

# **Records Management Standards Business Recovery Plans**

## **Standards for the management of Government records RMS 3.2**

### **Preface**

1. This standard has been prepared by the Public Record Office (PRO) and is one of a series of Records Management Standards for use by all organisations creating or holding public records.
2. Protection of records against elements such as floods, fire, theft and loss through carelessness is an essential part of the records management role. Adequate measures must be taken to safeguard all of an organisation's records.
3. While it is important to recognise the value of preventative measures, records managers should also have in place a plan specifically designed to secure an organisation's vital records and to react effectively and efficiently in the event of a disaster.
4. A business recovery plan should cover both prevention and reaction. It should be concerned with short to medium term measures enabling the organisation to continue its business with minimum disruption. It should not be confused with business continuity management, which is concerned with service over the longer term, such as staff shortages in specialist areas.

### **Contents**

- 1) Scope
- 2) Definitions
- 3) Responsibilities
- 4) Risk Assessment
- 5) Vital Records
- 6) Recovery Plan
- 7) Annexes
- 8) Model Recovery Plan
- 9) British and International Standards

### **1. Scope**

- 1.1 This standard is a best practice benchmark for all organisations creating or holding public records and is aimed at records managers who, with no conservation or preservation skills, are faced with potential risks to their organisation's records.
- 1.2 It provides advice and guidance on the development and implementation of business recovery plans, and covers three main areas: · Identification and protection of vital records · Measures to minimise the occurrence of disasters · Recovery plans and procedures in the event of a disaster
- 1.3 As far as possible the standard applies to all records, including electronic records. Procedures for risk assessment and the identification of vital records are the same for records in all media. Standards relating to the recovery of damaged electronic records are being developed by other organisations such as the Central Computer and Telecommunications Agency (CCTA).

### **2. Definitions**

For the purposes of this standard the following definitions apply:

**2.1 Active records.** Records still being used by an organisation for the conduct of its current business or still open for that purpose.

**2.2 Archives.** Those records that are appraised as having permanent value.

**2.3 Client Manager.** An officer of the Public Record Office responsible for giving advice and guidance to a group of government departments and agencies, to provide for the timely and effective appraisal, documentation and accessioning of departmental records.

**2.4 Departmental Record Officer.** The person appointed by a government department or agency as being responsible for the management of the records of that organisation.

**2.5 Electronic records.** Records where the information is recorded in a form that is suitable for retrieval, processing and communication by a digital computer.

**2.6 Fire-resistance.** The ability of an element of building construction to satisfy, for a stated period (usually expressed in hours), some or all of the criteria specified in the appropriate part of BS 476 Fire Tests on Building Materials and Structures, namely resistance to collapse (loadbearing capacity), resistance to flame penetration (integrity), and resistance to excessive temperature rise on unexposed surfaces (insulation).

**2.7 Microform.** Records in the form of microfilm and microfiche, including aperture cards.

**2.8 Public Records.** Records of, or held in, any department of Her Majesty's Government in the United Kingdom or records of any office, commission or other body or establishment whatsoever under Her Majesty's Government in the United Kingdom, as defined in paragraph 2 of the First Schedule to the Public Records Act 1958. Also records of organisations subsequently included in the table in the above Schedule or of those whose records have since been determined as public records by the Public Record Office.

**2.9 Public Records Act 1958.** Legislation 6 & 7 Eliz. 2, Ch 51.

**2.10 Relative humidity.** The amount of moisture in a given amount of air as compared with that of complete saturation at a given temperature (expressed as a percentage).

**2.11 Semi-current records.** Records which are no longer required for the conduct of current business and which are waiting to be appraised for their long-term value or disposed of in accordance with disposal schedules.

**2.12 Vital records.** Those records without which an organisation could not continue to operate, and which contain information needed to re-establish the organisation in the event of a disaster.

### **3. Responsibilities**

**3.1** Departmental Record Officers and Records Managers are responsible for safeguarding all the records of their organisation, including the safe-keeping, accessibility and retention of records for as long as required, the transfer of those public records selected for permanent preservation, and the timely destruction of records no longer required.

**3.2** Business Recovery Officers (or Disaster Control Officers) are responsible for:

- Maintaining a business recovery manual
- Attending the scene of an emergency

- Taking administrative responsibility for a business recovery operation
- Assessing the scale of damage and deciding on what is required to handle the situation
- Summoning recovery teams as necessary
- Informing senior management and contractors' representatives
- Liaising with the local fire brigade and other services
- Providing reports of incidents and evaluation of business recovery plan effectiveness
- Making arrangements for training and awareness

3.3 Business Recovery Teams are responsible for salvage operations and for assisting the Business Recovery Officer generally.

