NSW
GOVERNMENT
State Records

Guideline 5

Guidelines on Counter Disaster Strategies for Records and Recordkeeping Systems

June 2002

State Records Authority of New South Wales Sydney, Australia

Guidelines on Counter Disaster Strategies for Records and Recordkeeping Systems, June 2002

ISBN 0-7313-9369-4

Table of Contents

Foreword

The purpose of these guidelines is to assist NSW public offices establish and maintain effective counter disaster strategies for records and recordkeeping systems. The *Standard on Counter Disaster Strategies for Records and Recordkeeping Systems* and supporting guidelines have been produced to assist public offices to better meet their responsibilities under the *State Records Act 1998*.

Under the *State Records Act 1998*, 'each public office must ensure the safe custody and proper preservation of the State records that it has control of' (s. 11(1)). State Records' annual records management surveys have revealed that only a small percentage of public offices have planned for and put into place counter disaster strategies for records. As a result, organisations are placing themselves at great risk through this failure to protect records from disaster. Should records be lost or damaged, public offices may not being able to operate effectively, account for their actions and decisions, or comply with legal requirements. These guidelines aim to specifically support compliance with the *Standard on Counter Disaster Strategies for Records and Recordkeeping Systems*.

1. Introduction

1.1 Background

One of the major threats to the safety and preservation of State records is the risk of disaster. Disasters can at best be an annoying and expensive diversion for a public office. At worst, a disaster may impede the operations of the public office 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 is an area that has come under much scrutiny, owing to disasters in our jurisdiction, interstate and across the world. The *2001 NSW Government Records Management Survey* reveals that few agencies have disaster management plans for paper or electronic records. State Records issued guidelines on *Disaster Management for Records* and *Guidance for Senior Management on Disaster Management for Records* in 1999. This guidance is replaced by the new *Standard on Counter Disaster Strategies for Records and Recordkeeping Systems* and these guidelines.

Counter disaster management strategies yield many benefits for records and recordkeeping systems. Implementing risk management techniques, impact analyses, good recordkeeping practices, vital records programs and prevention and preparedness plans can reduce the likelihood of disaster. Business continuity planning and response and recovery planning will ensure that public offices 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.

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

The *Standard on Counter Disaster Strategies for Records and Recordkeeping Systems* builds on the *Standard on the Physical Storage of State Records* and a legacy of business continuity planning in NSW Government.[2] The *Standard on Counter Disaster Strategies for Records and Recordkeeping Systems* extends the focus to all records and recordkeeping systems for which a public office is responsible. The standard sets three principles and accompanying minimum compliance requirements in relation to counter disaster management for all records and recordkeeping systems, and is intended in part to ensure that records and recordkeeping systems are addressed in business continuity planning.

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

[2] *Ministerial Memorandum* No. 2001-04, issued March 2001 and available at http://www.premiers.nsw.gov.au/pubs_dload_part4/prem_circs_memos/prem_memos/2001/

1.2 Purpose

The purpose of the *Guidelines on Counter Disaster Strategies for Records and Recordkeeping Systems* is to assist public offices to implement the *Standard on Counter Disaster Strategies for Records and Recordkeeping Systems*. The standard, together with these guidelines, will better prepare public offices to prevent or minimise the risk or impact of disasters on records and recordkeeping systems.

1.3 Scope

The *Guidelines on Counter Disaster Strategies for Records and Recordkeeping Systems* are aimed at individuals or project teams who will be implementing the *Standard on Counter Disaster Strategies for Records and Recordkeeping Systems*. The guidelines cover records of all formats, recordkeeping systems, and critical data required to reconstitute electronic records in the face of a disaster. The guidelines focus on disaster prevention (measures to prevent or minimise the risk or impact of a disaster on records and recordkeeping systems) and disaster response and recovery.

The guidelines are meant to give a general overview of the process and refer, where appropriate, to more detailed sources.

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

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

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

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

1.5 Reference to the DIRKS manual

The DIRKS manual was originally published as an exposure draft by State Records NSW and the National Archives of Australia in 2000. Since the release of these guidelines in 2002, State Records and National Archives have now both reviewed the DIRKS exposure draft to meet their specific needs. These versions are known as:

- *Managing Business Information: the DIRKS Manual* by National Archives of Australia, and
- *Strategies for Documenting Government Business: the DIRKS Manual* by State Records NSW.

As a result, these guidelines have been amended to update links to the DIRKS manual. Currently, there are links to both manuals. Specific advice on risk management is contained in the National Archives version at *Appendix 11: Risk analysis in DIRKS*. This consolidated advice on risk management is not included in the State Records manual. State Records is currently reviewing its published advice on risk management for recordkeeping.

2. 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-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 the material on the shelf was uncopied, vital to the production of a product and cannot be salvaged, it is disastrous *for that agency* but perhaps not for the general community.[3]

2.1 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 public office. Disasters affecting records may include:

- natural events 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, riots, terrorism and war, and
- 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.

2.2 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 which have affected records in Local, State and Commonwealth agencies since 1974 include:[4]

1974	***Floods, Brisbane:*** 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. Recovery efforts were headed by staff at the Queensland State Archives.

[3] 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

[4] Ibid., pp. 5-24

1974	***Cyclone Tracy, Darwin:*** In the cyclone many government departments suffered losses. Boxed files and those in filing cabinet 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.
1988	***Floods, Perth**:* 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.
1991	***Fire, Melbourne:*** A fire gutted parts of the St Kilda Town Hall. A commercial company was brought in to remove all computer equipment to their computer cleaning facilities. Work stations were treated on an individual basis.
1994	***Fire, Perth:*** 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.
1994	***Fire, Melbourne:*** 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.
1994	***Fire, Fremantle:*** There was a file following a break-in at the Law Courts. There was no sprinkler system and the majority of paper-based records were destroyed. Paper materials which survived were badly damaged.
1994	***Flooding, Hobart:*** 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.
1994	***Fire, Melbourne:*** There was an explosion in the transformer at an SEC substation, which 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.[5] 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

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

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.

2.3 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 the public office's business continuity plan. Within that framework there are 4 stages:

1. 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
2. planning activities to establish a counter disaster plan to assist the public office to respond to an emergency event
3. the activities to identify and protect vital records of the public office, and
4. 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.

3. Risk assessment

The first principle of the Standard on *Counter Disaster Strategies for Records and Recordkeeping Systems* requires that *risks affecting records and recordkeeping systems should be identified and assessed*. This chapter covers the process of identifying and minimising exposure to certain threats to records and recordkeeping systems, which a public office may experience.

Risk management is recognised as an integral part of good management practice in NSW Government. Risk management process involves:

> *the systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.* [6]

Through the application of risk management methodologies, an organisation can ensure that it does not assume an unacceptable level of risk. Risk management underpins successful counter disaster strategies and other initiatives that the public office may adopt. Risk management strategies enable public offices to assess risks and the extent of planning and treatment methods that are required to mitigate or manage them. Risk analysis may also be used to calculate the cost and feasibility of embarking on counter disaster strategies.

Senior management have the responsibility to ensure that risk identification, analysis and assessment are carried out on a regular basis and that cost effective treatment methods are implemented to safeguard the public office's records and recordkeeping systems. As risk management involves high level planning, a senior officer or officers with the required knowledge should coordinate the program and ensure that it is implemented organisation-wide. These programs should include Nominated Senior Officers and/or Chief Information Officers, who should ensure that risks to the public office's records and recordkeeping systems, especially vital records, are addressed. It should cover records in all formats, including electronic records. Strategies and time frames for changes should be documented in Information Management & Technology security policies and plans, and the public office's counter disaster plan for records.[7]

Public offices also need to manage residual risks by planning for business continuity. Business continuity strategies involve planning to ensure that continued availability of information during a disaster or rapid business resumption after a disaster. Again this is a senior management responsibility and should be undertaken on a broad scale with input from a number of organisational areas.

This chapter of the guidelines is designed to assist records managers to contribute to the public office's broad risk management programs. In addition, the scope of this chapter 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:

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

[7] Office of Information Technology, *Information Security Guidelines for NSW Government Agencies: Part 1 – Information Security Risk Management,* January 2001.

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

3.1 Establish the context

The risk management process needs to occur within the framework of the public office'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.

An ideal starting point for understanding the public office's context is **Step A** of *Strategies for Documenting Government Business: the DIRKS Manual*. Step A of the manual involves identifying and documenting 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.

3.2 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 public office processes
- using established checklists to find inadequacies
- discussing risks with professionals like risk managers, emergency services and auditors
- making judgements based on experience, and
- 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, and
- accidental loss through human error.

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

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, and
- relevant procedures: for example, smoking restrictions, records handling procedures.

Risk audits should be applied to the public office'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. Chapter 5 contains further guidance on identifying and protecting vital records.

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.

Public offices should consult the Office of Information Technology's *Information Security Guidelines for NSW Government Agencies: Part 1 – Information Security Risk Management* for assistance in identifying the most common or generic threats and risks for information and technology installations. The standard AS/NZS ISO/IEC 17799:2001 *Information technology – Code of Practice for Information Security Management* should also be consulted. See the bibliography for these and other useful sources.

