility. Some disaster recovery vendors can assist in the cleaning of internal areas. In addition, containers and protective encasements like file covers, cartridges and diskettes may need to be replaced or cleaned. Computer equipment will either need to be cleaned or replaced and electronic imaging media may need to be duplicated or reformatted.

Teams also need to:

- restart non essential equipment, processes and systems
- resort, organise and index salvaged records and information before re-shelving and filing
- re-shelve and re-file salvaged records and information
- market the resumption of services.[21]

Evaluate disaster response and recovery activities

Once an agency has recovered from a disaster, teams should conduct a debriefing session with the staff and volunteers involved, to compare the counter disaster plan to what actually happened. This is vital in ensuring that confusing procedures or mistakes are eliminated and that the counter disaster plan will operate better in the future. The discussion results should be documented in a report that is included within the post disaster analysis activities.

Teams also need to conduct some residual tasks. For example, they should:

- inventory response and recovery supplies and replace used supplies
- evaluate performance of suppliers and recovery services and replace vendors that performed poorly
- monitor affected areas and records for signs of continuing problems.

Finally, government agencies should ensure that they reward staff for their efforts in disaster management. In some cases where trauma has been suffered they may require ongoing counselling and support.

Conclusion

It is important to assess the risks of a disaster occurring in your agency. Disasters are a real threat to all government agencies and without proper disaster recovery plans, they can be devastating in both operational and financial terms. Implementing good counter disaster strategies will allow your organisation to meet legal and statutory requirements, and to safeguard valuable records and information resources.

For more information on the development of Records Management Disaster Recovery Plans, please refer to the *Records Management Disaster Recovery Toolkit* and the *Recordkeeping Advice No. 016 on Adequate Records Management in Perspective – Disaster Management* both prepared by State Records of South Australia and consult the bibliography.

Bibliography

This bibliography is divided into:

- sources that cover many aspects of counter disaster management
- sources that relate to specific subjects within counter disaster management.

---

[21] Jones and Keyes, *op.cit.*, p.75.

Sources for counter disaster management

Alire, C. (ed) *Library Disaster Planning and Recovery Handbook,* Neal-Schuman Publishers, Inc., New York, 2000.

Baillie, J., Doig, J., and Jilovsky, C. (eds). *Disasters in Libraries: Prevention and Control.* 2nd ed. Cooperative Action by Victorian Academic Libraries Ltd, Melbourne, 1994.

Bates, R.J. *Disaster Recovery Planning: Networks, Telecommunications and Data Communications*. McGraw Hill, New York, 1992.

Buchanan, S. A. *Disaster Planning, Preparedness, and Recovery for Libraries and Archives: A Ramp Study with Guidelines*. General Information Programme and UNISIST, United Nations Educational, Scientific and Cultural Organisation, Paris, 1988.

Conservation Access, State Library of NSW. *De-dramatising Disasters. A Conservation Access Counter-Disaster Workshop.* The Library, Sydney, 1997.

Doig, J. *Disaster Recovery for Archives, Libraries and Records Management Systems in Australia and New Zealand.* Centre for Information Studies, Charles Sturt University, Wagga Wagga, 1997.

El Mahdy, G. *Disaster Management in Telecommunications, Broadcasting and Computer Systems.* John Wiley & Sons Ltd, Chichester, 2001.

Harvey, R. *Preservation in Australian and New Zealand Libraries: Principles, Strategies and Practices for Librarians.* Topics in Australasian Library and Information Studies. No.3. Centre for Information Studies, Charles Sturt University, Wagga Wagga, 1993.

Howell, A., Mansell, H., and Roubos- Bennett, M. (Comp). *Redefining Disasters: A Decade of Counter Disaster Planning. Proceedings of a Conference held Wednesday 20 - Friday 22 September 1995, State Library of NSW, Sydney, Australia.* State Library of New South Wales, Sydney, 1996.

International Council on Archives, Committee on Disaster Prevention. *Guidelines on Disaster Prevention and Control in Archives.* ICA, Paris, 1997.

Jones, V.A., and Keyes K.E. *Emergency Management for Records and Information Programs.* ARMA International, Kansas, 1997.

