# Guideline for Records Management

## Number 8 – Business Continuity and Records Management

This Guideline is to be read in conjunction with Territory Records Office *Standard for Records Management No.8 – Business Continuity and Records Management*.

# Contents

# INTRODUCTION

The *Territory Records Act 2002* requires all agencies to have a Records Management Program and to comply with that Program. The Program in turn must comply with Standards and Codes approved by the Director of Territory Records. The Territory Records Office *Standard for Records Management No.8 – Business Continuity and Records Management* is a Standard approved by the Director under the Act.

*Standard for Records Management No.8 – Business Continuity and Records Management* requires an agency to undertake a proper assessment and mitigation of threats to business continuity. While an agency's business continuity planning will be tailored to its own individual needs and circumstances, each agency's business continuity planning for records must comply with the principles set out in the Standard.

# PURPOSE

The purpose of this Guideline is to supplement *Records Management Standard No.8 – Business continuity planning and records management* in a practical way by providing Territory agencies with guidance on how business continuity planning for records might be undertaken.

# BACKGROUND

*Standard for Records Management No.8 – Business Continuity and Records Management* addresses the need for formal and consistent assessment and mitigation of recordkeeping-related threats to business continuity. The assessment and mitigation will be part of an agency's broader business continuity program and will form part of their Records Management Program.

## Business continuity management

Business continuity management helps an agency to prepare for and recover from a disruption to normal business operations. Business continuity planning and disaster recovery are essential elements in risk management and corporate governance.

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

- Understanding the importance of records management (Standards 1 to 7);
- Understanding the overall context within which the agency operates and manages records, including the agency's critical objectives (Principle 1 of Standard No. 7);
- Understanding the risk management and security context within which an agency's records management operates (Principle 1);
- Understanding the criteria or triggers for implementing emergency management, continuity response and recovery procedures in relation to records management (Principle 2 of Standard No. 7);
- Ensuring that all those with delegated or outsourced responsibility for records management play their part in ensuring business continuity (Principle 2); and
- Ensuring all staff understand their roles and responsibilities when a major disruption occurs (Principle 2).

## What is a disaster?

It is critical to plan and protect records and recordkeeping-related business information systems from the risk of disruption arising from a disaster. Standard No.8 uses the term "disaster" to cover a wide range of major and minor disruptions to records, records management and recordkeeping systems. It is used to cover a wide range of major and minor disruptions to records, records management and recordkeeping systems. From a management perspective, a disaster occurs when normal management arrangements cease to function, meaning that control is lost. So disasters are frequently characterised by external agencies taking over management of the event. However, this transfer of control is not an essential feature of a disaster for the purposes of this Guideline. An imminent threat of loss of normal management control is sufficient to classify an event as a disaster for the purposes of this Guideline. With minor disruptions, normal management control may be retained.

## What does business continuity planning for records involve?

Business continuity planning for records includes at least a:

- Business risk impact assessment for records; and a
- Business continuity plan for records.

An agency's business continuity planning for records must adequately address the principles contained in Standard No.8. All records and related systems for which an agency is responsible must be included.

The plan and procedures must detail how an agency will ensure that proper and adequate records of its business activities will be made and kept to ensure that it is able to conduct its business and fulfil its functions effectively and that there is sufficient evidence of the performance of those functions before and after a major or minor disruption.

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

ACT Government agencies use records for communication and conducting day-to-day business, within government and with the public. Poor records and/or document management may contribute to government failures, public embarrassment and litigation. It is critical to plan and protect records and recordkeeping-related business information systems from the risk of disaster to ensure the continuity of business operations in the event of any disruption. The term "disaster" is used here to cover a wide range of major and minor disruptions to records, records management and recordkeeping systems.

By the process of managing records-related disasters, a Records Manager can:

- Mitigate or avoid the effects of a records-related disaster on agency business;
- Identify and protect records vital to agency operation;
- Identify and protect records retained as Territory Archives, records that are required for evidence, subject to disposal freezes, vital or not-replaceable;
- Locate records e.g. on which drive, on which server, in which filing cabinet, which off-site storage facility or whether in use by another member of staff;
- Derive the context of documents retrieved;
- Identify levels of confidentiality and accessibility, and who has authorised access;
- Provide a secure environment for ongoing records and maintenance;
- Encourage the physical safety of people who work with records;
- Provide a framework for responding safely and efficiently to disasters when they occur; and
- Allow normal work to resume as soon as possible after a disaster.

To undertake an agency's business continuity planning, an agency's Records Manager must:

- Identify and describe the agency's broad recordkeeping requirements within the business and regulatory environments in which it operates;
- Identify how the agency will organise and resource its recordkeeping program;
- Specify the nature of the system or systems into which records are to be captured and maintained;
- Detail how records are to be cared for and protected from loss, destruction or tampering;
- Specify disposal arrangements for records; and
- Detail arrangements for access to records.

This information can be used in undertaking a business risk impact assessment for records.

Many agencies will have completed these tasks in complying with Standards for Records Management numbers 1 to 7:

- Standard for Records Management No.1 – Records Management Programs;
- Standard for Records Management No.2 – Appraisal;
- Standard for Records Management No.3 – Records Description and Control;
- Standard for Records Management No.4 – Access;
- Standard for Records Management No.5 – Recordkeeping and Outsourced Government Business;
- Standard for Records Management No.6 – Digital Records; and
- Standard for Records Management No.7 – Physical Storage of Records.

In any case where this has not occurred, these aspects must be included in the agency's business risk impact assessment for records.

The following sections explain the essential steps and issues to consider in undertaking a business risk impact assessment for records.

## Records

### Vital records

Vital records are records, in any format, which contain information essential to the survival or continuity of an organisation. Vital records must be identified in the process of undertaking business continuity planning for records. An agency's Records Management Program should identify, evaluate, protect and allocate responsibilities for vital records.

Vital records are those records that, if destroyed, must be recreated to resume essential business functions. Vital records provide current evidence of an agency's assets, services, transactions and actions. They protect the interests of the agency and people – both staff and customers. If a vital record is lost, damaged, destroyed or otherwise unavailable, the loss *is* a disaster, affecting critical operations. Vital records tend to be active, documenting the status of ongoing, current transactions and relationships. Increasingly, vital records are created and accessed electronically. In some cases, some level of security can be had by retaining the data which formed the basis of the vital record. Without the data, the record cannot be recreated.

Identification of vital records is agency specific. Probable examples of vital records are:

- Rates bills and receipts for the current year;
- Property records including plans;
- Open contracts;
- Active case files;
- Records of unfinished construction projects;
- Payroll records;
- Personnel records;
- Legal documents;
- Computer software and data;
- Accounts payable and receivable for the current year; and
- Indexes and finding tools for records.

To identify vital records, an agency must first determine:

- Critical processes and functions;
- Key internal and external dependencies on which these processes rely; and
- External influences that may impact on critical processes and functions.

Vital records can then be identified either by conducting a comprehensive records inventory or by undertaking a more focused survey where staff members are asked to identify those records they absolutely need to do their job. Those records that are essential to support the critical processes and functions of an agency are vital records. When identified, a list of what are vital records is to be widely distributed in an agency so that many people are aware of which records are included.

There is likely to be a cost associated with protecting vital records. So, it is desirable that only records that really are vital are identified as such. UK National Archives suggests consideration of the following points in determining vital records:

- Whether the process or function can be re-established without the records concerned;

- Senior management view of the importance of the functions to which the records relate; and
- The length of time for which information is required.

An inventory of vital records is to include:
- The Division or Branch responsible for the records series that contains vital records;
- Identification of each recordkeeping system that contains vital records;
- The title of each records series that contains vital records;
- The medium on which the records series are recorded;
- How the vital record is protected (duplicated, dispersed, etc.);
- Whether the record is the original or a copy of a vital record;
- Reference to any disposal schedule(s) that applies to the records series;
- The physical location for offsite storage of copies of the records series or system; and
- Reference to any supporting documents, such as finding tools.

Three options for protecting vital records include:
- Duplication and dispersal;
- Use of secure fireproof, waterproof and vermin-proof storage facilities; and
- Remote storage.

Vital records are to be the main priorities for recovery and salvage efforts when a disaster occurs. In collections, vital records are not necessarily valuable in monetary terms. Records are to be recovered in accordance with vital records schedules and priorities set for each functional area.

### Archival records

Archival records are those records that have been appraised as having long-term, enduring or permanent value.

It has been estimated that archival records may constitute as little as 2% of all records that are created. In the long term, the practice of appraising records as archives at the time of creation of the record is the easiest and most reliable approach for agencies to adopt.