There are a number of possible risk management models. For example, NSW Treasury has a comprehensive *Risk Management and Internal Control Kit* containing guidelines, a self-assessment matrix and implementation strategies. The National Archives of Australia's *Managing Business Information: the DIRKS manual* contains *Appendix 11: Risk analysis in DIRKS*. Included in this section are tools that may assist a public office apply the risk management framework and document the process for evidential purposes. They are a Risk Register and Risk Impact Matrix.

3.2.1 Critical needs determination

Public offices may have also determined their critical needs for information (often located in records and recordkeeping systems) and equipment which would be required in order to continue operations should the public office 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.

A 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 Appendix 1.

3.3 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.

	High	**2**	**1**
Probability	**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 public office.[9]

More priorities can be established by using a more detailed matrix. The *Risk Impact Matrix* in the *DIRKS Manual* can be used to analyse the impact of the risks. Entering the likelihood, consequences and level of risk into the *Risk Register* will then enable you to assess relative priorities for treatment.

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

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.

Public offices should also draw on their past work and methodologies used in analysing risks to their records and recordkeeping systems, for example NSW Government agencies may have used particular methodologies as part of their preparation for dealing with Y2K risks. In the *Premier's Department Circular No. 98-09 'the Year 2000 date problem'* the Business Risk Analysis to be undertaken by public offices was expected to yield several new assets including:

- a risk analysis profile for major functions and activities
- a business continuity plan including contingency planning
- a comprehensive critical resource register, and
- a risk based understanding of the business and its operating environment including dependencies on external factors and organisations.

The subsequent *Premier's Department Memorandum 98-14 Phase Two of the Year 2000 Millennium Strategy* required the completion of a Year 2000 risk assessment report, including a rectification plan and high level cost estimates, in accordance with the NSW Government's Business Risk Analysis Methodology or approved methodology. It is appropriate that agencies, State Owned Corporations, and Government Trading Enterprises having made an investment in such methodologies should continue to use them to assist in identifying risks to records and recordkeeping systems.

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 public office. See the bibliography for more information.

3.4 Assess the risks

Risk assessment involves assessing the acceptability of the risk and priorities for treatment. In the diagram in Section 3.3, low probability and low effect risks might be assessed and accepted, monitored and periodically reviewed. Higher risks should be prioritised and treated.

The Risk Register and Risk Impact Matrix in *Appendix 11: Risk analysis in DIRKS* in the DIRKS manual may assist public offices assess risks.

3.5 Treat the risks

Once risks have been assessed to determine which require treatment, the public office 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, and
- implementing the options.

For the major risks identified, public offices 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.

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, and
  - 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, and
- 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* and the Office of Information Technology's (OIT) Office of Information Technology, Information *Security Guidelines for NSW Government Agencies, Part 1 – Information Security Risk Management,* January 2001.

3.6 Monitoring 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]

3.7 Tips for small public offices

This guidance is designed to assist small public offices assess risk and prepare to manage risk. It is aimed at NSW public offices which are considered either 'small' or 'very small'. The following represent some indicators for the sorts of organisations which might fall into these categories:

- 80 staff or less
- budget of $10 million or less
- few or no property holdings
- unlikely to have regional offices, or
- few or no assets other than office equipment and furniture.

The following tips are not exhaustive in scope and must only be regarded as a starting point. Small public offices will need to consider the following points:

- review the history of disasters in the office and local community
- identify all risks to your building, and records and recordkeeping systems
- rate all risks according to probability and impact on your records and recordkeeping systems, and
- assess and treat risks.

At the end of this section is an action list for small public offices.

3.7.1 Review the history of disasters in the office and local community

This step should yield a list of known disasters (large and small) that have occurred in the past, both in the office and the community, with specific regard to their effect on your records and recordkeeping systems. Internal disasters in the building, records storage areas, shopfront areas, and your grounds should also be included. This could involve leaks, fires, thefts, and etc., while community disasters could include bushfires, earthquakes, and floods.

The Insurance Council of Australia may be able to provide some assistance in identifying what risks your region is exposed to, especially natural disasters. They have collated this information and divided Australia into zones depending on the history of events in that region. Also consult with local emergency services regarding their views on the risks to your office.

3.7.2 Identify all risks to your building, and records and recordkeeping systems

TIP: A brainstorming session with all personnel should be followed by a walk through of the office looking at all areas from the perspective of possible causes of disasters. Including local participants such as your builder, plumber, electrician, fire fighters, insurance broker and others may also be useful.

Building considerations should cover:

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

- building age
- floor condition
- wall material
- roof material and pitch
- large unprotected windows
- unlined eaves
- condition of guttering
- number of stories
- emergency exits
- perimeter fencing
- topography
- building work nearby, and
- any other characteristics specific to the building under review.

Risks to records and recordkeeping systems then need to be identified by checking:

- records storage cabinets and shelves (are they solid and made of stable material?)
- the records storage area (is it too cluttered and may cause accidents, or be a fire hazard?)
- power and phone lines (connected, reliable and protected?), and
- computer equipment.

3.7.3 Rate all risks according to probability and impact on your records and recordkeeping systems

TIP: Use a Risk Register to assist you in rating risks. You will also need to use a risk matrix (see above). An example of a Risk Register can be found in *Appendix 11: Risk analysis in DIRKS* in the DIRKS manual.

3.7.4 Assess and treat risks

TIP: Use a Risk Reduction Plan as a way of prioritising, treating and monitoring unacceptable risks.

TIP: Make building upgrades now that would prevent possible future damage or would prevent future risk. Strengthening exterior walls, adding a retaining wall, or shoring up a creek bank are relatively minor projects in comparison to losing the building to flood waters.

TIP: Make it a critical part of your routine to regularly back up files. Keep a backup copy of your computer's basic operating system, boot files, and critical software. Store a copy of all vital information on-site and a second copy in a safe off-site location. Remember that this should also be part of your vital records strategy. See Chapter 5 for further information.

TIP: Surge-protect all computer and phone equipment through power and phonelines. A power surge through a telephone line can destroy an entire computer through a connected modem. Invest in a surge protector that has a battery backup to assure that systems keep working through blackouts.

3.7.5 Action list

1. Prepare list of previous disasters in office or local community. What risks did these pose to records and recordkeeping systems?
2. Identify any potential risk on a Risk Register (see the example in *Appendix 11: Risk analysis in DIRKS* in the DIRKS manual).
3. Using the Risk Register:
   - Determine the probability of each risk happening and the impact on your records and recordkeeping systems.
   - Rate each type of risk as either having a high, medium, or low probability
4. Develop a prioritised action list to enable you to take action to reduce or remove risks.

3.8 Tips for public offices with multiple locations

This section is designed to provide guidance on how risk management and the requirements of the standard can be applied to public office with multiple locations. The concept of multiple locations can include central offices, their regional offices and/or local offices, or establishments within a particular region.

The tips included are not exhaustive in scope and must only be regarded as a starting point. They should not be seen rather as endorsing one approach over another, rather as a means of raising issues for counter disaster planners.

The risks associated with a large public office which also supports multiple locations may seem daunting as each scenario may carry its own unique problems and require ‘tailor made’ plans. The traditional textbook focus for large organisations involves a centralised approach to all potential problems. However, a modular approach where the task of planning is split amongst those organisational entities best able to respond to them should also be considered.

3.8.1 Centralised risk assessment

For many large organisations which have a head office and regional offices, assessing and managing risk centrally makes sense. Centralised risk assessment activities allows for:

- identification and assessment of risks common to all regional/district offices
- treatment of risks on an organisation-wide basis, and
- preparation of common counter disaster plans based upon common or generic risks identified for regional/district offices.

Centralised risk assessment ensures that risk assessment becomes a priority across the organisation.

Whilst risk assessment can be undertaken as a centralised activity, it is important that members of the regional/district offices are involved in providing comment on risk assessments. This local knowledge is invaluable in preparing risk assessments which incorporate risks known to a local community, for example, one regional office may be situated near a flood plain while another could be in an area of bushfire activity.

3.8.2 Modular risk assessment

Modular risk assessment helps relieve the organisation's risk manager in a large organisation of the burden of 'doing it all'. In a modular approach, the risk manager becomes more of a coordinator and guide. The risk manager should:

- identify units within the organisation (at all levels) that have prepared risk assessments for their records and recordkeeping systems, and
- identify those units within the organisation which do not have risk assessments for records and recordkeeping systems.

Once this has been undertaken, the risk manager's job becomes one of co-ordinating risk assessment activities, including:

- educating potential counter disaster planners in assessment and treatment of risks
- distributing templates to be used for assessing risk (eg. a risk register and risk reduction plan), and
- ensuring that all units prepare a risk assessment of their records and recordkeeping systems.

Responsibility for risk assessment and treatment at the local level rests primarily with the local operational units. Each operational unit should bring a knowledge of local risks and the challenges that they present.

The ultimate goal in a modular environment is a well thought out and coordinated risk assessment which allows for all locations of a public office to prepare counter disaster plans for records and recordkeeping systems.

4. Planning

The second principle of the *Standard on Counter Disaster Strategies for Records and Recordkeeping Systems* requires that *an effective counter disaster plan for records and recordkeeping systems should be developed, implemented and maintained*. This chapter covers the process of preparing a counter disaster plan to respond to identified risks to records and recordkeeping systems.

