MANAGING PUBLIC SECTOR RECORDS

A Training Programme

Emergency Planning for Records and Archives Services

INTERNATIONAL COUNCIL ON ARCHIVES

INTERNATIONAL RECORDS MANAGEMENT TRUST

EMERGENCY PLANNING FOR RECORDS AND ARCHIVES SERVICES

MANAGING PUBLIC SECTOR RECORDS

A STUDY PROGRAMME

General Editor, Michael Roper; Managing Editor, Laura Millar

EMERGENCY PLANNING FOR RECORDS AND ARCHIVES SERVICES

INTERNATIONAL RECORDS MANAGEMENT TRUST

INTERNATIONAL COUNCIL ON ARCHIVES

Emergency Planning for Records and Archives Services

Produced by the International Records Management Trust
12 John Street
London WC1N 2EB
UK

Printed in the United Kingdom.

Inquiries concerning reproduction or rights and requests for additional training materials should be addressed to

International Records Management Trust
12 John Street
London WC1N 2EB
UK
Tel: +44 (0) 20 7831 4101
Fax: +44 (0) 20 7831 7404
E-mail: info@irmt.org
Website: http://www.irmt.org

Version 1/1999

MPSR Project Personnel

Project Director

Anne Thurston has been working to define international solutions for the management of public sector records for nearly three decades. Between 1970 and 1980 she lived in Kenya, initially conducting research and then as an employee of the Kenya National Archives. She joined the staff of the School of Library, Archive and Information Studies at University College London in 1980, where she developed the MA course in Records and Archives Management (International) and a post-graduate research programme. Between 1984 and 1988 she undertook an onsite survey of record-keeping systems in the Commonwealth. This study led to the foundation of the International Records Management Trust to support the development of records management through technical and capacity-building projects and through research and education projects.

General Editor

Michael Roper has had a wide range of experience in the management of records and archives. He served for thirty-three years in the Public Record Office of the United Kingdom, from which he retired as Keeper of Public Records in 1992. He has also taught on the archives courses at University College London and the University of British Columbia, Canada. From 1988 to 1992 he was Secretary General of the International Council on Archives and since 1996 he has been Honorary Secretary of the Association of Commonwealth Archivists and Records Managers (ACARM). He has undertaken consultancy missions and participated in the delivery of training programmes in many countries and has written extensively on all aspects of records and archives management.

Managing Editor

Laura Millar has worked extensively not only as a records and archives management consultant but also in publishing and distance education, as an editor, production manager and instructional designer. She received her MAS degree in archival studies from the University of British Columbia, Canada, in 1984 and her PhD in archival studies from the University of London in 1996. She has developed and taught archival education courses both in Canada and internationally, including at the University of British Columbia, Simon Fraser University and the University of Alberta. She is the author of a number of books and articles on various aspects of archival management, including *A Manual for Small Archives* (1988), *Archival Gold: Managing and Preserving Publishers' Records* (1989) and *A Handbook for Records Management and College Archives in British Columbia* (1989).

Project Steering Group

Additional members of the Project Steering Group include

Association of Records Managers and Administrators (ARMA International):	Hella Jean Bartolo
International Council on Archives:	George MacKenzie
Project Management Consultant:	Tony Williams
University College London:	Elizabeth Shepherd
Video Production Co-ordinator:	Janet Rogers

Educational Advisers

Moi University:	Justus Wamukoya
Universiti Teknologi Mara:	Rusnah Johare
University of Botswana:	Nathan Mnjama
University of Ghana:	Harry Akussah, Pino Akotia
University of New South Wales:	Ann Pederson
University of West Indies:	Victoria Lemieux

Project Managers

Lynn Coleman (1994-6)
Laura Millar (1996-7)
Elizabeth Box (1997-8)
Dawn Routledge (1999)

Production Team

Additional members of the production team include

Jane Cowan
Nicki Hall
Greg Holoboff
Barbara Lange
Jennifer Leijten
Leanne Nash

Donors

The International Records Management Trust would like to acknowledge the support and assistance of the following:

Association of Records Managers and Administrators (ARMA International)
British Council
British High Commission Ghana
British High Commission Kenya
Caribbean Centre for Development Administration (CARICAD)
Canadian International Development Agency (CIDA)
Commonwealth Secretariat
Department for International Development (East Africa)
Department for International Development (UK)
DHL International (UK) Limited
Foreign and Commonwealth Office Human Rights Fund
Hays Information Management
International Council on Archives
Nuffield Foundation
Organisation of American States
Royal Bank of Scotland
United Nations Development Program

Emergency Planning for Records and Archives Services

Principal Author

LAURA MILLAR

For information on Laura Millar, see her biography above as Managing Editor.