3.4 PRO Client Managers are responsible for giving advice and guidance to government departments and agencies on the management of their records, including the identification and storage of vital records, the development of business recovery plans and the provision of sources of expert advice on the conservation and preservation of damaged records.

#### **4 Risk Assessment**

4.1 The process of risk assessment has three elements:

- Identification
- Estimation
- Evaluation

4.2 Identification

The identification of risk to records and information falls into four main categories:

- Flood
- Fire
- Security
- Infestation, environmental pollution, etc

4.2.1 Flood. Water damage is the most common form of disaster to affect records. Much of this can be avoided by improving design and maintenance of buildings and expert advice in this area should be sought. However, there are a number of actions which records managers can undertake to minimise the risk of damage:

- Identify and check regularly potential internal and external hazards (for example, heating systems, water tanks and water pipes)
- Identify and check regularly potential penetration hazards (for example, windows, gutters, skylights and drains)
- Ensure that heating and air-conditioning systems are regularly checked and serviced
- 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
- Never put records on the floor

4.2.2 Fire. Fire Prevention Officers must be made aware of important collections of records and information, including catalogues and metadata. The Health and Safety at Work Act 1974 and related regulations place

particular obligations on organisations in respect of fire precautions. Records managers should be aware of these obligations. In identifying their own risks the following actions can be undertaken:

- Ensure that all existing fire regulations in respect of doors, extinguishers and alarm systems are enforced
- Maintain a list of inflammable substances and isolate them from the building
- Keep storage areas clean and tidy
- Check electrical wiring regularly
- Permit smoking only in designated, safe areas
- Maintain liaison with local fire prevention officers

4.2.3 Security. Each building and each collection of records poses its own security problems. Records managers should liaise closely with departmental security officers to minimise the risk to their holdings from loss or theft. The following actions should be undertaken:

- Caretakers/security guards should 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
- Buildings with no caretaker or security cover should be fitted with an automatic intruder alarm system
- All staff members should be aware of the need for good security (for example, good key control; checks on criminal records; and identification procedures)

4.2.4 Other. Unlikely risks to the records, such as infestation from insects and animals, and environmental pollution, should also be taken into consideration. Prevention measures, including traps and poisons, and filtering systems, might be taken.

### 4.3 Estimation

4.3.1 However many risks an organisation faces, there are relatively few effects. They might be categorised as:

- Loss of critical systems, site or personnel
- Denial of access to systems or premises

4.3.2 In order to estimate potential disasters, local geographical, environmental and political factors, as well as the nature of the work of the organisation, should be taken into account. For example:

- What is the likelihood of flooding?
- What is the quality of the fire precautions systems?
- Is the work of the organisation of a sensitive nature which might attract theft or bomb threats?
- What is the volume of the identified vital records?
- What are the retrieval requirements of the identified records?
- Are special storage facilities required for all, or some, of the records, such as electronic and microfilm?

These estimations should be prioritised in order of the degree of risk.

4.3.3 The risks to electronic records may be significant. For example, electronic records could be lost through a system failure caused by internal or external factors. The risks are best avoided by having suitable storage plans and strategies. A back-up system is generally recommended. The ease with

which back-ups can be rotated and protected is a key consideration in the selection of storage options.

4.4 Evaluation An indicator system might be used to evaluate the risks:

**Impact:**

1. Major problem; mixture of business risks and project risks
2. Could cause problems - mainly project risks
3. Unlikely to cause real problems

**Likelihood**

- a. High - likely to happen business risks and project risks
- b. Medium to high - could happen
- c. Medium - might happen in right conditions
- d. Low to medium - probably will not happen
- e. Low - very unlikely

## 5 Vital Records

Vital records are those records without which an organisation could not continue to operate. They are the records which contain information needed to re-establish the business of the organisation in the event of a disaster and which protect the assets and interests of the organisation. It is estimated that up to ten per cent of an organisation's records can be classified as vital.