The options for protecting original archival records include the provision of secure fire-proof, water-proof, vermin-proof, temperature and humidity controlled environments. To ensure continued access for current use, the early duplication and dispersal of copies of the original record is desirable. This has the advantage of allowing the original to be placed in secure, off-site storage. See *Standard for Records Management No.7 – Physical Storage of Records*.

For an agency adopting a strategy of early duplication and dispersal of archival records, the costs need not be enormous where identification occurs early (preferably at creation). If an agency has an electronic recordkeeping system costs can be minimised where duplication and dispersal is conducted electronically and automatically.

Where archival records have not been appraised on creation or sentenced against the relevant Records Disposal Schedule, they can be identified by conducting a comprehensive census of existing records that have been put away, or by a focused survey of staff responsible for active records.

## Valuation of records

Valuation of Territory records may be undertaken using one of several approaches:

- Market valuation. This method tends to be associated with determining an amount to be included for financial purposes in an agency's accounts.
- Costing disaster recovery and business continuity.

Where initial valuations are undertaken, agencies may seek to employ a professional valuer.

### *Market valuation*

Valuing for accounting purposes provides an agreed amount, based on assessing the current market value of an asset. This helps in determining the current value of Government assets, which is a necessary part of accrual accounting.

In addition to the cost of creation of the original record, valuers may make estimates based on a number of measures that may indicate the market value of records, such as iconic/unique characteristics, availability of duplicate collections, comparable private records, anything similar available in the market, relationship to other records, nature of the content and the interest in it or use of it.

### *Costing of disaster recovery and business continuity*

Appendix A provides some guidance on assessing the cost of recovering from an identified disaster.

Insurance of a records collection may be based on the replacement of some records or the conservation costs of salvaged records. Detailed guidance on the methodology of obtaining cost estimates is not provided here however the Director of Territory Records has provided a Records Advice on valuing ACT Government collections for insurance purposes.

### *Insurance of records*

The ACT Government manages its insurance exposures and liabilities though a managed insurance fund under the control of the ACT Insurance Authority. All ACT Government agencies contribute premiums to, and are protected by this fund.

The insurance provides protection against the following risks for all insured assets.

- Loss of the collection itself if the collection has been declared to ACT Insurance Authority (ACTIA) at full insurance replacement value.
- Needing to restore records during disaster recovery if costs can be sensibly identified;
- Needing to recreate records during disaster recovery if necessary source data is available and costs can be sensibly identified;
- Being unable to provide a service may be insured if costs can be sensibly identified; and/or
- Having to engage in disaster mitigation or emergency recovery work may be insured if costs can be sensibly identified.

Agencies covered by ACTIA are required to declare the full insurance replacement value of all assets to ACTIA each year. Agencies are not in a position where they can choose whether to insure or not.

The full insurance replacement value of records may be difficult to arrive at and this will be markedly different from values used for accounting purposes which may reflect written down or depreciated values. The full insurance replacement value should reflect the estimated cost to the agency to refurbish or reconstruct the record if it is damaged or destroyed.

The cost of restoration of records or extra costs involved in providing a business service following the loss of records would not be covered unless the records are declared under the physical loss section of the insurance arrangements with ACTIA.

In disaster recovery, a related question concerns the nature of the conservation and restoration to be undertaken. For instance, what conservation measures are to apply to the 500 shelf-kilometres of mainly hand-written records that agencies hold that are not yet copied? These records are unique and the information they contain cannot be reconstituted. Suppose those records were not obliterated by fire but were water damaged. Are agencies to attempt to restore these with a view to retaining them as ongoing archives? Or are agencies to aim to restore them only to the point where they are able to be copied?

Insurance only covers the risk of financial loss following loss or damage to the records. Vital records may require a greater level of physical protection. Records protection is discussed later, but, as indicated earlier, the three basic options are duplication and dispersal, secure fire-proof, water-proof and vermin-proof storage, and remote storage.

In the event of any loss, damage or destruction to collections it is important that the ACTIA be advised as soon as possible so that an Insurance assessor can be appointed to deal with any potential insurance claim for replacement or restoration of records.

## Outsourced government records

The concept of outsourcing involves contracting the delivery of a service to an outside organisation. It does not allow Government to divest itself of its responsibilities. An agency always retains responsibility for providing evidence of Government accountability for that service. Records form a vital part of the evidence of accountability.

The requirements to retain control of records related to an outsourced service must be a part of the outsourcing contract. This is stated in *Standard for Records Management No.5 – Recordkeeping and Outsourced Government Business:*

> Agencies must make full and accurate records of their activities, including those outsourced to external providers. In outsourced arrangements, agencies must be careful to ensure recordkeeping responsibilities are specified in outsourcing contracts… It is very important the ownership of records is made clear in any outsourcing contract (P.2).
>
> When selecting a contractor to provide records management services, agencies must ensure that the contractor is able to meet the standards and codes approved by the Director of Territory Records (P.3).

Accordingly, contractors must comply with *Standard for Records Management No.8 - Business Continuity and Records Management* to which this Guideline relates. This means that appropriate disaster management arrangements must be made by a contractor for records held, and recordkeeping systems used, by outsourced providers.

It also means that an agency must consider the full range of business continuity risks arising from the operation of an outsourced service. The safest means of achieving this is to use, as a starting point, the risks faced by an agency itself, and then add to those risks any additional risks that may be specific to an outsourced provider. The simplest and most effective approach is to require a contractor to undertake business continuity planning for the records for which it is responsible.

## Records-related risks

Records-related risks must first be identified and then evaluated.

### Identification of records related risks

Records-related risks can be any of five types:

- Water damage;
- Fire damage;
- Environmental damage, including infestation, environmental pollution and geographic and climatic hazards;
- Security, including access security, building security and storage security; and
- Records management, including recordkeeping systems, IT failure, human error and conservation and preservation.

A starter checklist of risks in each of these categories is provided in Appendix B, which agency records managers and risk managers can use. It should be added to and amended to accommodate agency-specific risks. In many cases, expert advice will be needed to identify all the risks that apply. Detail will need to be provided and this may also require expert advice. Conversely, some risks may not apply. The final three columns suggested in the checklist (ie "Impact", "Likelihood", and "Recovery and continuity costs") relate to the next section: "Evaluation of identified risks".

#### *Water damage*

Water damage falls within the category of environmental risks. It is treated separately here because flooding is the most common form of environmental disaster to affect records. Also, like fire, a lot of records can be adversely affected very quickly.

Location and design of buildings used for records storage can mitigate this risk considerably, but there is also a lot that records managers can do. For example: select storage areas with adequate drainage ensuring records are shelved at least five centimetres above floor level.

#### *Fire damage*

Fire damage also falls within the category of environmental damage. It is also treated separately because of the devastating effect on records that a fire can have.

Compliance with fire regulations is axiomatic. However a realistic assessment of the likelihood of a fire may lead to additional protection measures, such as storage location and duplication of vital records and archival records.

#### *Environmental damage*

The potential of a wide range of threats to records from risks in the local environment is to be assessed. Although the likelihood may be low, the impact could be considerable if the hazard ever materialised.

In practice, the most frequent hazard is likely to arise from vermin infestation.

### *Security*

Damage from failed security arrangements covers a wide range of risks. Three categories are: access security, building security and storage security. These categories are to be interpreted broadly so that no risk facing an agency's records or recordkeeping systems fails to be identified.

### *Records management*

Like "security", damage arising from poor records management covers a wide range of risks, which are to be interpreted broadly to ensure that all records-related risks are identified.

Recordkeeping systems are often agency specific, so the risks that are identified are to reflect the real risk situation that is faced by an agency. Risks will frequently arise because of the details of a particular recordkeeping system, and no attempt has been made to spell out all such risks in Appendix B.

Risks to IT systems and risks associated with failure of IT equipment may have been dealt with by an agency in meeting *Standard for Records Management Number 6 – Digital Records*. However, care must be taken to ensure that the risk identification and analysis has been thorough and comprehensive.

Human error covers a wide range of risks that may be difficult to foresee and may be even more difficult to mitigate because of the one-off nature of these events. At the same time, where events occur repeatedly, such as putting away records and files, frequency rates of one-off errors can be determined. Human error includes breakdowns in accountability, inappropriate disposal of records, alteration of records, release of records younger than 20 years old other than through FOI, and operational and organisational failures. Failures that arise partly because of the way in which the recordkeeping system itself is working are to be identified as risks associated with the recordkeeping system, and are to not simply be attributed to human error.