Many public offices 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. Information Management and Technology (IM&T) 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:

1. minimalist planning - so that the plans are easily updateable and less resource intensive, and so that response is facilitated or
2. 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 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, which can be circulated to all staff and kept for reference at strategic points on and off the premises. Kahn's *Disaster Response and Prevention for Computers and Data* (see bibliography) provides examples of how the treatment steps for recovering water damaged media might be illustrated to assist in recovery. An extract is included at Appendix 9.

If public offices 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. The *Counter Disaster Manual* (see bibliography) produced by the State Library of the of New South Wales is a library plan that might be emulated in part. Remember, if generic or other plans are used as a basis **they must be adapted to the specific needs of the public office'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 public office 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.

4.1 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, and
- 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.

4.1.1 Project team responsibilities

The size and responsibilities of the team can vary according to the public office 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 or the identification of vital records.

Project teams should use project management methodologies to manage their projects. Project teams will need to develop work plans and timetables for their projects.

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.

Management should be briefed at all stages of the project so that they can assess progress against work plans and provide input and assistance. Staff should also be briefed about the project. This is a useful step in preparing staff for training activities to be conducted once the counter disaster plan is prepared.

4.2 Content of the plan

The basic components of the plan may vary according to organisational needs, but should include the following as noted in the Australian Standard on records management (AS 4390—1996, Part 6, *Storage*, Appendix B):

a) List of vital records, particularly significant or vulnerable holdings, and location and control documentation.

b) List of equipment and materials available for use in disaster salvage and recovery.

c) The function, composition and chain of command of the salvage and recovery team and their contact information.

d) Procedures for identification and declaration of a disaster situation and initiation of the disaster response chain of command by the normal business operation.

e) Provisions for the training and current awareness of the team.

f) List of sources of back-up resources, including expertise, tradespeople, materials, equipment, vehicles and accommodation.

g) Procedures for updating and testing plan.

h) Simple technical information on the handling of damaged material, directed towards establishing priorities for early action.

The counter disaster plan should be supported by:

- a clear policy statement which 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 and procedures.[11]

A model counter disaster plan is provided at Appendix 2 of these guidelines. Appendix 8 contains a checklist which may be used to check that all aspects of counter disaster management have been covered in 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
- 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, and
- interlink with supporting documentation and inventories.

4.2.1 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

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

internal team can be appointed. If internal staff are allocated the responsibility, members should represent employees from all areas of the organisation. The response and recovery team need to:

a. Determine the preparedness strategy

By employing methods like research, brainstorming and simulations, the team can determine what the public office 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, and
- what to do when a bushfire threatens the premises.

b. 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.

c. 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.

d. 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 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 in *Section 4.2.3*.

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 a public office 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 at Appendix 1 of these guidelines.

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

4.2.2 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:

a. 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 must be approved of and supported by the CEO.

b. 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 public offices 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 must be given the time and authority to be accountable for this plan. Once a manager is given the role of disaster coordinator they must be supported and assisted.

c. 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.

d. 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.

e. 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. See Chapters 6 and 7 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, which covers the major record formats and their treatment requirements, should also be given or provided as appendices to response and recovery information. See Appendix 5 and 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.

f. 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.

4.2.3 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 public office 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 records 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 released
- ‘action sheets’ describing procedures for each recovery team
- other proformas and recording sheets for disaster activities, and
- 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.

4.2.4 Insurance and emergency funding arrangements

Details of insurance arrangements can be included in the plan, attached as 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, and
- 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 public office.

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.

4.2.5 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. See *Appendices 3 and 4* for details of the contents of disaster recovery bins and disaster recovery rooms.

Public offices 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.

4.3 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, and
- 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, public offices 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, and
- regularly practice and test the plan through training exercises.

4.4 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, or
- changes to standards or best practice.

[12] Ibid., pp.35 - 38

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. See Section 4.5 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. Public offices may also consider having their plan externally audited by a disaster management service provider.

4.4.1 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 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.

4.4.2 Plan maintenance responsibilities

Plan maintenance responsibilities should be clearly defined in both the plan and the individual positions 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.

4.4.3 Training and testing

A plan is not a plan until it has been tested. Plans must 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
- practicising debriefing of staff, and
- 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 practise their response or recovery tasks. Training can use a sequence of learning and rehearsal approaches, involving:

- background reading of books, published articles, the Internet

- lectures
- videos
- case studies of past disasters
- computer based exercises
- computer simulations
- tabletop exercises
- field exercises, and
- 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 organisations approach to disaster management to move towards co-ordinated 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:

1. case study or conference room analysis
2. tabletop exercise of the management team, or
3. 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 courses are available through the State Library of New South Wales. Doig (see bibliography) gives practical advice about developing simulations and training sites and evaluating and reviewing participants, of public offices wish to compile and run their own.

A counter disaster plan must 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 organizational records that will affect designated warm or hot site resources and equipment, and
- changes in personnel.

4.5 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. A self-assessment from the actual disaster response team is not desirable nor appropriate.

It must 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, and
- 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.

4.6 Tips for small public offices

This section is designed to provide guidance on how counter disaster planning options and the requirements of the standard can be applied to a small public office. The tips, however, are not exhaustive in scope and must only be regarded as a starting point.

Following the identification, assessment and analysis of risks posed to records and recordkeeping systems (see Chapter 3 for guidance), the small public office must now develop a counter disaster plan to manage those risks and respond to disaster situations. The first step is to establish a small project team to develop the response strategies and prepare the counter disaster plan.

Generic counter disaster planning tools are available (see bibliography) and there is also a model counter disaster plan at Appendix 2 which can be used as a basis. Other similar public offices may have developed a plan which can be used as a starting point. Remember, generic planning tools must be customised so that it is specific to your office and its records and recordkeeping systems. Consultants can be used to customise plans, however ultimately skills and knowledge will need to be developed within your office.

The project team will need to plan for all scenarios identified in the risk assessment. Checklists, steps and illustrations will need to be used to explain what actions should be taken, including the lists of priority records to be recovered in a disaster. Planning must also cover equipment and other resources needed to manage a disaster. The plan should include a policy statement which is endorsed by the Chief Executive Officer.

Depending on the extent of the disaster, the following can be used as an example of the team members required to counter the effects of a disaster:

- an **officer in charge** or coordinator who will manage the situation and liaise with all outside agencies, contractors, and experts. The person must be able to think clearly under pressure, have the ability to prioritise needs and make hard decisions. The officer in charge must also have the necessary authority to do their job.
- an **officer in charge** of communications who has the task of ensuring that the lines of communication are open (land lines, mobile phones, cables)and effective.
- a **volunteer coordinator** to direct any volunteers who come forward to help after a disaster.
- a **recordkeeper** whose job involves documenting the disaster site, areas of damage, and damaged records. This person also manages the register of records moved off site or placed in salvage procedures.
- a **finance officer** to facilitate the recovery process by providing finances. The finance officer will need to keep an account of the monies spent or allocated, and be able to advise on the financial picture.
- an **IT adviser** who can be called for if computers and electronic records are damaged or inaccessible.
- **Response and recovery team** members who will carry out the salvage, evaluation, packing and drying of damaged records and recordkeeping systems.

In the event of a major disaster a **site security officer, general workers,** and an **OH&S monitor** should be included in the team structure. In small organisations, team members may carry out more than one role.

In planning to counter a disaster one officer may be designated as a **supply coordinator** who has an ongoing role to source supplies to be put in the Disaster Bin, and the extra supplies and specialist equipment needed to treat damaged records.

Remember contacts and relationships with specialist companies need to be made before the disaster occurs. The **supply coordinator** should regularly check and maintain the contents of the counter disaster bin.

4.7 Tips for public offices with multiple locations

This section is designed to provide guidance on how counter disaster planning options and the requirements of the standard can be applied to a public office with multiple locations. The concept of multiple locations can include central offices, their regional offices and/or local offices, or establishments within a particular region. The tips, however, are not exhaustive in scope and must only be regarded as a starting point.

For a public office with multiple locations, support networks could be established at a regional level. Contact should be made the other public offices in your region to determine what stage they have reached in their counter disaster planning:

- How does their plan compare to yours?
- Have they found specialist companies and supply sources for expert help and materials?
- Could a joint disaster supply store be established for common use?
- Could you share training workshops to develop your staff skills and reduce costs?

For local councils this process of seeking regional assistance may be facilitated through existing structures such as the Regional Organisations of Councils (ROC groups).

The ultimate aim of any joint activity should be to establish a regional support network where a number of public offices could assist each other when a disaster strikes. However, each office involved must be fully aware of its own capabilities and the level of outside expertise it requires. It must be remembered that the development of protocols and agreements on joint action between public offices may require lengthy timeframes.

Following the identification, assessment and analysis of risks posed to records and recordkeeping systems (see Chapter 3 for guidance), the public office must now develop a counter disaster plan to manage those risks and respond to disaster situations. The first step is to establish a project team to develop the response strategies and prepare the counter disaster plan. For public offices with multiple locations there are two options:

- centralised planning, and
- modular planning.