### 5.1 Identification

5.1.1 The records manager needs to analyse the business and the records it produces in order to:

- Identify critical processes and functions
- Identify key internal and external dependencies on which these processes rely
- Identify external influences which may have an impact on critical processes and functions
- Identify the records relating to the critical processes and functions

5.1.2 Since it is expensive to make special protection arrangements for records it is important not to be tempted to include everything that might be vital. Key points to consider are:

- Whether the processes or functions can be re-established without the records concerned
- Senior management view of the importance of the functions to which the records relate
- The length of time for which information is required

5.1.3 For the purpose of identifying vital records, all records might be classified as follows:

- Vital - see 5 above
- Important - can be reproduced from original sources but only at considerable expense
- Useful - loss would cause temporary inconvenience
- Non-essential - no value beyond immediate purpose

5.1.4 Examples of records which might be classified as vital:

- Minutes of management board meetings
- Manuals and instructions
- Pay rates
- Annual reports and other personnel records
- Legal documents, including current contracts
- Computer software programmes and data
- Accounts, payable and receivable
- Plans
- Communications/contact information
- Indexes/finding aids to records

5.1.5 When vital records have been identified they should be documented so that everyone in the organisation is aware of them. A sample inventory form follows:

Division:			Contact:		
Description:	Disposal Reference:	Protection:		Supporting Documents:	Original or Copy:
		Format:	Location:		

*Description* - category or type of vital record

*Disposal reference* - cross reference to any disposal schedule pertaining to the record(s)

*Format* - how the vital record is protected (duplicated, dispersed, etc)

*Location* - where protected vital record is held (the copy, if duplicated)

*Supporting documents* - description of any supporting documents such as finding aids

*Original or copy* - whether the protected vital record is an original or copy

5.2 Protection

5.2.1 There are three options for protecting vital records:

- Duplication and dispersal (the duplicate may be in paper or alternative format, such as microform or CD)
- Use of fireproof and secure storage facilities
- Remote storage

5.2.2 The storage of records in electronic form may involve significant risks but many of these can be avoided by the use of adequate storage plans and strategies. A back-up system is generally recommended.

## **6 Recovery Plan**

6.1 The business recovery plan brings together the actions necessary at the time of an incident, who needs to be involved, and how and when they are to be contacted. The plan must be reviewed at least once a year and updated, if necessary. The plan should cover:

- Identification of business recovery teams
- Training and awareness programmes
- Emergency equipment
- Supplies and services
- Back-up and off-site storage arrangements
- Vital records

### **6.1.1 Recovery Teams**

Teams of three or four people should be formed to undertake salvage operations under the supervision of the Business Recovery Officer. They should be prepared to take part in the operations during or after a disaster and appropriate terms and conditions for overtime and unsocial hours work should apply. They should live within a reasonable distance of the building(s) by walking, driving or reliable public transport, and should be available on the telephone.

### **6.1.2 Training and Awareness**

It is essential that all staff, especially new staff, 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 business recovery should make regular tours of buildings to familiarise themselves with:

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

They should also liaise with local fire prevention officers, be familiar with the use of fire-fighting equipment, and ensure that business recovery information is kept up to date.

The Business Recovery Officer and Business Recovery Teams should undertake regular practices of the recovery plan to ensure that the procedures are still effective.

6.1.3 Emergency Equipment It is unlikely that equipment and materials to cover every emergency can be stored. However, supplies of essential equipment should be kept in different strategic areas of the building in

storerooms or cupboards that are clearly marked. Small items for use in an emergency should be kept on trolleys for easy transportation. Larger items might be stored centrally or available for loan or hire at the time of the emergency. Essential equipment should comprise:

- Mops
- Rubber gloves
- Floor cloths
- Hazard tape
- Torches
- Protective clothing
- Plastic sheeting
- Blotting paper
- Plastic crates
- One crate containing:
  - Identification forms
  - Large polythene bags
  - Name tags and string
  - Pencils and pencil sharpeners
  - Scissors - Cotton tape
- Plan of the building showing:
  - Electricity cut-off
  - Water shut-off valve
  - Gas shut-off
  - Sprinkler system/CO2 system
  - Fire extinguishers
  - Stored chemicals
  - Emergency equipment

#### 6.1.4 Supplies and Services

The plan must include lists of staff having specific responsibilities, with their contact details, who may need to be summoned in an emergency. In addition to the Business Recovery Officer and Business Recovery Teams, these may include:

- Key holders
- Building maintenance managers
- First aiders
- Security

A list of services, companies and individuals, with contact details, should also be made. Those that might be needed in an emergency include:

- Gas/water/electricity authorities
- Fire/ambulance/police services
- Carpenter - Glazier
- Locksmith
- Electrician
- Plumber
- Pest control officer
- Fire alarm service
- Legal adviser

- Conservation document salvage service
- Deep freeze facility

The most common items likely to be needed are:

- Pumps
- Fans
- De-humidifiers
- Vans/trucks

Additional crates There are a number of organisations providing document salvage services or deep freeze facilities. If it is likely that such a service will be required, it is advisable that they be contacted for details before an emergency occurs. By doing this it is possible to evaluate services and costs outside an emergency situation.