Criminal behaviour includes such acts as theft, arson, malicious computer hacking, vandalism, deliberate alteration of records, deliberate release of records that are not to have been released, deliberate illegal destruction of records, and so on.

## Evaluation of identified risks

An agency must evaluate the risks that have been identified. The evaluation is to be rigorous and include an assessment of the likelihood and consequence of each risk. The third and fourth columns of Appendix B allow for such an assessment in summary terms.

UK National Archives suggests the following indicator system which is recommended here (*Records Management Standards Business Recovery Plans*, P.4).

| **Impact/consequence** | **Likelihood** |
|---|---|
| 1. Major problem | a. High – likely to happen |
| 2. Could cause problems | b. Medium to high – could happen |
| 3. Unlikely to cause real problems | c. Medium – could happen in right conditions |
| | d. Low to medium – probably will not happen |
| | e. Low – very unlikely |

The evaluation of each risk is also to include estimates of the costs of recovery processes and business continuity that would result should the identified hazard occur. This is the subject of the final column in Appendix B "Disaster & continuity costs". These costs reflect the impact

of the disaster on ensuring business continuity and maintenance of an agency's archival legacy. These estimates allow an agency to be aware of the magnitude of the financial task it may face in the event of any disaster.

The estimates also provide a marker against which the costs of disaster mitigation may be assessed. In other words, it allows the costs of mitigation to be set against the costs an agency would face if the disaster should occur. These cost estimates place senior management in an informed position to make informed decisions about which mitigation measures to undertake.

These estimates are to be as solid as possible. For example, estimate the potential costs of having insufficient evidence to defend a legal action, or the costs of having to find records to place before an Inquiry, or the costs of freeze-drying and fumigating damaged records, and the potential for loss of human life. Appendix A provides some initial guidance on starting cost estimates.

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

## Requirements for business continuity planning for records

To manage records disasters, an agency must address those events that could potentially damage or destroy its records.

*1.* *Business continuity planning for records encompasses four related activities.* These four activities may be characterised temporally as occurring before, during, after and looking back on a disaster:

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

*2.* *Business continuity planning for records includes procedures.* Procedures specify how the planning will be implemented. They detail the practical requirements for each agency of the four activities above and identify responsibility for each of the tasks in the process.

*3.* *Business continuity planning for records is explicit.* The documents that comprise the business continuity planning for records must be able to be easily and clearly identified. Many agency Records Managers will find it useful to pull all the parts of a business continuity plan into a single document for ease of reference.

*4.* *The planning must be adequately rehearsed.* Acceptable documentation alone is not sufficient to meet the requirements of the Act. A part of the implementation is rehearsing necessary actions as far as possible. The records equivalent of fire alarm drills are required.

With the wide variety of risks and impacts that are possible, a single rehearsal will be insufficient to ensure that all players practice exercising their roles and responsibilities in all disaster scenarios. A variety of drills means that participants will have had some practice in a drill that simulates the roles and responsibilities required in the event of a disaster. Unlike a fire alarm drill, it will generally not be the case that all members of an agency need be involved in rehearsals. All those with specified roles and responsibilities will be involved.

## Business continuity planning for an outsourced provider

An agency must consider the records-related business continuity risks that face an outsourced provider. Specific disaster mitigation, disaster response and business continuity measures are to be included in each outsourcing contract as required. The simplest and most comprehensive approach is for each contractor to develop their own plan. This is consistent with the requirement of *Records Management Standard No.5 – Recordkeeping and Outsourced Government Business* that "the contractor is able to meet the standards and codes approved by the Director of Territory Records" (P.3).

Failure to include such measures in a contract does not remove responsibility and accountability from an agency. It means that an agency would be unable to include the contractor as being partially responsible, because the contractor would not have been required to comply. As a result, the full weight of responsibility and accountability would reside with the agency.

## Disaster mitigation

Disaster mitigation is the process of anticipating potential disasters. Anticipation allows an agency to have measures in place that reduce the likelihood of the occurrence of a disaster or will reduce the impact of any disaster that does occur.

There is a distinction between actions that lessen the likelihood or severity of a disaster that will affect an agency's records, and actions that protect the records themselves in the event of a disaster occurring. The two may overlap.

### Reducing the likelihood of a disaster

Records Managers can take action to minimise the risk of a disaster occurring. In most cases, the actions need to be taken on a regular basis. The trigger for the action will vary. For instance, pipe inspections may occur at regular time-based intervals, whereas storm protection may occur after a storm warning has been issued (See National Archives of UK, Business Recovery Standard Plans, p.4 ff).

Examples of simple and effective measures include talking to local emergency services personnel, identifying and contacting other agencies who may be able to assist in the event of an emergency (such as by lending fans for drying following an immersion disaster), and having simple equipment on hand to deal with minor disasters (such as an "emergency trolley").

Ultimately, mitigation becomes a compromise between the costs and benefits of prevention, and these decisions will be made at senior levels. An agency's business risk impact assessment for records will assist senior managers in this decision-making which will be part of the agency's business continuity planning for records.

The following actions are suggestions for the sorts of actions that records managers can consider. The list for each agency will be specific to that agency, although discussion with other agencies may assist. An agency's list of actions will grow from the list of risks identified in their risk assessment undertaken as part of Principle 1 above.

#### *Water damage*

. The following are some examples of actions that can be taken to minimise the risk of a disaster or its severity caused by water damage:

- Identify and check regularly potential internal and external hazards (for example, heating systems, water tanks, water pipes and sewerage pipes);
- Ensure that heating and air-conditioning systems are regularly checked and serviced;
- Identify and check regularly potential penetration hazards (for example, windows, gutters, skylights and drains);
- Consider the possibility of installing flood alarm systems (for example, sensors on water tanks);
- Raise bottom storage shelves five centimetres above floor level;

- Fit top storage shelves with metal covers;
- Consider boxing important series of records;
- Obtain information on local flood danger periods; and
- Never put records on the floor;
- Identify freeze drying facilities that would be available in your area; and
- Identify conservation laboratories in your area.

### *Fire damage*

Health and safety regulations regarding precautions against fires must be observed at all times. In addition, actions that records managers may take on a regular basis include:

- Ensure that fire prevention officers are aware of important collections of records and information, including catalogues and metadata;
- Ensure that all existing fire regulations in respect of doors, extinguishers and alarm systems are enforced;
- Maintain a list of flammable substances and isolate them from the building;
- Keep storage areas clean and tidy;
- Check electrical wiring regularly;
- Adhere to ACT Government no smoking policies; and
- Maintain liaison with local fire prevention officers.

### *Environmental damage*

Actions that records managers may take to avoid environmental damage include:

- Monitor Bureau of Meteorology storm warnings;
- Monitor environmental conditions surrounding records storage sites (for example, does long grass need mowing? Is an adjacent construction site causing concern?);
- Regularly fumigate records storage areas;
- Consider vermin traps and poisons as appropriate;
- Liaise with tenants located adjacent and nearby about any vermin problems they experience and strategies they adopt; and
- Maintain liaison with local emergency services staff.

### *Security*

Each building and each collection poses its own security problems. Actions that records managers may take include:

- Liaise with agency security officers to minimize risks from theft or loss;
- Ensure caretakers/security guards check all entrances to buildings, including ground floor windows and basements, after closing time each day and at least once every twenty-four hours during weekends and holidays;
- For buildings with no caretaker or security cover, fit them with an automatic intruder alarm system; and
- Make all staff members aware of the need for good security (for example, good key control; checks on criminal records; and identification procedures).

### *Records management*

Actions that records managers may take include:

- Ensure adequate staff training in relation to recordkeeping systems;
- Ensure adequate staff training regarding fraud, theft and recordkeeping processes; and
- Consider succession planning for key staff positions, and a “buddy” system on key projects so that more than one person is up to date.

### Protecting records

Three options for protecting records are duplication and dispersal (the duplicate may be in paper or alternative format, such as microfiche or DVD), secure fire-proof, water-proof and vermin-proof storage, and remote storage. These options may be used in combination.

Instituting any of these options involves a cost, at least initially and often on an ongoing basis. Senior management approval may be required, together with a business case.

A business case will require costings of the proposed initiative set against the costs of continuing with present practices – that is, the "do nothing" case. Fortunately, the base-case costs, or the costs of doing nothing are to appear in the final column of the risk identification checklist in Appendix B. These are to contain the so-called "do nothing" costs of disaster mitigation and disaster recovery for the present level of records protection.