4.7.1 Centralised planning

Centralised planning allows for:

- preparation of counter disaster plans for risks common to all regional/district offices, and
- common response strategies deployed across the organisation regardless of location.

Centralised planning ensures that counter disaster planning becomes a priority across the organisation.

While planning can be undertaken as a centralised activity, to plan for risks that are less generic requires more de-centralised activity, hence the use of local knowledge and local risk assessments. For example, risks to district offices could be very similar, however, some offices may face a higher risk of flooding than other offices due to location and this must be planned in the counter disaster plan. It is important to gauge the opinion of members of the regional/local offices who will be implementing plans. Additionally, generic plans will need to be modified to suit particular locations, so including members of the regional/local offices in the centralised planning activities will assist in skills transfer.

If public offices undertake a centralised approach to planning, they are also able to undertake a centralised approach to training members of staff in their response roles, particularly when dealing with risks and disasters common to many offices.

4.7.2 Modular planning

Modular planning activities, like modular risk assessments, helps to spread the work amongst a number of staff. Once again, it is important that there is a risk manager or Corporate Records Manager to coordinate and guide the planning process. This manager should:

- identify all the risk assessments that have been undertaken throughout the organisation and all its locations
- assemble a group that is representative of all offices and locations as the key counter disaster planners
- provide a generic plan or template which each location can use with risks identified earlier, and
- ensure that all offices and locations prepare a counter disaster plan.

Using this approach, responsibility for the counter disaster plan and its implementation rests squarely with the unit that has prepared the plan. It is important that these staff receive adequate support and training for preparing their office’s counter disaster plan.

5. Vital records protection

The third principle of the *Standard on Counter Disaster Strategies for Records and Recordkeeping Systems* requires that *vital records should be identified and protected*. This chapter covers this essential component of the counter disaster plan, the identification and protection of vital records.

Vital records are records, in any format, which 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.

The Australian Standard AS 4390-1996, *Records Management* notes that vital records include records that are needed to:

- operate the organisation during a disaster
- re-establish the organisation's functions after a disaster, or
- establish and protect the rights and interests of the organisation and its clients.[13]

Vital records usually constitute a small percentage of records created by an organisation, normally 5%, however the range can vary from 3% to 10%.[14] 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 unaudited accounting and tax records, current personnel and payroll records
- current client files, and
- standard operating procedures.

As noted in the *Standard on Counter Disaster Strategies for Records and Recordkeeping Systems*, vital records in NSW public offices also include:

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

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

A *vital records program* should be established within each public office'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

[13] Australian Standard AS 4390-1996, *Records Management*, Part 6, Storage, Clause 6.1.2.
[14] Parker, Elizabeth *Managing your organization's records*, Library Association Publishing, London 1999, p. 61.

> 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.'[15]

5.1 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 a number of strategies which 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 co-ordinating retention-oriented management actions for records in any format, and
- reviewing organisational documentation.

Step B of *Strategies for Documenting Government Business: the DIRKS manual* provides detailed information on identifying functions.

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

1. vital records: those records which are irreplaceable and mission-critical.
2. important records: those records which are not irreplaceable but could be reproduced only at considerable expense, time and labour
3. useful records: those records which, if lost, will cause some inconvenience but could be readily replaced, and
4. non-essential records: those records which are listed in disposal authorities for routine destruction.[16]

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 public office.

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

[15] National Archives and Records Administration, *Vital Records and Records Disaster Mitigation and Recovery: An Instructional Guide.* An instructional guide. Available at www.nara.gov/records/pubs/vital.html

[16] W. Maedke, M. Robek and G.Brown, *Information and Records Management*, 2nd ed., Glencoe Publishing, California, 1981, p.98.

- functional/organisation charts
- records disposal authorities, and
- current file plans.

Another approach to identifying vital records may be to take 'a layered approach', particularly for larger public offices. 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 which are vital to a particular section of the organisation.

Once identified, vital records must 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, and
- the frequency of update.

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 public office's locations, and
- 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 which allow the protection of the rights of individuals, and
- those which allow the protection of the university's rights, assets, and 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 judgement 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.

5.2 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 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 New South Wales 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, and
- 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, and
- recovery and restoration measures if a disaster does occur.

5.2.1 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 public office. Public offices 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, a public office which has State archives 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.

Specific protection strategies for vital records may include:

1. duplication and dispersal
2. ensuring high levels of fire and security protection in storage containers and spaces, ie on-site and off-site storage
3. establishing procedures for managing critical work in progress which 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 public office 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, public offices may wish to reproduce to a medium, such as microfilm, which 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 public office must 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.

If storing vital records off-site, the facility should be in a safe location at sufficient distance from the main office to be unaffected by the same disasters but close enough for the convenient delivery of records. Records should be housed appropriately, and locatable when required. Storage facilities should meet requirements of the *Standard on Physical Storage of State Records*. The Australian Standard AS 4390*, Records Management,* Part 6, *Storage*, contains guidance on choosing storage options for records and what service contracts with storage service providers should contain. 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, 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.

Although backup schedules are recommended, they are not a comprehensive disaster prevention strategy. See Section 5.2.3.

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.

5.2.2. Recovery and restoration

To facilitate systematic vital records recovery, the vital records recovery plan, ie 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, and 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.[17]

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 must also be identified. The officer in charge of this operation, and their 24-hour contact, must 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 must 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!

5.2.3 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.

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

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, and
- those electronic records, which 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 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 must 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.

A source for this data planning would be the public office's information security policy developed through the Office of Information Technology *Information Security Guidelines for New South Wales Government Agencies.* These guidelines *provide a generic framework to all New South Wales government agency personnel who are responsible for establishing, implementing or maintaining information security in their respective agencies.* These guidelines also require information assets and their values along with any threats and vulnerabilities to be defined.[18]

[18] 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/Guidelines/Security_Part1.pdf

5.3 Tips for small public offices

This section is designed to provide guidance on identifying and protecting vital records and how the requirements of the standard can be applied to a small public office. The tips, however, are not exhaustive in scope and must only be regarded as a starting point.

The small public office should refer to work undertaken in risk assessment, business continuity and resumption planning strategies as this work will have identified records as essential or critical in restoring critical functions of the organisation. Preparation of disposal authorities also allows for the assessment of functions of the organisation and the records which document functions. If a function is identified as significant or critical, then the records pertaining to that function need to be assessed as to whether they are vital. For example if the function of the organisation is to register practitioners within a profession and this function is the most critical and important function of the organisation, then the record or roll of practitioners registered to practice would be a vital record.

It is also possible to refer to organisations similar to yours and compare listings of vital records. Have you identified similar functions as vital or are there differences? How has this other organisation protected its vital records?

For an administrative office if your initial estimate of your vital records is well outside the 3 to 10% range of your holdings, re-evaluate what has been designated vital. However, a counselling, medical, law enforcement or welfare office may have a higher proportion of active case files regarded as vital records.

Remember that vital records may be in any medium or format. They may be active or inactive. They may even be awaiting transfer as State archives.

TIP: If your vital records are in a technology dependent medium, you need to make sure that the technology is preserved as well as the records. If you duplicate your computerised accounts to computer output microfilm, you'll need a microfilm reader to access the records. If you duplicate to CD, you'll need a CD drive.

TIP: Organise procedures to access and retrieve vital records in an emergency. These should be incorporated into your counter disaster plan. Make sure you have lists and indexes that indicate what records there are and exactly where they are. Make sure that the officers designated in the counter disaster plan are

- authorised to retrieve records (including security rated material)
- able to access storage areas (with keys, key cards, entry codes, emergency overrides or knowledge of release switches) and,
- able to use any equipment which is required to retrieve records (computers, microfilm equipment, ladders, trolleys, forklifts).

TIP: Reviews should be scheduled to determine whether vital records are adequately protected, current and accessible to staff who require them. This step is particularly important if functions and activities change significantly or if compliance to the program is wavering. Periodic testing can be part of the process of testing emergency plans. Consult the bibliography for more information regarding vital records programs.

5.4 Tips for public offices with multiple locations

This section is designed to provide guidance on how identifying and protecting vital records and how the requirements of the standard can be applied to public offices with multiple locations. The concept of multiple locations can include central offices, their regional offices and/or local offices, or establishments within a particular region. The tips, however, are not exhaustive in scope and must only be regarded as a starting point.

It is advisable to consider taking a ‘layered approach’ to identifying and protecting vital records in organisations which have multiple locations. Such an approach would identify those records which are vital to the entire organisation and those records which are specific to an individual location.

As vital records occur across the organisation, activities to identify and protect vital records should be coordinated from the central office, however local knowledge and participation should be encouraged. Regional and local offices should be encouraged to identify vital records and suggest appropriate protection measures. Remember large-scale disasters will require a wide reaching and cohesive approach to protect vital records at multiple locations.

While overall coordination is necessary, the idea that the whole effort be completely designed by some central authority may lead to a flawed vital records program. This process would involve a joint effort to

- identify vital records along with the dependencies for critical data
- identify minimum resources and equipment configurations required to access/read vital records in various formats, and
- implement appropriate protection and recovery options.