Ling, Ted. *Solid, Safe, Secure: Building Archives Repositories in Australia*. National Archives of Australia, Canberra, 1998.

National Library of Canada. *Emergency Planning and Response,* 1996. http://www.nlc-bnc.ca/8/14/r14-209-e.html

Robek, Mary F., Brown, Gerald F., and Maedke, Wilmer O. *Information and Records Management.* 3rd ed. Glencoe Publishing, California, 1987.

Rudich, J. 'Thinking the Unthinkable', *Network.* 1997, 12,7, pp.81-85.

State Records Authority of New South Wales. *Records Management Checklist for Local Government, 1997*. Sydney, 1993.

State Records Authority of New South Wales. *Standard on Physical Storage of State Records.* Sydney, 2000.

State Records Authority of New South Wales. *Standard on Counter Disaster Strategies for Records and Recordkeeping Systems.* Sydney, 2002.

Toigo, J.W. *Disaster Recovery Planning: Strategies for Protecting Critical Information,* Prentice Hall PTR, Upper Saddler River New Jersey, 2nd Edition, 2000

Wold, G. and Shriver, R.F. 'Risk analysis techniques', *Disaster Recovery Journal.* 1997. http://www.drj.com/new2dr/w3_030.htm

Yorke, S. 'Coping with disasters: Strategies for the records manager', *Informaa Quarterly*. May 1997, pp.16-21.

Vital records

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

Parker, Elizabeth. 'Sorry, there wasn't time to switch off the light! Protecting vital records' in *Managing Your Organization's Records,* Library Association Publishing, London, 1999.

Saffady, William. 'Managing vital electronic records' in *Managing Electronic Records*. ARMA International, Kansas, 1992.

Risk management

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

Moore, P. 'Safeguarding your company's records'. *Risk Management.* September 1996, pp.47-50.

NSW Treasury. *Risk Management and Internal Control: A Step by Step Approach to Managing Risk More Effectively*. The Treasury, September 1997.

Office of Information Technology, Information Security Guidelines for New South Wales Government Agencies, Part 1 – Information Security Risk Management, January 2001 http://www.oit.nsw.gov.au/pages/4.3.Guidelines.htm

Office of Information Technology, Information Security Guidelines for New South Wales Government Agencies, Part 2 – Examples of Threats and Vulnerabilities, January 2001 http://www.oit.nsw.gov.au/pages/4.3.Guidelines.htm

Office of Information Technology, Information Security Guidelines for New South Wales Government Agencies, Part 3 – Information Security Baseline Controls, January 2001 http://www.oit.nsw.gov.au/pages/4.3.Guidelines.htm

Pember, M. 'Information disaster planning: An integral component of corporate risk management', *Records Management Quarterly.* April 1996, pp.31-37.

Prince, M. 'Computer exposures can byte the unaware; Organisations often not prepared for threats from inside, outside system', *Business Insurance.* 1997, pp.1-4.
http://rmisweb.com/96birev/computer.htm

Wold, G. and Shriver, R.F. 'Risk analysis techniques', *Disaster Recovery Journal.* 1997.
http://www.drj.com/new2dr/w3_030.htm

Business continuity

Australian National Audit Office Better Practice Guide, *Business Continuity Management – Keeping the wheels in motion,* Australian National Audit Office, Canberra, 2000

Emergency Management Australia. *Non-Stop Service. Continuity Management Guidelines for Public Sector Agencies.* Commonwealth of Australia, Canberra, 1997.

Heath, R. *Crisis Management for Managers and Executives.* Financial Times Pitman Publishing, London, 2000.

Long, M.H. *Business Interruption Risk Assessment: A Multi-Disciplinary Approach*. 1997.
http://www.drj.com/new2dr/w3_029.htm

Security

Australian/New Zealand Standard ISO/IEC 17799:2001, Information technology – Code of Practice for Information Security Management

Davies, J. 'Locks, bolts and bars - real and virtual: Computer security,' Managing Information. 1, 7/8, 1994, pp.28-32.