It is of course necessary to cost the proposal. If the proposal is for a new building, quantity surveyors will apply standard costing procedures, and ongoing costs can be estimated on the basis of scaling existing expenditures. In other cases, costings will be derived from a detailed understanding of the processes involved and the way in which the proposed initiative will alter those processes.

For instance, where digital records are identified on creation as vital records or archival records and are sentenced at the time they are created, the cost of electronic duplication and dispersal are to be small relative to the cost of disaster recovery and business continuity.

The comparison of the estimated costs of the proposed initiative set against the costs of doing nothing places management and Government in an informed position to make decisions about the benefits and detriments resulting from different possible expenditures.

## Disaster response

Disaster response is work undertaken to lessen the impact of a disaster after it has occurred. While the starting point for disaster response is generally clear (that is, the discovery of a disaster), the end point may be less clear as the response work grades into business continuity.

The steps required for an effective response to a disaster can be codified, and one such set of steps is described in this section. The extent to which each step applies will vary with the size of the disaster. Numerically, most "disasters" (in the wide-ranging meaning of the term as used in this Standard and Guideline) will be simple service disruptions that can be ameliorated quickly using common sense. However, it is sensible for agencies to get into the habit of using procedures that are scalable to major disasters, so that staff members become familiar with them. Appendix C contains several checklists that agencies may wish to use as a basis for their own disaster mitigation planning.

Two tasks must be completed before a disaster occurs. The results must be distributed to those who may require them before a disaster occurs. The results are specific to each agency.

First, a list of people who are to be contacted in the event of a disaster and their contact details must be widely distributed. Procedures must nominate which people are, in turn, to be contacted by the Records Manager or delegate, and the records security officer or delegate, and the business unit manager or delegate, before these people go to the disaster site. At the

very least this will put these people on alert that their services may be required. Appendix C contains a contact list in case of disaster, which agencies may wish to use as a starting point.

Secondly, Appendix D contains a list of responsibilities which need to be allocated to people before a records related disaster occurs. The list identifies a decision maker for each responsibility, and a delegate for each decision maker. The aim is to leave no one in doubt in a time of crisis about who has the responsibility to decide something, and how to get in touch with them or their delegate. Ultimately the agency Records Manager is responsible; however, it is not possible to rely on one person or their delegate in a crisis, when decisions may be needed quickly at the site.

The list needs to encompass aspects where the need for decisions can be foreseen, from the point of discovery of a disaster until the point where full business operations resume.

In addition to Appendix D (ie not replacing it), agencies could also turn the list around and, for each decision maker, list the areas of decision making for which they have responsibility. This simply ensures that each person is clear about their area of jurisdiction.

## Steps in effective disaster response

The following steps should be included in every disaster response plan, beginning with the initial discovery that something is wrong.

Planning documents must show who in the agency has responsibility for each step. This is to provide an orderly frame of reference in a chaotic situation. Human safety is the primary objective during any disaster response. Dedicated employees may feel obligated to take unnecessary risks to rescue records and other property, but they must understand that nothing is worth injury or loss of life. The goal is to prevent complete chaos, which could lead to secondary disasters, personal injury, and a greater impact of the initial disaster.

### *1. Identify an emergency and raise the alarm*

A record-related disaster can happen at any time and be discovered by anyone. Safety is the primary consideration.

If a disaster occurs during working hours, it is essential that at least every member of staff associated with records be acquainted with procedures to raise the alarm. Other staff members may also need to be acquainted with these procedures. Even if the situation can be contained, the person responsible for the security of records or their delegate must be contacted. Raising the alarm involves at least:

- Where the situation clearly warrants it, contacting police and emergency services;
- Contacting a person responsible for the security of the infrastructure affected. This may be the agency's buildings officer, or, if IT infrastructure is involved, it may be the IT security officer. The officer or a delegate must be able to be contacted at all times;
- Contacting a person responsible for the security of records. In many agencies this will be the agency Records Manager. A delegate must be provided in case the Records Manager is not available. The Records Manager or a delegate must be able to be contacted at all times;
- Taking any action that will reduce or limit the potential damage, if it is safe to do so. This might include:
  - turning off stopcocks, especially gas and water;
  - switching off electricity, electric lights, etc;
  - unplugging electrical appliances;

- closing doors and windows; and
- using hand-held fire extinguishers; and

- Contacting the records-related team leader or business unit manager or their delegate, if this person is different from the person responsible for the security of records. These people must be able to be contacted at all times.

Out of working hours, the first four actions involved in raising the alarm, listed above, are to be undertaken. Out of working hours, the people involved may be night security guards. If the function of out-of-hours security has been outsourced, close liaison may be required with the security company on an ongoing basis to ensure continual readiness.

### *2. Assess the overall situation*

Procedures must provide guidance as to the appropriate person or persons to assess the overall situation. Often, assessing the overall situation will not primarily be a records-related function. The appropriate assessors are likely to vary with the scale of the disaster. For larger disasters, emergency procedures not directly concerned with the management of records will be instituted by police or emergency services officers. Safety is, as always, the primary consideration.

The necessary tasks are to estimate the amount of time that has elapsed since the disaster occurred, assess the level of impact during that time, and attempt to project how quickly the situation will deteriorate. Perhaps check the current temperature, humidity, and air circulation. Look for damaged pipes of any kind and standing water or other fluids. Also check for downed branches and power lines or submerged electrical wires. Make sure that the levels of particulate matter in the air from burnt building materials or chemicals do not pose a threat to the response team.

Where it is a larger disaster, it may be necessary to stabilise the environment. Personnel may not enter a facility or affected area until it is safe to do so. In many cases, other authorities will stabilize the situation first, especially in cases of fire, severe floods, downed trees or power lines, or damaged roofs or exterior walls. Others will check for secondary threats, such as leaks caused by the primary disaster, structural instability, and so on.

### *3. Identify an appropriate initial records response*

The records disaster response team is likely to be led by the records team leader or business unit manager or delegate. The team is to identify an appropriate initial response. Procedures provide guidance about appropriate responses for different levels of disaster, recognising that every disaster is different.

For example, procedures may suggest that, once it is safe for records staff to enter, they are to try to remove standing water as soon as possible. It may suggest that they try to stabilize the temperature and humidity. Or it may suggest procedures where only digital or only paper records are affected. Or it may suggest calling in additional external assistance in specified situations.

While the advice will be agency-specific, it is very possible that a similar approach will be useful for a number of agencies, with only minor variations required to accommodate agency variations. This is likely to lessen the workload and assist staff moving between agencies as they will already know the basic disaster response.

Photographs are useful for measuring damage and formulating methods of response and recovery. They may also be necessary to satisfy insurance requirements.

Appendix E is a sample Disaster Equipment List and a sample List of External Equipment Sources. Agencies may choose to use these lists as a starting point in developing their own. Supplies of essential equipment are to be kept in different strategic areas of the repository in storerooms or cupboards that are clearly marked. Small items for use in an emergency are to be kept on trolleys or in bins for easy transportation. Larger items might be stored centrally or available for loan or hire at the time of the emergency. It is unlikely that equipment and materials to cover every emergency can be stored. However, essential equipment would be expected to include:

- Mops;
- Rubber gloves;
- Floor cloths;
- Hazard tape;
- Torches;
- Protective clothing;
- Plastic sheeting;
- Blotting paper;
- One container of useful items such as identification forms, large polythene bags, name tags and string, pencils and pencil sharpeners, scissors, cotton tape; and
- Plan of the building showing: electricity cut-off, water shut-off valve, gas shut-off, sprinkler system/CO2 system, fire extinguishers, stored chemicals, and emergency equipment. This may already exist as part of an agency's broader disaster preparedness.

It is important that cupboards or doors leading to the bins containing these materials not be locked. The locations of these bins must be clearly identified.

### *4. Assess records damage*

In order to develop a coherent salvage strategy, it is necessary to make some form of reasonably consistent and comprehensive assessment of the damage that the disaster has caused to records. Appendix F contains an "Initial Damage Assessment Form" that agencies can use to gather preliminary data about the disaster's impact on its records. Assessment will be required of:

- The severity of damage, from minor impact to total destruction;
- The total quantity of records affected; and
- The name, quantity, format and severity of damage of each records series involved.

### *5. Develop a records salvage strategy*

Salvage is essentially a process of triage of records that have been damaged. The development of a records salvage strategy is likely to be led by the business unit manager or delegate.

Vital records and archival records (from the records assessment under Principle 1 above) as well as those records needed to be retained only temporarily will need to be identified as such.