Remember, work undertaken in risk assessment, business continuity and resumption planning strategies, and the assessment of functions of the organisation for the preparation of disposal authorities will have identified records as essential or critical in restoring critical functions of the organisation.

Once vital records have been identified, special attention must be paid to identifying any current local methods that are being used to safeguard records against loss. The central office may find that the fear of potential loss has motivated ‘owners’ to develop their own strategies for safe storage of vital records. These strategies already afford varying degrees of vital records protection. To facilitate the security and recoverability of vital records, fireproof cabinets may have been purchased, local agreements may have been struck between a records administrator and a vendor who provides microfilming services or off-site storage facilities. Staff may have also come up with ‘home-grown’ strategies to safeguard records.

Discovering the extent of existing local strategies can be a challenging proposition for a head office. When local strategies are discovered, they need to be incorporated into the consolidated vital records program (if appropriate) and the designer of strategies recruited into assisting in identifying vital records or verifying vital records work elsewhere in the public office.

TIP: In transit active case files (regarded as vital records) must also be included in any vital records protection and recovery procedures. An audit of how a public office manages this process should be done to see whether these vital records are being transferred safely in compliance with records storage and handling procedures. Checks should also be made of the public office’s records transfer policy, the documentation it uses for transfers, and its ability to track these records. In transit case files are vulnerable during travel time, at their new location, and on their return journey.

TIP: For an administrative office if your initial estimate of your vital records is well outside the 3 to 10% range of your holdings, re-evaluate this figure. A counselling, medical, law enforcement or welfare office may have a higher proportion of active case files regarded as vital records.

TIP: As your counter disaster strategies will depend on the availability of vital records all off-site storage vendors, alternate storage locations or in-house vaults or backup location used by your public office must be assessed in terms of records storage standards and technical protection criteria. Storing vital records off-site requires more than just a storage warehouse. If an off-site storage vendor experiences a major loss to their facilities and to the vital records stored there this will have a major effect on your public office. It is of the utmost importance to review and understand what protection and response standards your selected vendors or alternate storage locations adhere to.

TIP: Reviews should be scheduled to determine whether the public office's vital records are adequately protected, current and accessible to staff that require them. This step is particularly important if functions and activities change significantly or if compliance to the program is wavering. Periodic testing can be part of the process of testing counter disaster plans. Consult the bibliography for more information regarding vital records programs.

6. Response

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

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

6.1 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 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 organization 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 which are in danger.

6.2 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), and
- 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.

If required, public offices 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.[19]

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

6.3 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.

Once the site can be entered, the response team need to carry out a damage assessment. The assessment is to estimate the damage in order to plan the salvage operation and to 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, and
- 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, and
- whether the agency can still continue to function at the site or needs to find alternative means.[20]

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

[19] Jones and Keyes, op.cit., p.64

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

looking more closely at the damage that particular records series have sustained. See Sections 7.1 and 7.2.

6.4 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. Public offices must 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
- 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, and
- asking for police assistance.[21]

6.5 Contingency arrangements

When a disaster strikes, public offices 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.

[21] Jones and Keyes, op.cit.,p.67

7. Recovery

The final phase of managing a disaster, is recovery. This is 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.

7.1 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 (which is likely to begin within 48 hours) and exhaust any soot. Temperature and humidity levels can be monitored by using equipment such as thermohygrographs and sling psychrometers. Digital data loggers, if available can be used with these instruments to achieve quick and easy readings.

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.

7.2 Records assessment

When security and contingency operations have been established and the environment stabilised, the damage that records have sustained can be examined.

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, and
- 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, and
- items that have already developed mould.

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

- items printed on parchment, vellum or coated paper which 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 which should be dried or frozen within 72 hours
- wet silver halide microfilm which should be immersed in clean water immediately
- wet diazo or vesicular microfilm which should be dried as soon as possible
- colour prints and slides which should be immersed in water and treated professionally to prevent separation of the layers within 48 hours
- black and white films which should be immersed in water immediately
- wet magnetic discs or tapes without backup copies which should be dried within 24 hours, and
- CD-ROMs and other optical disks.[22]

7.3 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, and
- 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.[23]

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

[23] Doig, op.cit., p.92.

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, and
- other staff.

7.3.1 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 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 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 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. See Appendix 5.

7.3.2 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.[24]

Information on the treatment of materials is available in Appendix 6 and Appendix 7.

7.3.3 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. See Appendix 5 for information on how to pack materials.

7.3.4 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.

See Appendix 6 for more information on air-drying.

7.3.5 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.

7.4 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

[24] ibid., p.83.

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 reshelving and filing
- reshelve and refile salvaged records and information, and
- market the resumption of services.[25]

7.5 Evaluate disaster response and recovery activities

Once a public office 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 which is included within the post disaster analysis activities. See Chapter 4.

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, and
- monitor affected areas and records for signs of continuing problems.

Finally, public offices 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.

8. Conclusion

Don’t ever fall into the trap of thinking ‘disasters will not happen to my organisation’. Disasters are a real threat to all public offices and without proper counter disaster strategies, 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.

[25] Jones and Keyes, op.cit., p.75.

Appendix 1 Critical needs questions

- If a disaster occurred, how long could the public office function without the existing equipment and organisation?
- What are the high priority tasks including critical manual functions and processes in the public office? How often are these tasks performed? Daily? Weekly? Monthly?
- What staffing, equipment forms and supplies would be necessary to perform the high priority tasks?
- How would the critical equipment, forms and supplies be replaced in a disaster situation?
- Does any of the above information require long lead times for replacement?
- What reference manuals and operating procedure manuals are used? How would these be replaced in the event of a disaster?
- Should any forms, supplies, equipment, procedure manuals or reference manuals from the public office be stored in an off-site location?
- Identify the storage and security of original documents. How would this information be replaced in the event of disaster? Should this information be in a more protected location?
- What are the current computer backup procedures? Have the backups been restored? Should any critical backups be stored off-site?
- What would the temporary operating procedures be in the event of a disaster?
- How would other public offices be affected by an interruption?
- What effect would a disaster at the main computer server have on the public office?
- What outside service/vendors are relied on for normal operation?
- Would a disaster in the public office jeopardize any legal requirements for reporting?
- Are any of the public office's staff trained in disaster procedures?
- Have personnel been specially trained in debriefing techniques?
- Who would be responsible for maintaining the public office's contingency plan?
- Is the organisation moving to new or updated electronic systems and how would this be affected by a disaster in terms of "in-house" knowledge available?
- How have any current projects to improve the accuracy and completeness organisation's databases been factored in your disaster planning?
- Do you know the development history of your databases; the uses of any locally defined codes, practices and requisite system capabilities?
- How many users of your computer system need access to its applications to continue your business functions at emergency levels? Can this team be mustered in time and have the computer network recovery requirements been defined?
- Do the agreements with external consultants developing or updating systems cover disaster events? Has any form of incident management planning been undertaken?

- Has there been any co-ordination or melding of the teams responsible for facility integrity and information security? Has your organisation moved away from separate plans to protect physical structures and information assets to a plan to protect your ability to operate? Can your organisation's intellectual property, in confidence dealings, trade secrets, or proprietary information be protected during and after a disaster event?
- Are there other concerns related to planning for disaster recovery and have these concerns been addressed?

Appendix 2 Model Counter Disaster Plan

Background Cover page identifying organisation/branch/location

This carries such details such as issue number/date/key telephone alert number.

Authorisation page

This may take the form of a letter from the Chief Executive Officer.

Distribution

The staff required to read the plan (overall) or the people needed to read the plan (strategy) or the specific person or group that uses the plan (action).

Confirmation form

Usually signed by the holder of the plan. Some organisations insist that all who read the plan need to sign and date the form.

Policy section

Contains:

- policy on confidentiality of counter disaster plans and information held by the organisation
- aims and priorities of the organisation in terms or disaster and recovery management
- overall goal of the plan
- authority and responsibility designations
- who changes policies and how policies are changed, and
- conditions for invoking the counter disaster plan.

Plan administration section

Sometimes this section is located at the end of the document. This section includes:

- the plan's designers
- who maintains the plan
- how changes are made to the plans (including time limits for any review or evaluation of incidents
- plan review and audit procedures, and
- exercise and training activities.

Risk assessment section

This section indicates how and when risk assessments are conducted and outlines key or probable risks that may be encountered.

Pre-disaster section

This section deals with the organisational policy on disaster management. It includes:

- responsibilities of the organisation
- individual or group or department responsibilities for health, safety and disaster reduction
- risk reduction control
- management procedures for dealing with non-organisational people on site when a disaster occurs, and
- general instructions on information management.

Communication policy section

This section details organisational policy on information management in more detail. It includes:

- who is informed
- how information will be exchanged
- media briefing instructions
- instructions on dealing with inquiries from outside the organisation
- instructions on dealing with stakeholders (including staff, customers, suppliers, creditors and insurers), and
- ministerial liaison.

Finance, legal and administration

This section outlines how these specialist activities will be conducted within the disaster management response (and recovery management) to monitor and coordinate activities.

Warning and alert section

This section outlines:

- alert and warning systems used in the organisation
- designated officer(s) for alert/warning systems review
- alert/warning systems maintenance
- alert and warning messages (descriptions of sounds, statements or any announcements)
- staff obligations when alerted
- evacuation and security procedures
- safety or evacuation sites, and
- contact telephone, pager, or e-mail addresses and internal information procedures during and after a crisis.