**6.1.5 Storage Arrangements** In the event of an emergency it is likely that alternative provisions for storing records will be required. The recovery plan must include the location and contact details of back-up storage facilities, which may be off-site.

**6.1.6 Vital Records** The plan should include priority lists of what items should be salvaged first. The inventory of vital records (see 5.1.5 above) could be annotated accordingly.

Annex 1  
Model Recovery Plan  
Reaction Procedure

## **1 During Working Hours**

1.1 For emergencies occurring during working hours, it is essential that every member of staff be acquainted with procedures to raise the alarm.

1.2 The Head of Security [or Estates Manager or designated person] must be contacted. That person should be aware of maintenance or building work in progress in order to be able to assess the disaster situation effectively in so far as it affect records and information.

1.3 If the incident cannot be contained, the Business Recovery Officer must be contacted. That person will contact people from the Business Recovery Teams.

1.4 No records should be moved until the arrival of the Business Recovery Officer who will assess the damage and the help required in the first instance.

## **2 Out of Working Hours**

2.1 Night security guards should take any action which will reduce or limit the potential damage, if it is safe to do so. This might include:

- Turning off stopcocks
- Switching off electric lights
- Unplugging appliances
- Closing doors and windows
- Using hand-held fire extinguishers

2.2 Even if the incident can be contained, the Estates Manager [or designated officer] must be informed.

2.3 If a disaster cannot be contained the emergency services must be informed and the following personnel must be contacted immediately:

	Tel no.
<i>name</i> Estates Manager	xxx xxxx
<i>name</i> Central Services Manager	xxx xxxx
<i>name</i> Head of Security	xxx xxxx

[or designated staff]

2.4 The Estates Manager must visit the site and, after assessing the disaster, contact the Business Recovery Officer or their deputy:

	Tel no.
<i>name</i>	xxx xxxx
<i>name</i>	xxx xxxx

2.5 No records must be removed until the arrival of the Business Recovery Officer who will assess the damage to the records and the help that is required in the first instance. They will:

- Contact emergency services if necessary
- Contact appropriate staff
- Decide on the area(s) to be used for the assessment of damaged records
- Allocate staff rest area(s)

2.6 If it seems that the emergency will mean the closure of the office, the Business Recovery Officer must contact the organisation's head to inform them of the situation. Emergency procedures not directly concerned with the management of records and information should then be implemented (for example, procedure in the event of a power cut).

#### Recovery Procedure

All staff must wear protective clothing before starting work

#### **1 Instructions for Estates Manager [or designated officer]**

1.1 When alerted about a disaster the Estates Manager must view the disaster location as soon as possible and assess the situation, in order to estimate the extent of the disaster recovery procedures and back-up facilities required.

1.2 The Estates Manager must contact the Business Recovery Officer and appraise them of the situation so that procedures to contact Business Recovery Teams can begin.

1.3 The Estates Manager must also contact facilities management personnel.

1.4 Facilities management personnel will liaise with security staff to ensure that the building and surrounding areas are secure from unauthorised access.

#### **2 Instructions for Business Recovery Officer**

2.1 When alerted about a disaster the following members of staff must be contacted before going to the disaster location. They should be put on alert for possible further action:

[Name]	[Post]	[tel no]
--------	--------	----------

[these staff members might be those most closely concerned with the particular records that have been damaged or senior management]

2.2 The designated conservation document salvage service or deep freeze facility must be contacted and informed about the disaster.

2.3 On arrival at the disaster location contact must be made with the Estates Manager and, when access to the building is permitted by the Emergency Services, the damage assessed.

2.4 Air drying will be suitable for small quantities of records which have only been slightly damaged by water. Thus, if the disaster can be contained in this way, the following procedures should be followed:

- The requisite number of people from the Business Recovery Teams summoned to deal with the situation
- 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
- Change blotting paper regularly
- Do not attempt to separate material stuck together; this is a job for expert conservators

2.5 Small amounts of dry fragmentary material (resulting, perhaps, from fire damage) should be gathered and made available to staff of the business area to which the records belong in order that it might be identified and salvaged, if necessary.