The priorities and steps necessary to make the identified vital records and archival records usable again form a major part of the salvage strategy.

If the records are not vital or archival, they may be set aside to consider the resources available for repair or for preventing further damage. If some affected records have already met their legal retention periods under an approved Records Disposal Schedule, they are to be tagged for destruction rather than moved to temporary storage. Appendix G contains a draft Records Salvage Priority form.

Reconstruction of vital records or archival records is a related topic that falls under business continuity.

In the event of a disaster it is likely that alternative provisions for storing records will be required. Procedures are to identify the location and contact details of back-up storage facilities, which may be off-site.

As part of the procedures, a log of events is to be kept, commencing as soon as reasonably possible after a disaster. In the heat of a crisis, it is easy to forget. However an inquiry is likely to follow a disaster of any size, and notes made at the time are invaluable. The list of responsibilities is to nominate the people, or positions, who are required to keep a log of events. The timing of the commencement of the log is to be as early as possible, although this will be dependent on the unfolding of the disaster. As early as convenient, recollections of events early in the unfolding of the disaster are to be added to the log.

As the keeping of a log is frequently forgotten in the heat of the event, it is wise to practise it with every opportunity. Every disaster is to have a log, no matter how small the disruption. Those required to keep a log are to be advised to have notebook and writing implements ready at convenient locations.

A related topic is the handling of the media. If the disaster is sizeable, the media will be onsite very quickly. Those on the ground need to know the agency's policy about who is to speak to the media. The agency may choose to have all media contact handled centrally; in this case, those on the ground may be required to keep the central media area informed.

### *6. Implement the records salvage strategy*

Procedures for staff will stress that personal safety is paramount, and may suggest a series of actions, such as "Start moving the records from the affected area to temporary storage". All staff need to be aware of what records salvage may involve.

The needs of staff involved in salvage efforts must be considered. Someone needs to be in charge of salvage operations; if it is not the business unit manager, the person in charge needs to be clearly nominated. It is suggested that teams of three or four people be nominated to undertake the salvage operations. Special working arrangements may need to be negotiated with these people in advance.

The person in charge (business unit manager, team leader or delegate), must ensure that staff have:

- Security clearances (obtained in advance);
- Location of first aid areas and rest areas;
- Information about any areas declared out of bounds;
- Access clearance to relevant areas of the disaster;
- Information about the location of damaged records; and
- The task assigned to the team or staff member.

Disasters are frequently a source of stress, especially if they result in injury, death, or total destruction. The procedures are to address the need to arrange for food, water, a rest area, a first aid area, and even grief counselling if necessary. The procedures are to require that all staff involved in salvage operations work in short, rotating shifts.

The procedures are to also anticipate the need for an assessment area to which damaged material can be taken. The major requirement for this will be enough space to lay out records and pack material for freezing.

Priority and procedures must be advised, such as the following:

- The location of trolleys, crates, polythene bags, gloves, etc.;
- Vital records and archival records are highest priority;
- When records are removed from the disaster area, they must be labelled in the most convenient way to indicate their title/reference/series and location;
- Remove records from the floor first, keeping them open or closed as found;
- When removing records from shelves, the top shelf must be emptied first, working sequentially towards the bottom shelf;
- The records are to be placed in polythene bags to prevent further damage before being loaded into crates;
- Boxed records may be removed without having to place them in crates;
- Lists of material removed must be kept, include the contents of trolleys, crates, etc., and their proposed destination;
- Lists of the contents of temporary storage must be kept, including the contents of deep freezers;
- Material that is only slightly water damaged may be fan dried. Appendix H contains some advice about handling wet paper records that agencies can incorporate, as water damage is one of the more frequent disasters;
- Dry but fragmented material, such as following fire damage, are to be placed in a designated area ready for inspection by staff from the business area to which the records relate. If possible, they are to be sorted into those business areas; and
- After records have been removed, excess water is to be mopped up.

If a log of events has not already commenced, it must certainly start at this stage.

Restoration of the disaster site will generally not be responsibility of recordkeeping staff. However, before returning records to the cleaned up area, procedures may advise on measures to be taken, such as:

- Insisting that temperature and relative humidity levels have been stabilised at acceptable levels for at least a week before records are returned;
- Installing dehumidifiers and fans if necessary; and
- Washing down walls, ceilings, floors and shelves in a fungicide to inhibit mould growth.

The Standard requires agencies to produce and widely distribute the disaster response and business continuity documents. This ensures that as many people as possible have seen and understood the instructions about what to do in a disaster. The purpose is to enable staff not only to understand their own tasks, but to see the overall picture of what are to happen when disaster strikes.

In addition, agencies are to extract relevant instructions and display them in places where affected employees will see them.

## Business continuity

Business continuity refers to measures that are necessary for the swift and efficient resumption of normal business operations and normal service delivery after an emergency. The transition from disaster response to business continuity occurs when the immediate rush

of the emergency has passed. The immediate tension of the crisis is over, and the emphasis turns to reconstruction. Although implementation of the salvage strategy for damaged records continues, the focus of business continuity is broader as efforts shift from the damaged records to ongoing operations.

Apart from saving time and money, an agency will win support from the Government, its own people and the community if it gets back to work as quickly as possible after a disaster. Predetermined locations are to be nominated in advance, from which services can continue to be delivered if the main facility requires repair. If the damage is minor, records managers are to rearrange their remaining available workspace to accommodate displaced staff. If damage is extensive or complete, move to a pre-arranged site with a view to continuing essential operations. Business continuity requires that an agency set up shop as soon as possible after a disaster, so the procedures are to spell out how records-related services will resume work: where temporary offices will be located, what office equipment will be used, and what records and data will be available to do work.

At the same time, contractors who can remedy damaged records are to be contacted. The risk assessment will have identified which records have been protected by duplication and dispersal. Procedures are to detail how these duplicates can be brought into operation. The risk assessment will also have identified which vital records can be reconstructed from other sources, perhaps by re-keying. The Records Manager is to combine this information with the records damage assessment undertaken during the disaster response phase. A data recovery contractor or a freeze-drying specialist who may be able to reconstruct some of the records or the information contained in them should have been identified in advance.

Scanning or photocopying services that are able to film, digitise or copy smoke- or water-damaged paper records should also have been identified in advance, as the value of the records may not merit the cost of hiring a professional conservator or freeze-drying specialist. Alternative storage areas may be needed where smoke-damaged records can be retained for a short period. This may allow time for a decision to be made about their future, or it may be that the records need only be retained for a relatively short period so they can then be disposed of rather than paying to clean and deodorize them.

The log of events must continue during the business continuity phase of returning operations to normal.

It may be that salvage and business continuity operations are handled by teams of people working together. An important consideration is to ensure that communication between the teams is maintained at all times. It is unwise to rely solely on the business unit manager, team leader or delegate who is in overall charge of recovery operations. Recovery team leaders are to be given the responsibility and the means to maintain contact.

The business continuity plan, together with the disaster response plan, is to be published separately and widely distributed. Also, relevant instructions are to be displayed in places where people affected by the instructions will see them. Wide distribution will include holding copies offsite and giving relevant staff copies to have at home.

## Periodic review

As with all policies and procedures, the plan and associated procedures are living documents that must be reviewed, evaluated, and adjusted as needed. The plan must include a section that sets out the procedures that the agency will use to review and update it. The review

procedures are to nominate who, or which position(s), will undertake the review, and what their roles and responsibilities will be.

The review portion of business continuity planning must address how often the plan will be reviewed. Not every review need be major. The following are minimum review points:

- After every disaster rehearsal (or emergency practice), to identify any flaws that may have been identified and so correct the procedures or instructions affected;
- After every disaster, analyse to what extent the plan worked in practice and respond to any perceived weaknesses in strategies in the risk assessment, business continuity planning or associated procedures;
- Annually, to ensure risks and information are up to date; and
- After any event that changes the risk assessment significantly. For instance, a new recordkeeping system will change some risks, as will a new storage facility.

The annual review is to, as a minimum, update changes in:

- Records-related risks;
- Vital records assessment
- Archival records assessment;
- Roles, responsibilities and contact details, especially of disaster recovery teams;
- Training and awareness programs;
- Emergency equipment;
- Supplies and services;
- Back-up and off-site storage arrangements; and
- Alternative sites for recovery and conducting business.