Command and co-ordination section

This section defines:

- lines of command and communication in terms of the disaster structure
- the site and location of the disaster command centre (and alternatives)
- contact list of non-internal emergency service agencies (contacts and authority), and
- disaster manager contact and disaster team contact numbers (and alternatives).

Disaster response section

This is a large and often sub-sectioned set of outlines covering disaster response actions and activities. These include:

- identification and declaration of disaster situation
- procedures for handling elements of the disaster event, and
- procedures for handling elements of disaster impact.

Note: with each indicated group, team, branch or unit in the above procedures, there will be an accompanying team leader and alternative contact list and a list of team member contacts.

Recovery management section

This section includes:

- activating the restoration or continuity plans
- priority recovery of vital records and critical data (includes lists of vital records, location and control documentation)
- procedures and technical information for handling damaged materials
- lists of resources, equipment and services required to deal with disaster situation
- debriefing personnel involved in the disaster
- advice to staff regarding the recovery operation, and
- assistance and counselling information.

Aftermath management section

This section includes:

- Dealing with outside organisations such as insurers, professional disaster response organisations
- review and evaluation of the disaster situation
- procedures for formal closure of a disaster
- disaster response evaluation form for feedback on perceptions of warnings, impacts, management and outcomes of the disaster situation
- procedures for post disaster analysis, review and updating of plan, and
- reporting requirements for disaster (to Board, Committees etc).

Checklists

This section holds checklists for use in preparing for, and conducting disaster management or recovery management activities. Checklist groups should cover:

- preparation (including equipment lists, skill lists, procedural lists)
- action (strategy and unit-action sequential checklists)
- contact (alert or warning contact lists, specialist assistants, teams and leaders), and
- equipment (supply and use during response lists, loss list, logistics and supply lists).

Appendix 3 Contents of a disaster recovery bin or water damage recovery kit

Contained within a distinctively coloured wheelie bin

Plastic aprons	Squeeze Mop
200 sheets of blotting paper	Note pad/folder
2 buckets	Paper towel
200 butchers paper	Plastic cloths pegs
Chux cloths	Pencil
12 cotton gloves	Plastic canister
Disposable camera	Plastic bin liners
Dust coat(s) size 3, 4, 5	Plastic sheeting 2x10m
Dust masks	Post it notes
Extension cord	Power board
Fire blanket	Rubber gloves
Freezer bags	Scissors
Hand towel	Sponge
Utility knife	Tags/ties
Masking tape	Torch and batteries
Heavy duty aprons	Waterproof marking pens
Synthetic chamois	(Optional: first aid kit, clothes line)
100 A4 Manilla folders	

Appendix 4 Suggested contents of a disaster recovery room

Much of the specialised equipment can be hired as the need arises.

extra supplies of disaster bin contents	Plastic milk crates/bread crates
Chairs and trestle work tables	Rubber boots
Chalk	Safety glasses
Dehumidifiers	Environmental monitoring equipment ie Sling hygrometers
Distilled water	Sponges and wiping cloths
Drying space	Spray bottles
Emergency lights	Staplers and non-rust staples
Pedestal fans	Trolleys
Fire extinguishers	Walkie talkies
First aid kit	Wet/dry vacuums
Plastic rubbish bins	Whistles
Hard hats	Broom
Ladders	Clean rags/towels
Masks/respirator	Electrical safety switches
Overalls/disposable overalls	Garden hose on a roll
Plastic gloves	Rope clothes line
Hammer, pliers, saw, screwdriver kit etc	Self adhesive paper labels
Rolls of plastic sheeting	Spun polyester such as Reemay (for carrying fragile items)

Appendix 5 Packing records in a recovery operation

There are two types of packing that may be needed in a recovery operation:

- pre-evaluation packing where records need to be packed and taken to a different treatment site, in other parts of the building or in a different building, and
- post evaluation packing where records are packed for freezing.

Using either method, boxes should not exceed the weight recommended by Occupational Health and Safety officers. All rare, intrinsically valuable and delicate material should be prepared for freezing separately from other materials and in separate categories so they can be located and identified for treatment by a conservator.

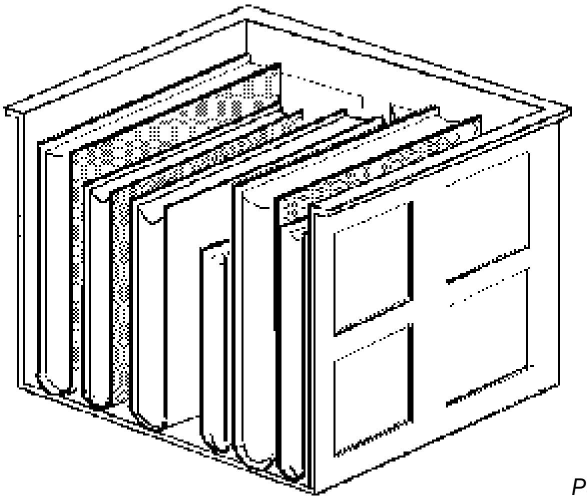
For pre-evaluation packing, paper records can be packed in plastic crates and taken by trolleys to the vehicle. Plastic crates are better for very wet records than cardboard boxes, which can sag and break with moisture and pressure. Volumes should not be flattened, simply packed as they are. They should be taken to the evaluation manager at the treatment site.

For post evaluation packing where there are small amounts of damaged materials, debris can be washed away under cold running water (if clean) by experienced people unless the material is fire damaged or contains soluble inks and dyes. Volumes, books or groups of papers should be held in two hands and dipped into containers of clean water or a hose should be gently applied providing the water is not contaminated. No materials should be scrubbed. In cases where there are vast amounts of material to pack, washing may not be viable.

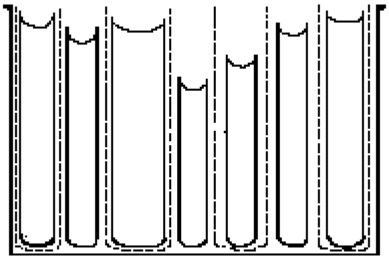
The following packing rules should apply:

Volumes

- Very wet volumes should be packed vertically with their spines down. Volumes of similar size should be packed together in a single layer and supported so that they do not bend. There should be a little space left in plastic crates to allow for their expansion when frozen.
- If it is likely that dyes from the covers of volumes will run, or if time allows, they should be individually wrapped or at least every other wrapped. Use wax or freezer paper, not plastic or plastic coated paper.



Packing wet records in plastic crates reproduced with permission of National Archives of Australia



Preparing wet records for freezing
reproduced with permission of National Archives of Australia

Documents, files and cards

- Wet files should be wrapped in batches that are not more than 10cm deep. Large items should be packed flat on the bottom so that they will not sag. If wet file covers are removed because of damage care should be taken to identify loose documents.
- Soaking wet bundles of wet paper that sustain damage should be packed into large plastic bags or packed on their side in boxes. Do not try and separate them as it is labour intensive.
- Scattered sheets should be placed together in relation to their location and the approximate location noted.
- Files and cards should be left where possible in the original boxes, unless the contents are dry and can be taken out and put in dry boxes without risk of damage.
- Burnt, scorched or dirty records should be supported on single sheets of uncoloured cardboard or heavy paper when transferring to crates.

Microfilm

- Microfilm should be left in storage cartons and secured with rubber bands to retain labels.

Maps and plans

- Large format items such as maps should be interleaved with blotting paper and polythene and placed on flat supports (may be several on each). Do not build up too much weight.

Remember when packing that you need to record information about the item and its location. If records are not in boxes or containers, or if the containers have no identification, label each box or bundle showing the location and identification if possible. Use a soft pencil and paper to write on labels which should be tied onto boxes or bundles. Do not use coloured paper, felt tipped or ballpoint pens or write on the records themselves. Crates should be numbered and the numbers added to documentation, and the removal and destination of boxes should be recorded.

Material should not be piled on top of each other or moved in large batches. It not be left packed for more than a few hours. If the journey to the freezing facility is long, refrigerated vans are desirable.

Appendix 6 Stabilising and drying methods

There are a number of stabilising and drying methods that can be used in the recovery phase of disaster management. It is important to remember that different types of materials need different techniques, and that different types of damage may require different recovery options. Below are general tips on stabilising and drying water damaged paper-based materials. However, advice should be sought from a trained conservator before proceeding. Whichever method is chosen, dried materials should be monitored for potential mould growth.

Freezing

For stabilising and restoring large quantities of records, or records that are already starting to grow mould, freezing is the most effective method. If there are only small quantities of records then other methods, such as airdrying, should be employed.

Freezing is a useful alternative for some records as:

- it stops the growth of mould and mildew (while the object is still frozen)
- it may stop bindings from warping, depending on the method of drying
- it stabilises water soluble materials such as inks and dyes, and
- it gives your organisation time to plan for recovery and restore buildings and equipment ready for the material.

However, conservators ***do not*** advise the freezing of vellum, photographs, glass plate negatives, electronic media such as diskettes, videos, cassettes or vinyl records.