2.6 If the disaster cannot be contained, as many members of the Business Recovery Teams as possible should be summoned. They will work under the direction of the Business Recovery Officer. When they arrive at the location of the disaster, security staff should issue them with special passes for which they must sign when entering or leaving the building. They must also be issued with protective clothing.

2.7 An assessment area must be designated 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.

2.8 Arrange with the facilities management staff for the installation of emergency lighting, if this is necessary.

2.9 A suitable rest area for the business recovery staff should be provided. If there is no mains water supply, the Estates Manager should be asked to arrange for a supply of drinking water and other necessary facilities. Health and safety of the staff must be given the highest priority.

2.10 Cupboards and doors to storerooms containing emergency equipment must be unlocked. These are located at:

xxx

xxx

2.11 Before any full-scale salvage operation is begun the Business Recovery Teams must be briefed on the following:

- Location of disaster
- Allocation of tasks
- Location of assessment area
- Location of rest area
- Location of first aid room
- Rotas and rest breaks

2.12 A log of events must be kept (including photographs, if possible) and a final report on the disaster made to senior management.

2.13 Communication between teams must be maintained at all times.

2.14 Liaise with the Press Officer if the disaster attracts media attention. All requests from the media are to be referred to the Press Officer or, in their absence, to the most senior person available.

### **3 Instruction for Business Recovery Teams**

3.1 Try to get to the location of the disaster as quickly as possible. Keep the Business Recovery Officer informed if any delay is encountered.

3.2 Having been issued with a special pass and protective clothing, report to the Business Recovery Officer.

3.3 Make sure that you have the following information:

- Location of damaged records
- Task assigned to
- Assessment area
- Rest area
- Location of first aid facilities
- Any areas declared out of bounds

3.4 Any areas adjacent to the location of the disaster should be protected by plastic sheeting to prevent any further damage occurring.

3.5 When records are removed they must be labelled in the most convenient way to indicate their title/reference and location.

3.6 Damaged records must be removed from the location of the disaster to the assessment area using plastic crates and trolleys. Records should be removed 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 should be placed in polythene bags to prevent further damage before being loaded into the crates. Boxed records might be moved without having to place them in crates.

- Trolleys are to be found in [xxx]
- Crates are to be found at [xx]
- Recovery materials are kept in the emergency equipment cupboards and storerooms located at [xx]

3.7 Material slightly damaged with water can be treated by fan drying (see section 2.3).

3.8 Dry but fragmented material should be placed in a designated area ready for inspection by staff from the business areas to which the records relate. If possible, they should be sorted into those areas.

3.9 Records which have suffered bad water damaged must be packed in polythene bags and packed into crates. Lists of material removed must be kept, showing the number of the crate in which it has been packed. The crates must then be taken to a collection area for transportation to the allocated deep freeze facility. Freezing records in this way will prevent further damage while they are waiting to receive attention. Other badly damaged records should be set aside for the attention of the designated conservation document salvage service.

3.10 After records have been removed, excess water should be mopped up.

### **4 Restoration of the Disaster Area**

4.1 The disaster area should be restored to normal use as soon as possible. The prime responsibility for this will rest with the facilities management staff.

4.2 Temperature and relative humidity readings should be taken as soon as the disaster area has been cleared.

4.3 De-humidifiers (to reduce relative humidity) and fans (to increase air circulation) should be installed, if necessary.

4.4 Walls, ceilings, floors and shelving should be washed thoroughly with a fungicide (such as sodium ortho-phenyphenol solution in water) to inhibit mould growth.

4.5 Areas can be put back to use when the temperature and relative humidity levels have stabilised at acceptable levels for a period of seven days (see the Records Management Standard: Storage of Semi-Current Records, RMS 3.1, PRO, 2000).

## APPENDICES

1 Location of Disaster Equipment

.....  
2 Plans of Buildings

## ANNEX 2

### **British and International Standards Relevant to Business Recovery**

BS 4783	Storage, transportation and maintenance of media for use in data processing and information storage, 1988-94
BS 5454	Recommendations for the storage and exhibition of archival documents
BS 5588	Fire precautions in the design and construction of buildings, 1983 (amended 1989)
BS 5839	Fire detection and alarm systems in buildings, 1983-95
BS 6266	Code of practice for fire protection for electronic data processing installations, 1992
BS 7083	Computer rooms - guide for accommodation and operating environment of information technical equipment, 1989