## Roles and Responsibilities

Agencies must identify roles and responsibilities so that it is clear:

- Who will do what, both in an emergency and in preparation for, and planning to counter, a disaster; and
- Who has the authority to make decisions in relation to the management of a disaster

Many roles and responsibilities will be agency-specific. These must be spelt out so that staff members understand their roles and can rehearse them as far as practicable. They are not dealt with here. Agencies may find it useful to discuss roles and responsibilities at the Records Managers' Forum, as there may be benefits in having similar disaster-response positions in many agencies. The benefits are likely to be in staff learning similar roles in different agencies and in reducing the workload of business continuity planning for records.

Agency-specific roles and responsibilities are to include checklists of actions required of staff in nominated positions.

One position that is common to all agencies is the agency Records Manager. The roles and responsibilities of an agency Records Manager regarding the Records Management Program are discussed below.

### Responsibilities of an agency Records Manager

The agency Records Manager has responsibility for implementing the agency's Records Management Program, including identifying and managing vital records and archival records.

The records-related risk management and business continuity responsibilities of an agency Records Manager include:

- Ensuring the agency complies with *Standard for Records Management No.8 – Business Continuity and Records Management*;
- Carrying out the agency's business continuity planning for records;
- Ensuring that records are handled satisfactorily from a risk-management perspective;
- Ensuring that storage of records is satisfactory from a risk-management perspective, including ensuring that records are located as far as possible away from hazards, and that hazards are identified and preventative measures incorporated in the design and management of records storage facilities and workplaces;
- Implementing security and access requirements based on the agency's risk assessment of records-related threats to business continuity;
- Ensuring that access control to the agency's records management infrastructure is consistent with the security and access requirements;
- Maintaining document security practices that are consistent with the security and access requirements, such as a clear desk policy where appropriate;
- Monitoring the level of records security breaches and assisting with investigations;
- Providing briefings on records business continuity and risk management arrangements;
- Assisting in the development of the agency's business continuity and risk management plan and its security policy and plan;
- Developing an ongoing program of identifying and managing vital records and archival records, and ensuring these records become a critical part of the agency's business continuity planning for records;
- Attending the scene of a disaster (the agency Records Manager may delegate the attendance, but not the responsibility);
- Taking responsibility for all aspects of records-related risk assessment including risk identification and risk evaluation;
- Taking administrative responsibility for operating all aspects of business continuity planning, including the disaster response and business continuity phases;
- Assessing the scale of a disaster and deciding what is required to handle the situation;
- Ensuring disaster response team(s) have been brought in after a disaster;
- Liaising with emergency services;
- Managing the return to full business operations, possibly in conjunction with other agency staff;
- Providing reviews and evaluation of the agency's business continuity planning for records;
- Ensuring that sufficient staff training and awareness is provided, including training in emergency procedures to protect and salvage records;
- Ensuring that the integrity of vital records and archival records is maintained even in the event of a major disaster;
- Seeking to ensure that the Government and community are satisfied with the speed and comprehensiveness of an agency's resumption of full business operations following a disaster; and
- Seeking to ensure that the totality of records-related risk management is such that any post-disaster inquiry clears, or preferably praises, all aspects of the records-related handling of the disaster.

### Staff training and awareness

Staff training and awareness are critical components in successful risk management. It is essential that all staff members, especially new people, are made aware of potential hazards,

what to look out for, and what to do in the event of an emergency. This should be part of general health and safety awareness programmes. Information distributed to staff must be regularly updated.

Staff directly involved in records recovery are to make regular tours of buildings to familiarise themselves with:

- Alarm systems;
- Fire extinguishers;
- Shut-off points for water, gas and electricity;
- Location of records recovery equipment; and
- Assembly points in the event of an emergency.

It would be appropriate for key records staff to liaise with local emergency services, and to ask these staff to ensure that business recovery information, especially contacts, is kept up to date. Regular practices of the records disaster response are to be undertaken.

### Strategies for undertaking business continuity planning for records

Especially in larger agencies, business continuity planning for records has a greater chance of success if developed as a cooperative project involving records staff from across the agency. This is broader than simply employees whose duty statements refer to records. It should involve all those for whom good records management is essential.

The Records Manager may choose to delegate much of the development work, but responsibility for the success of the process remains with the agency Records Manager. The Records Manager should formally indicate the support of senior management for the work, and should notify all staff of the phases of the plan's development.

Charging a small team from across the agency with the development work may be a productive strategy, as the team is likely to call on co-workers to provide the background information (the records they create, their job functions, and work environment, risks etc.) that is essential. Staff must be committed enough to the plan to implement it as needed and to ensure that it remains a current, living document.

### Security clearances for records managers

There is a requirement for key staff dealing with records and information to have security clearances undertaken because of increased emphasis on security across ACT Government and in particular with regard to information/records in many different forms.

The *ACT Protective Security Policy and Guidelines* states on page 38 "If a person's duties require access to security classified information or areas he or she should have an appropriate clearance". Records managers have access to the whole of the department's records management system, including electronic records and so fall within this description.

# COMPLIANCE CHECKLIST

## Agency

A compliant agency can demonstrate that:

- The agency complies with *Standard for Records Management No.8 – Business Continuity and Records Management*;
- Records and records storage are handled satisfactorily from a risk management perspective;
- A current business risk impact assessment for records exists for the agency;
- A current business continuity plan for records exists for the agency and is adequately rehearsed;
- The agency's business risk assessment and business continuity plan for records are reviewed and updated;
- The control of vital records and archival records is maintained even in the event of a major disaster;
- The Government and community are satisfied with the speed and comprehensiveness of an agency's resumption of full business operations following a disaster; and
- The totality of records-related risk management is such that any post-disaster inquiry clears or praises every aspect of the records-related handling of the disaster.

## Principle 1

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

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

## Principle 2

A compliant agency can demonstrate that it has undertaken business continuity planning for records incorporating four phases of planning for business continuity:

- Disaster mitigation: a system of preventative measures to minimise the likelihood of the occurrence of anticipated disasters
- Disaster response: instructions that will lessen the impact of a disaster after it has already occurred

- Business continuity: measures that are necessary for the swift and efficient resumption of daily operations after a disaster
- Periodic review: adaptation of the business continuity plan for records to reflect current conditions.

A compliant agency can demonstrate that its Records Manager meets his or her responsibilities, by ensuring that:

- Instructions about disaster response and business continuity are widely distributed so that instructions during a time of crisis are sufficient, clear, understood and accessible;
- An agency's business risk impact assessment for records is used as the basis of a security and access classification scheme for records of the agency, so that it is clear who has access to which records;
- Records managers have access to all relevant parts of an agency's records management system, including electronic records. This is likely to mean that key staff dealing with records and information will require security clearances (see the ACT Protective Security Policy and Guidelines (p.38);
- Ongoing document security practices are consistent with the security and access requirements, such as a clear desk policy where appropriate;
- The level of records security breaches is monitored and investigations undertaken as required;
- Outsourced providers are meeting the agency's obligations regarding records, records management, recordkeeping systems and business continuity planning;
- All relevant staff are trained and adequately rehearsed in emergency procedures to protect and salvage records;
- Disaster mitigation measures are incorporated in the design and management of all of that agency's records storage facilities and workplaces.
- Briefings on security and access arrangements, and business continuity and risk management arrangements are provided as required;
- The scene of a disaster is attended (the agency Records Manager may delegate the attendance, but not the responsibility);
- All aspects of business continuity planning, including the disaster response and business continuity phases operate satisfactorily; and
- The return to full business operations following a disaster happens smoothly.

# DEFINITIONS

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

### Archival Records
See Territory Archives.

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

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

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

### Disaster
A wide range of major and minor upsets to records, records management and recordkeeping systems, ranging from a localised disruption to an emergency, crisis, catastrophe or disaster.

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

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

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

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

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

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

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

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

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

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

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

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

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

## REFERENCES AND FURTHER READING


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

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

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

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

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

Przybyla, Ann Marie and Geof Huth (2004) *Preparing for the Worst: Managing Records Disasters* Archives Technical Information Series # 82 2004 http://www.archives.nysed.gov/a/records/mr_pub82.pdf

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

*Public Sector Management Act 1994*

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

Standards Australia (2002*). AS ISO 15489-2002 Records management.* Sydney, NSW, Standards Australia International Ltd

Standards Australia. (2004). *HB 22:2004: Business continuity management*. Sydney, NSW, Standards Australia International Ltd.