Office of Information Technology Security of Electronic Information: Planning Guideline. OIT, Sydney, 1997. http://www.oit.nsw.gov.au/guide/electg/electg.asp

Fire and water detection systems and standards

There are a number of sources regarding detection systems listed in the general section above. There are also a whole host of Australian standards related to fire protection, sprinkler systems, automatic fire detection and alarm systems. Refer to the Standards Australia Web site at http://www.standards.com.au/catalogue/script/search.asp for further information.

Planning for staff needs

Baillie, J., Doig, J., and Jilovsky, C. (eds). *Disasters in Libraries: Prevention and Control.* 2nd ed. Cooperative Action by Victorian Academic Libraries Ltd, Melbourne, 1994.

Doig, J. *Disaster Recovery for Archives, Libraries and Records Management Systems in Australia and New Zealand.* Centre for Information Studies, Charles Sturt University, Wagga Wagga, 1997.

Howell, A., Mansell, H., and Roubos- Bennett, M. (Comp). *Redefining Disasters: A Decade of Counter Disaster Planning. Proceedings of a Conference held Wednesday 20 - Friday 22 September 1995, State Library of NSW, Sydney, Australia.* State Library of New South Wales, Sydney, 1996.

Preparedness

Alire, C. (ed) *Library Disaster Planning and Recovery Handbook,* Neal-Schuman Publishers, Inc., New York, 2000.

Australian Archives. *Australian Archives Counter Emergency Manual*, 1994.

Be Prepared: Guidelines for small museums for writing a disaster preparedness plan, a Heritage Collections Council Project, undertaken by Soderlund Consulting Pty Ltd, May 2000

Dorge, V. & Jones S. *Building an Emergency Plan: A Guide for Museums and other Cultural Institutions*. Getty Conservation Institute, Los Angeles, 1999.

National Archives of Australia. *Disaster Preparedness Manual for Commonwealth Government Agencies* (2000)
www.naa.gov.au/recordkeeping/preservation/disaster/intro.html

National Archives and Records Administration. *A Primer on Disaster Preparedness, Management and Response: Paper Based Materials,* October 1993.
www.archives.gov/preservation/primer_disaster_preparedness.html

Office of Secretary of State, Georgia Department of Archives and History. *Disaster Preparedness Planning* www.sos.state.ga.us/archives/ps/disaster.htm

Smithsonian Institution, *et.al. Smithsonian Institution Staff Disaster Preparedness Procedure.* October 1992 revised October 1993.
http://www.nara.gov/arch/techinfo/preserva/primer/eng8.html

State Library of New South Wales. *Counter Disaster Manual*. The Library, Sydney, 1992.

State Library of New South Wales. *Counter Disaster Manual*. The Library, Sydney, 1995.

Toigo, J.W. *Disaster Recovery Planning: Strategies for Protecting Critical Information,* Prentice Hall PTR, Upper Saddler River New Jersey, 2nd Edition, 2000

Reaction and recovery

Hendriks, K.B. and Lesser, B. 'Disaster preparedness and recovery: Photographic materials,' *American Archivist.* 46,1, Winter, 1983, pp.52-68.

Kahn, M.B. *Disaster Response and Prevention for Computers and Data*. MBK Consulting, Columbus, Ohio, 1994.

Library of Congress. *Emergency Drying Procedures for Water Damaged Collections.* 1996.
http://www.lcweb.loc.gov/preserv/emerg/dry.html

National Archives and Records Administration. *A Primer on Disaster Preparedness, Management and Response: Paper Based Materials,* October 1993. http://www.nara.gov/arch/techinfo/preserva/primer/eng1234.html

Northeast Document Conservation Center. *Technical Leaflet: Emergency Salvage of Mouldy Books and Paper.* http://www.nedcc.org/plam3/tleaf39.htm

Northeast Document Conservation Center. *Technical Leaflet: Emergency Salvage of Wet Books and Records.* http://www.nedcc.org/plam3/tleaf37.htm

Syracuse University Library, *Central New York Disaster Recovery Resource Guide*, 1994. http://libwww.syr.edu/information/preservation/resourceguide.htm. This guide is for suppliers in the New York region. However, the description of materials may be useful for Australian agencies assembling supplies.

Syracuse University Library. *Syracuse University Library Disaster Manual.* Revised 8/95 http://libwww.syr.edu/information/preservation/manual.htm