As soon as the record quantities requiring freezing are decided, companies with appropriate freeze facilities (listed in the counter disaster plan) should be contacted and arrangements made for transport. You can:

1. ***Blast freeze*** Commercial blast freezers are ideal as they drop the temperature quickly and have a large capacity.
2. ***Freeze in refrigerated chamber*** This could be slow but there are benefits to reducing temperature even before freezing point is reached.
3. ***Use a home freezer unit to freeze small quantities quickly*** Ensure that it reaches a temperature of –10C and do not open until ready to remove the material (otherwise it will cause a freeze-thaw cycle).

Once the material is frozen and you have the time and resources to defrost and treat it, you need to look at drying options.

Freeze drying

The frozen items are placed in a vacuum chamber, which allows the water to evaporate without melting. This is of a huge advantage for water sensitive inks as it minimises the risk of them running further. Likewise it is also good for glossy papers as it prevents them from sticking together. But if these situations have begun freeze drying will not reverse it.

Vacuum freeze drying is not recommended for photographic materials unless there is no alternative, as their surfaces may be damaged. Leather and vellum may not survive. Volumes that are vacuum freeze dried should be acclimatised for at least one month before opening to avoid cracking the bindings, and monitored for mould.

It is important to have an agreement with a freeze-drying facility before a disaster so that costs, packing requirements and what items are suitable for the procedure are understood.

Dry air purging or dehumidifying

Dry air purging can be used if records are not soaking. A building or site is sealed in plastic sheeting and dry air, at least 26ºC and 15% relative humidity, is pumped in using desiccant or refrigeration equipment. The water vapour is then absorbed in the dry air. This method is rapid and has the advantage of being in situ, but is only useful when the whole site can be sealed off.

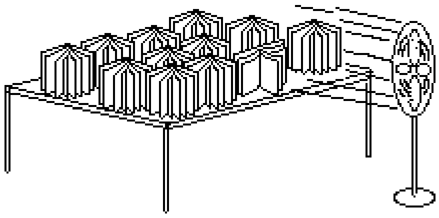
Airdrying

Airdrying can be attempted if it is within two days of the disaster and if material is not soaked. Otherwise, mould will start to grow, and items that are suitable should be frozen. Airdrying may result in some distortion of items and should not be used for items with soluble inks.

Airdrying requires a large space with good air circulation and temperatures below 21ºC. Circulation may be encouraged by positioning fans and opening windows. If available, dehumidifiers can be used in the drying process to reduce relative humidity (ideally to 25-35%). Screening material such as window screens can provide an excellent compact drying surface which allows for air circulation (although metal mesh will rust in contact with moisture).

Volumes

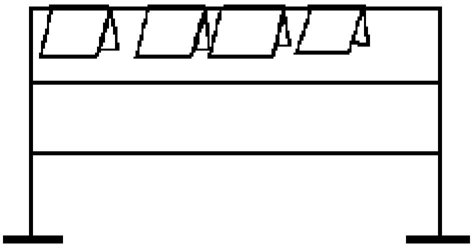
- Closed volumes can be cleaned before drying, by washing off dirt or mud on covers and edges using clean running water and a sponge.
- Books and volumes which can stand upright can be placed on paper towelling with their covers slightly open and their pages lightly fanned. A gentle breeze from a fan can assist the drying process. Do not use heat as it will encourage mould.
- Priority volumes can be dried by placing plastic sheeting on the floor, standing volumes upright with pages fanned (if their spines will support them), and then forming wind tunnels around them from cardboard or plastic sheeting. Cool air from fans can then be directed down the tunnels.
- Interleaving can be used for wet volumes that cannot support their own weight. Loose sheets of paper towel or blotting paper can be placed at 1 centimetre intervals though the volumes. Do not allow interleaving materials to exceed a third of the thickness of the volume or the spine will be damaged (the exception is with coated papers where each page must be interleaved). Replace interleaving materials when wet.
- If adhesives are sticking to the interleaving sheets, a release material such as nylon gauze should be used as a barrier between them.



Drying bound volumes by standing upright
reproduced with permission of National Archives of Australia

Pamphlets

- Pamphlets and loose pages can be hung on lines or improvised drying racks providing you have enough space and assistance.



Hanging small items
reproduced with permission of National Archives of Australia

Files

- Files should be removed from boxes carefully and laid flat. Bundles can be interleaved and pressed under a light weight or pages turned regularly, ensuring that the original order is maintained for each bundle. Cool air can be directed to the pages, but ensure that it is directed upward rather than directly on the pages. Replace the interleaved sheets when they become wet. Glossy papers should be fully separated and interleaved or frozen.
- For saturated files, metal binders should be replaced with plastic tubing or plastic coated wire and pages fanned with some interleaving.

Maps and plans

- Maps and plans can be interleaved with blotting paper stacked up to 10 high and pressed dry under glass, Perspex or thick board and weighted evenly.

Card indexes

- Card indexes should be removed from drawers, stack on sides loosely and supported at each end.

Vellum and parchment

- Vellum and parchment items are very fragile and susceptible to damage when wet. They should be fully supported at all times when being moved. Consult a Conservator before proceeding with any treatments. If nobody can be contacted interleave and freeze.

Photographic prints

If treated rapidly, photographic prints may be air dried. Photographs can be frozen if necessary but do not freeze dry as it may result in disfiguring marks on the surface of the photograph. To air dry:

1. remove photographs from mounts or separate from each other to prevent the emulsion sticking
2. rinse with cool water if necessary. Do not touch or blot surfaces, and
3. place emulsion side up on blotters or lint free cloths or hang by placing clips on non-image areas, ensuring there is no overlap.

If wet, immerse in clean cold water in polyethylene bags. Send to a processing laboratory within 2-3 days for reprocessing and drying (except historic ones).

Photographic negatives

To air dry:

1. remove negatives from envelopes
2. wash in clean running water, and
3. hang to dry or lay flat with emulsion side up.

Eastman colour film should only be handled by a processing lab. If there are large quantities of negatives they should be frozen and air dried.

If wet, negatives should be sealed in polyethylene bags and placed in plastic garbage cans under cold, clean running water while the negatives are still wet. They should be transferred to a laboratory within three days.

Glass plate negatives

Glass plate negatives should **NOT** be immersed in water. They should never be frozen or freeze dried. Air dry them immediately by laying flat onto blotter with the emulsion side up (duller side) or upright in a dish rack.

Fire

While water damaged materials do cause problems, simple techniques such as those described above can be used. The recovery of burnt collections presents additional problems. The effects of fire include heat, soot, burnt edges, melted coverings such as plastics, and possible water damage. The costs of restoration should be weighed against other alternatives. Burnt materials can be frozen, but any restoration other than basic cleaning, rebinding and rehousing should be left to an experienced conservator.

Appendix 7 How to recover records

Records should be recovered in accordance with vital records schedules and priorities set for each functional area. These should be included in the counter disaster plan.

The following instructions are just a guide. For more detailed information on recovery please consult the bibliography. The State Library of NSW, *Counter Disaster Manual* has a comprehensive recovery section detailing treatment for a variety of formats.

Paper-based records

See Section 7.3 for information on how to proceed with the recovery of paper-based records. See Appendix 5 for methods of packing paper-based records for transport or freezing. See Appendix 6 for a description of the best methods of drying paper-based records.

If dealing with non-paper media, teams need to obtain assistance from professionals. Some general principles are explained below.

Magnetic media

If magnetic media (disks, audio, video) is damaged, teams should never try to make copies of it immediately because it might damage the hardware. If exposed to heat, an expert can advise of the chances of preserving the information.

Floppy disks and diskettes

If floppy disks are wet, they should be placed upright in cold distilled water until very is possible. Do not dry or attempt to freeze them. If full backup copies exist, then damaged media can be destroyed and replaced. If they need to be salvaged:

1. Remove from water immediately
2. Remove from jacket
3. Rinse off dirt with clean distilled water. Do not soak.
4. Drip dry vertically in a disk drain or rack.
5. Clean with a soft lintless cloth, move perpendicular to grooves, not in a circular motion. Do not use hairdryers.
6. Place cleaned compact disk in clean jackets.
7. Replace if mould or condensation is present or if there are deep scratches. Check playability and readability.

Magnetic tapes

- **DO NOT** freeze because the moisture in the tapes will cause permanent damage when frozen. Do not use magnetised tools/scissors.
- **DO NOT** use hot or warm air to dry as it will cause the tape to adhere.

Treatment of magnetic tapes will depend on the extent of water penetration. The casing usually keeps tapes clean and dry. If full backup copies exist, then damaged media can be destroyed and replaced.

Wet tape

- Disassemble the case and remove the tape.
- Rinse dirty tapes, still wound on reels in lukewarm water.
- Support vertically on blotting paper to air dry.
- Reassemble and copy.

Optical media

Compact disks

If full backup copies exist, then damaged media can be destroyed and replaced.

1. Remove from water immediately
2. Remove from jacket.
3. Rinse off dirt with clean distilled water. Do not soak.
4. Drip dry vertically in a disk drain or rack.
5. Clean with a soft lintless cloth. move perpendicular to grooves, not in a circular motion. Do not use hairdryers.
6. Place cleaned compact disk in clean jackets.
7. Replace if mould or condensation is present or if there are deep scratches. Check playability and readability.