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

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

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

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

*Territory Records Act 2002*

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

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

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

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

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

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

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

US National Archives and Records Administration. (1999). *Vital records and records disaster mitigation and recovery: an instructional guide.* Available 17 April 2007, from
http://www.archives.gov/records-mgmt/vital-records/

# APPENDIX A: ESTIMATING MITIGATION AND RECOVERY COSTS

After Przybyla and Huth, 2004, p.7

**Estimating costs**

Determine the potential costs of disasters to convince management of the need for a plan, compare the costs of recovery to those of initiating preventive measures, and budget ahead to respond to the likeliest disasters. You can also prioritize potential risks by estimating the relative costs of different types of disasters. Estimating possible recovery costs is never an exact science, but several methods do allow you to be fairly precise.

Base your estimates on the projected cost of losing specific records series or access to them. For example, calculate the labour hours needed to re-key data into an electronic records system, the cost of recovering essential data, the potential loss of income that would result from the unwanted destruction of vital records series, and the cost of litigation for which you lacked sufficient evidence. You can also use the following formula to estimate your *annualized loss expectancy*, or the amount that you could lose annually if a specific kind of disaster occurred:

Probability (P) x Cost (C) = Risk (R) or potential loss

In this formula, P represents the probability that a threat will occur in any given year. If a specific kind of disaster is likely to occur once a year, P equals 1; every two months, P = 6; every four years, P = 0.25; every ten years, P=0.10, and so on. Provide costs, or C, in terms of the dollar amount of replacing, reproducing, or doing without a records series. For example, if you know that a flood tends to occur every ten years, and the potential cost of litigation for which you didn't have the necessary records is $25,000, then your annualized loss expectancy or risk is $2500. This formula is a useful way to develop consistent figures on the potential costs of records disasters, which you can then compare to those of prevention.

## APPENDIX B: STARTER RISK IDENTIFICATION AND EVALUATION CHECKLIST

| **Water damage** | **Details** | **Impact** | **Likelihood** | **Recovery & continuity costs*** |
|---|---|---|---|---|
| Stormwater flooding – external to building | | | | |
| Poor roof drainage/flat roof | | | | |
| Rain gutters obstructed/clogged | | | | |
| Inadequate roof covering and flashings | | | | |
| History of roof leaking | | | | |
| Poor window/skylight seals | | | | |
| Broken/cracked windows | | | | |
| Hydrants not marked or accessible | | | | |
| Leaking water pipe in building | | | | |
| Leaking sewerage pipe | | | | |
| Leaking steam pipe | | | | |
| Old water pipes | | | | |
| Evidence of previous water leaks | | | | |
| Fire sprinkler discharge | | | | |
| Inadequate or infrequent inspection of water hazard sources | | | | |
| **Fire damage** | **Details** | **Impact** | **Likelihood** | **Recovery & continuity costs*** |
| Bushfire, including grass fire | | | | |
| Fire in adjacent building | | | | |
| Fire in adjacent lease within the building | | | | |
| Old or overloaded electrical system | | | | |
| Electrical failure leading to fire | | | | |
| Inadequate or infrequent inspection and testing of fire control systems | | | | |
| Water supply failure | | | | |
| Insufficient number of fire extinguishers | | | | |
| Extinguishers not properly charged | | | | |
| Fire alarms not working | | | | |
| Fire alarms not tested regularly | | | | |
| No fire suppression system | | | | |
| No sprinkler system | | | | |
| Fire exits blocked | | | | |
| Inflammable substances stored in building | | | | |
| No back up power supply (if required for fire control systems) | | | | |
| Smoking not restricted to safe areas with fireproof containers for butts | | | | |
| Liaison not maintained with local fire prevention officers | | | | |

| **Environmental damage** | **Details** | **Impact** | **Likelihood** | **Recovery & continuity costs*** |
|---|---|---|---|---|
| Earthquakes | | | | |
| Hail storms | | | | |
| In a flood plain | | | | |
| Large trees nearby | | | | |
| Location of utility poles | | | | |
| Located near highway | | | | |
| Located near hazardous material transport route | | | | |
| Chemical spill | | | | |
| Possible terrorist target | | | | |
| Construction site or adjacent to construction site | | | | |
| Vermin infestation | | | | |
| Vermin infestation in adjacent leases/tenants/buildings | | | | |
| **Security – Access, Building, Storage** | **Details** | **Impact** | **Likelihood** | **Recovery & continuity costs*** |
| Access: no or inadequate access arrangements in place for staff | | | | |
| Access: poor key control | | | | |
| Access: no or inadequate access arrangements in place for visitors | | | | |
| Access: unsupervised access to records | | | | |
| Access: no monitoring during use of records | | | | |
| Access: no automatic intruder alarm system fitted | | | | |
| Access: staff members unaware of the need for good security | | | | |
| Access: vandalism | | | | |
| Building: no dehumidifiers | | | | |
| Building: dehumidifiers do not drain automatically | | | | |
| Building: dehumidifiers not checked regularly | | | | |
| Building: problems with heating or cooling systems | | | | |
| Building: fire alarms and extinguishers not marked on floor plans | | | | |
| Building: door alarms on fire exits not functioning | | | | |
| Building: alarms do not ring within facilities | | | | |
| Building: alarms do not notify first responders | | | | |
| Building: no security service contract | | | | |
| Building: no emergency lighting system | | | | |
| Building: no emergency generators | | | | |
| Building: fire exits not clearly market | | | | |
| Building: fire exits blocked | | | | |

| | | | | |
|---|---|---|---|---|
| Storage: open files or volumes on shelves | | | | |
| Storage: unstable shelving | | | | |
| Storage: shelving not anchored to wall or ceiling | | | | |
| Storage: bottom shelving not raised at least 50mm off floor | | | | |
| Storage: records stored in basement | | | | |
| Storage: records stored near bathrooms or sewerage pipes | | | | |
| Storage: records stored near windows, skylights, air conditioners, boilers, etc | | | | |
| Storage: storage area not locked | | | | |
| **Records Management – recordkeeping systems, IT failure, human error** | **Details** | **Impact** | **Likelihood** | **Recovery & continuity costs*** |
| Systems: vital records inaccurately identified | | | | |
| Systems: archival records inaccurately identified | | | | |
| Systems: vital records not quickly accessible and usable | | | | |
| Systems: failure of recordkeeping system controls | | | | |
| Systems: record finding tools are inadequate or fail | | | | |
| Systems: recordkeeping system not up to date | | | | |
| Systems: recordkeeping system inadequate | | | | |
| Systems: inadequate or incomplete staff training | | | | |
| Systems: inadequate preparation for the natural decay of materials | | | | |
| IT: Virus/firewall protection fails | | May be | redundant | with |
| IT: Regular backup fails | | Standard | 6: Digital | Records |
| IT: Backups too infrequent to allow recent records to be recovered | | | | |
| IT: computer equipment failure | | | | |
| Human error: record filed in wrong place | | | | |
| Human error: file put away in wrong place | | | | |
| Human error: record lost/damaged during transfer | | | | |
| Human error: key staff leave | | | | |
| Human error: staff not at work | | | | |
| Human error: recordkeeping system procedures not followed | | | | |
| Human error: criminal behaviour | | | | |

* "Disaster & continuity costs" means estimates of the disaster recovery and business continuity costs that would result should the identified hazard occur.

## APPENDIX C: DISASTER RESPONSE CONTACT DETAILS

This response checklist will help you determine which individuals to contact in case of disaster, each person's assignments, and key sites to use for coordinating the recovery. A completed checklist will save time and effort during an emergency.

| **Contacts – people who may be notified** | **Name** | **Work ph.** | **Mobile** | **Home ph.** |
|---|---|---|---|---|
| Emergency Services | | | | |
| Police | | | | |
| Records Manager | | | | |
| Building supervisor | | | | |
| Building maintenance manager | | | | |
| Building security officer | | | | |
| Business unit manager – must contact | | | | |
| Business manager's delegate – if BM n.a. | | | | |
| Records Recovery Team Coordinator – must | | | | |
| Recovery Team members | | | | |
| Territory Records Office | | | | |
| | | | | |
| **Internal Contacts – may be needed** | **Name** | **Work ph.** | **Mobile** | **Home ph.** |
| Key holders | | | | |
| Holders of first aid certificates | | | | |
| OH&S officers | | | | |
| | | | | |
| **External Contacts** | **Name** | **Work ph.** | **Mobile** | **Home ph.** |
| ActewAGL | | | | |
| Locksmith | | | | |
| Plumber | | | | |
| TransACT | | | | |
| Electrician | | | | |
| | | | | |

## APPENDIX D: DISASTER RECOVERY AND BUSINESS CONTINUITY RESPONSIBILITIES

| Action | Officer and his/her contact details | Delegate and his/her contact details |
|---|---|---|
| Assess situation | | |
| Determine safety of building/site | | |
| Ongoing emergency services liaison (during disaster response and business continuity) | | |
| Identify appropriate initial records response | | |
| Take log of events | | |
| Photograph the situation and progress | | |
| Assess records damage | | |
| Develop records salvage strategy | | |
| Media liaison (or liaison with agency's media unit) | | |
| Authorise disposition of damaged records | | |
| Authorise external salvage assistance | | |
| Implement salvage strategy | | |
| Team leader 1 – salvage operations 1 | | |
| Team leader 2 – salvage operations 2 | | |
| Rosters, staff wellbeing, counselling, refreshments, etc | | |
| Coordinate volunteers | | |
| Authorise purchases (eg additional materials) | | |
| Authorise record reconstruction | | |
| | | |

# APPENDIX E: LIST OF DISASTER EQUIPMENT AND EXTERNAL EQUIPMENT SOURCES

## Location of recovery facilities

| Location of recovery facilities | Onsite | Offsite |
|---|---|---|
| Command post | | |
| Disaster supplies | | |
| Recovery or salvage site | | |
| Duplicate or backup of vital records | | |
| Duplicate building plans | | |
| Duplicate disaster plan | | |
| Salvage team(s) rest area (incl. toilets) | | |
| Assessment area | | |
| Alternative site for commencement of business operations | | |
| | | |

## Supplies and equipment for disaster response

| Type | Location |
|---|---|
| Fire extinguishers | |
| Dehumidifier | |
| Fans | |
| Pallets | |
| Plastic sheeting | |
| Duct tape | |
| Portable sump pump | |
| Wet-dry vacuum | |
| Plastic garbage cans | |
| Plastic crates | |
| Rubber gloves | |
| Protective clothing | |
| First aid kit | |
| Paper towels | |
| Blotting paper | |
| | |

## Outside sources for equipment and supplies

| Item | On site | Firm and contacts | Phone numbers (day and night) |
|---|---|---|---|
| Freezer space | | | |
| Dehumidifiers | | | |
| Drying space | | | |
| Fans | | | |
| Plastic crates | | | |
| Pallets | | | |
| Plastic sheeting | | | |
| Portable sump pump | | | |
| Refrigerator | | | |
| Wet-dry vacuum | | | |
| Packing paper | | | |
| Blotting paper | | | |

| | | | |
|---|---|---|---|
| Plastic trash cans | | | |
| Plastic trash bags | | | |
| Rubber gloves | | | |
| Protective clothing | | | |
| Respirators | | | |
| Fork lift | | | |
| Fumigation supplies | | | |
| | | | |

# APPENDIX F: INITIAL DAMAGE ASSESSMENT FORM

**Initial Damage Assessment Form**

(After Przybyla and Huth, 2004)

## DISASTER LOCATION

Address: _____

Name of person reporting: _____

Telephone: _____

Date and time of report: _____

Estimated start time of damage: _____

## DESCRIPTION OF DISASTER

### *Type of damage:*

☐ **Fire and smoke**

☐ **Water:** ☐ Sewage ☐ Muddy ☐ Clean ☐ Other _____

Source: ☐ Roof ☐ Pipe ☐ Window ☐ Wall _____

☐ **Collapsed:** ☐ Roof ☐ Wall ☐ Shelves ☐ Other _____

☐ **Infestation:** ☐ Mould ☐ Rodent ☐ Insect ☐ Other _____

☐ **Other** _____

### *Amount of damage:*

☐ Boxes: _____ ☐ Stacks: _____

☐ Whole floor: _____ sq. m. ☐ Whole building: _____ sq. m.

### *Type and quantity of materials involved:*

___ Bound volumes _____ Vital records _____ Photographs

___ Microfiche/microfilm _____ Archival records _____ Computer disks, tapes, compact disks, etc

___ Paper _____ Maps Other: _____

### *General condition of records:*

☐ Soaked ☐ Still under water ☐ Damp

☐ Dirty or muddy ☐ Scattered on floor ☐ Mouldy

☐ Smoke damage Other: _____

## SITUATION AT DISASTER SITE

Has the source of the problem been halted or controlled? ☐ Yes ☐ No

Do you have access to the building? ☐ Yes ☐ No

If no, when will you have access? _____

Are the following available: If no, when will these services resume:

| | | | |
|---|---|---|---|
| Electricity | ☐ Yes | ☐ No | _____ |
| Water | ☐ Yes | ☐ No | _____ |
| Air conditioning | ☐ Yes | ☐ No | _____ |

Are there health hazards at the disaster site? ☐ Yes ☐ No

If yes, please detail:

Are there environmental hazards at the disaster site? ☐ Yes ☐ No

If yes, please detail:

| Have you contacted? | | | Time of contact, and comments: |
|---|---|---|---|
| Emergency Services | ☐ Yes | ☐ No | _____ |
| Police | ☐ Yes | ☐ No | _____ |
| Records Manager | ☐ Yes | ☐ No | _____ |
| Building supervisor | ☐ Yes | ☐ No | _____ |
| Building maintenance manager | ☐ Yes | ☐ No | _____ |
| Building security officer | ☐ Yes | ☐ No | _____ |
| Business Unit Manager | ☐ Yes | ☐ No | _____ |
| Business Manager's delegate | ☐ Yes | ☐ No | _____ |
| Recovery team coordinator | ☐ Yes | ☐ No | _____ |
| Recovery team members | ☐ Yes | ☐ No | _____ |
| Territory Records Office | ☐ Yes | ☐ No | _____ |
| Others _____ | | | _____ |
| _____ | | | _____ |
| _____ | | | _____ |
| _____ | | | _____ |
| _____ | | | _____ |

## APPENDIX G: RECORDS SALVAGE PRIORITY LIST

List records for salvage in order of priority, taking into account which records are stored near each other. If necessary, attach a floor plan to illustrate where the records are located. (include e records)

| | RECORDS | VOLUME | LOCATION |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 10 | | | |
| 11 | | | |
| 12 | | | |
| 13 | | | |
| 14 | | | |
| 15 | | | |
| 16 | | | |
| 17 | | | |
| 18 | | | |
| 19 | | | |
| 20 | | | |

(After Przybyla and Huth, 2004)

# APPENDIX H: WET PAPER RECORDS

*After Przybyla and Huth, 2004, pp.15*

**Wet paper records**

Wet records are of critical concern because they can begin to grow mould within forty-eight hours. First, salvage any records threatened with further damage because they are under water or about to fall. Immediately reduce temperature and humidity levels in wet or humid storage areas, and set up fans, air conditioners, and dehumidifiers to help dry out these areas. If some boxes holding records are falling apart, temporarily store their contents in plastic crates to keep them neat and under control. You can use cardboard boxes if you don't have any plastic containers. After re-boxing the records, move them to a safe and environmentally stable area. Finally, move all re-boxed records to a dry, sheltered location. Never leave wet records to dry on their own, and do not leave them in an area with standing water, high humidity levels, or mould growth.

To remedy damage to the records themselves, move them to a cold, dry environment. If a large quantity of records is involved, check with supermarkets, or businesses to see whether space is available in an industrial-size freezer for temporary storage. Then contact a company that specializes in freeze-drying records to extract moisture completely. Freezing records will prevent further damage while they are waiting to receive attention.

If you are dealing with a small quantity of records, sort them according to type of material and dry them using the appropriate method listed below:

- *Damp, coated or uncoated paper:* Fan pages open, insert blotter paper, and position them under a fan so air circulates between the leaves.
- *Wet, uncoated paper:* Interleave pages with a paper towel or blank newsprint until damp, then remove the interleaving and proceed as above.
- *Wet, coated paper:* Interleave pages with waxed paper, then fan open, and proceed as for wet uncoated paper.
- *Photographs:* Rinse in clear, cold water. Dry them face-up on a blotter or hang them on a laundry line.

Once dried, place the records in new cartons. Label the boxes with records series titles, dates, and retention periods so that you know what each box contains.

*After National Archives of the UK, p.9:*
Air drying will be suitable for small quantities of records which have only been slightly damaged by water. If the disaster can be contained in this way, the following procedures are to be followed:

- Use fans and de-humidifiers to assist the drying process
- Stand damp volumes upright and gently fan out the pages; interleave with blotting paper, if possible
- Books printed on coated paper and photographic prints should be interlaced with silicone release paper to prevent blocking
- Blotting paper should be placed between individual sheets of files
- Do not attempt to separate material stuck together; this is a job for expert conservators