Microforms

If backup copies exist, damaged media can be destroyed and replaced.

Silver halide microfilm should be kept underwater and not allowed to dry out. It should be sent to a processing laboratory within 72 hours. Vesicular and diazo film should be separated and air dried:

1. Extract water affected records and dry separately.
2. Peg aperture cards up for drying.
3. Unroll microfilms and air dry with the emulsion side up or send to film laboratory.
4. Rewind film and store in dry containers.

If microforms cannot be dried immediately, they should be immersed in clean, cold water for no more than 2 to 3 days and taken to a laboratory. Duplication is recommended where possible.

Appendix 8 Disaster management team checklist

Some of the questions in this checklist are drawn from, or adapted from, State Records' *Records management checklist for local government, 1997*. pp.79-87.

1. Have you been trained before commencing the disaster management project?

   □ Yes □ No

2. Have you developed a project work plan and a strategic plan for the project?

   □ Yes □ No

3. Have you arranged to report regularly to senior management?

   □ Yes □ No

4. Have you informed all staff of the project?

   □ Yes □ No

Prevention

Records management policies

5. Do you have current records inventories which list a record's function, format, location and use, and whether it is vital?

   □ Yes □ No

6. Have you documented classification and retrieval systems so that files can be found easily?

   □ Yes □ No

7. Have you documented retention and disposal schedules?

   □ Yes □ No

8. Have you determined requirements for recordkeeping?

   □ Yes □ No

Vital records programs

9. Have you identified your vital records in all record formats?

   □ Yes □ No

10. Have you addressed actual and potential risks that could adversely affect vital records?

    □ Yes □ No

11. Are vital records copied for backup protection and the copy stored at a different site to the original?

□ Yes □ No

12. Are vital records stored on or offsite in appropriate storage conditions and housings?

□ Yes □ No

13. Are vital records secured from unauthorised access?

□ Yes □ No

14. Do you have a vital records plan?

□ Yes □ No

15. Are there procedures to review and test the vital records program and manage the identification of new vital records based on the risk analysis?

□ Yes □ No

Risk management

16. Have the risks to records been addressed in organisation-wide risk assessments?

□ Yes □ No

17. Have you assessed the risks to records as part of your disaster management project?

□ Yes □ No

18. Have cost effective risk treatment options been implemented?

□ Yes □ No

19. Are risk management strategies for records regularly reviewed to ensure they are effective?

□ Yes □ No

Security

20. Are the records unit work area and all records storage areas secure against unauthorised access?

□ Yes □ No

21. Are there procedures and equipment for securing records not normally held in records storage areas?

□ Yes □ No

22. Do the procedures in Question 21 cover:

a. the issue of records to/from agency staff

□ Yes □ No

b. removal or borrowing records from agency premises

❑ Yes ❑ No

23. Do you have procedures to secure your electronic records from unauthorised access?

❑ Yes ❑ No

24. Have you identified records which require special handling because they may contain confidential or valuable information?

❑ Yes ❑ No

25. Are such records stored securely and flagged to indicate restricted access?

❑ Yes ❑ No

Business continuity / resumption planning

26. Have the critical functions of your agency been identified?

❑ Yes ❑ No

27. Are the records to support these functions managed as part of your vital records program?

❑ Yes ❑ No

28. Has your agency identified and listed other business resources needed to perform critical functions (such as computer equipment)?

❑ Yes ❑ No

29. Has your agency identified alternative sources for these business resources?

❑ Yes ❑ No

Disaster planning, response and recovery

30. Does your agency have a counter disaster plan for agency records based on the risk analysis?

❑ Yes ❑ No

31. Does planning include:

a. preventative measures?

❑ Yes ❑ No

b. preparedness measures?

❑ Yes ❑ No

c. response information?

□ Yes □ No

d. recovery information?

□ Yes □ No

32. Does your plan include lists of contacts of personnel, suppliers and vendors in the local area who can be called on for assistance in a disaster?

□ Yes □ No

33. Has the plan been communicated to all relevant staff?

□ Yes □ No

34. Are staff trained in basic response and recovery procedures?

□ Yes □ No

35. Does your agency have some basic recovery equipment (buckets, paper towels, plastic sheeting) carefully stored in a strategic location?

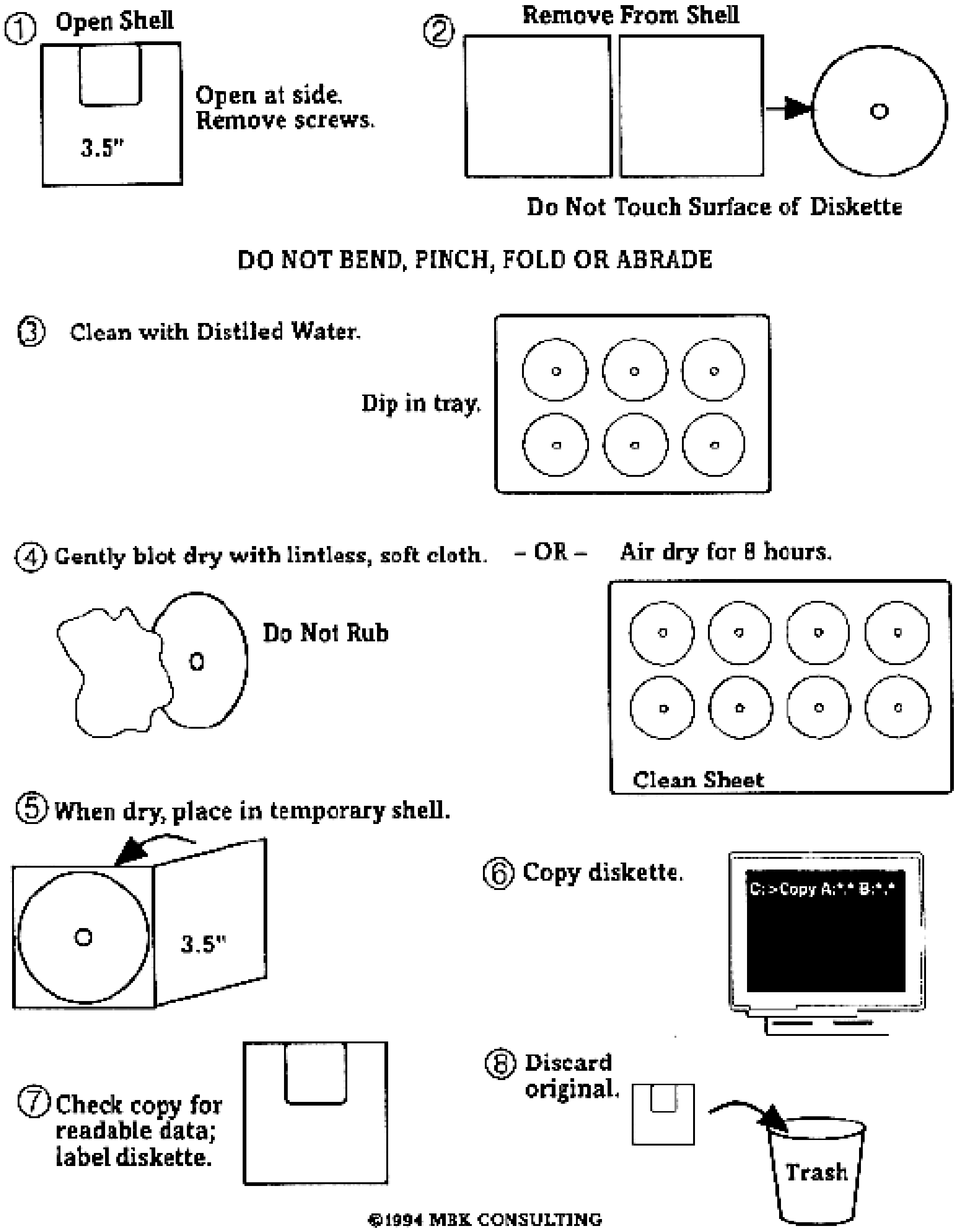
□ Yes □ No

Appendix 9 Recovery of water damaged 3.5” diskettes

This illustration is drawn from Kahn, M.B. *Disaster response and prevention for computers and data*. MBK Consulting, Columbus, Ohio, 1994, p. 19.

Water Damaged 3.5" Diskettes

Stabilize within 48 hours to prevent mold.



① Open Shell

Open at side.
Remove screws.

② Remove From Shell

Do Not Touch Surface of Diskette

DO NOT BEND, PINCH, FOLD OR ABRADE

③ Clean with Distilled Water.

Dip in tray.

④ Gently blot dry with lintless, soft cloth. – OR – Air dry for 8 hours.

Do Not Rub

⑤ When dry, place in temporary shell.

⑥ Copy diskette.

```
C:>Copy A:*.* B:*.*
```

⑦ Check copy for readable data; label diskette.

⑧ Discard original.

©1994 MBK CONSULTING

19

Bibliography

This bibliography is divided into:

- sources which cover many aspects of counter disaster management, and
- sources which relate to specific subjects within counter disaster management.

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 Moldy 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