Contributor

Laura Simmermon

Reviewers

Roger Craig, Cayman Islands National Archive
Jan Liebaers, Cayman Islands National Archive
Stephen Yorke, National Archives of Australia

Testers

Jamaica Archives and Records Department
National Archives of Sri Lanka

CONTENTS

FIGURES

INTRODUCTION TO *EMERGENCY PLANNING FOR RECORDS AND ARCHIVES SERVICES*

No organisation is totally immune from emergencies or disasters, either from natural causes or human action. Earthquakes, tornadoes, hurricanes, floods and fires take place all around the world. As well, wars and civil strife occur in many countries. Even power failures or electrical faults, leaks or drainage problems, or mishandling and human error can lead to an emergency. Offices, people and records can suffer in an emergency, even an event as seemingly insignificant as a leaking water pipe, a broken humidifier or a shutdown in temperature controls.

In order to protect themselves and their assets, including records and archives, many organisations develop 'emergency plans', which are also called 'disaster plans' or 'business resumption plans'. Such plans are based on the concept that an organisation should identify its assets – including its people, its equipment and supplies, and its critical information sources – and then establish establishes procedures to protect those assets. An emergency plan seeks to protect people and property and ensure that, in the event of an emergency, action is taken immediately to reduce the damage incurred and institute recovery procedures right away.

> ***Emergency plan**:* Policies and procedures developed by an organisation to be used during an emergency or disaster to prevent or minimise damage to an organisation, its people and its resources.

The first priority in all emergency planning is to secure human life and safety. The second priority is to ensure the organisation can resume its operations and protect its resources, includes equipment, supplies, information, records and other assets. The records and archives manager's priority is to protect one particular asset: the organisation's records.

Not all records can be protected equally in an emergency. Rather than simply start moving boxes and, perhaps, end up rescuing supplies but losing valuable documents, it is better to plan what will be receive first priority for protection in the event of an emergency. It is possible to identify those records essential to the organisation's business and ensure those records are protected first. Those records are called 'vital records'.

***Vital records*:** Records considered critical to the ongoing operations of an organisation or the re-establishment of operations after an emergency or disaster. Also known as essential records.

This module outlines the steps involved in establishing and maintaining emergency planning programmes and protecting vital records.

Emergency Planning for Records and Archives Services consists of four lessons:

Lesson 1: Identifying Risks to Records and Archives

Lesson 2: Preparing an Emergency Plan

Lesson 3: Identifying and Protecting Vital Records

Lesson 4: What to Do Next?

AIMS AND OUTCOMES

Aims

This module has four primary aims. These are

1. to outline the methods used to identify threats to an organisation's records and the impact of damage or loss

2. to explain how to develop an emergency plan

3. to outline the steps involved in identifying and protecting vital records

4. to provide sources of additional information on emergency planning and vital records management.

Outcomes

When you have completed this module, you will be able to

1. identify threats to your organisation's records and assess the impact of damage or loss

2. understand how to develop an emergency plan

3. know how to identify and protect vital records

4. know where to look for more information on emergency planning and vital records management.

METHOD OF STUDY AND ASSESSMENT

This module of four lessons should occupy about 40 hours of your time. You should plan to spend about

15 hours on Lesson 1

10 hours on Lesson 2

10 hours on Lesson 3

5 hours on Lesson 4.

This includes time spent doing the reading and considering the study questions.

At the end of each lesson there is a summary of the major points. Sources for additional information are provided in Lesson 4.

Throughout each lesson, activities have been included to help you think about the information provided. Each activity is a 'self-assessed' project; there is no 'right' or 'wrong' answer. Rather, the activity is designed to encourage you to explore the ideas presented and relate them to the environment in which you are studying or working. If you are studying these modules independently and are not part of a records or archives management organisation, you should try to complete the activities with a hypothetical situation if possible. If the activity suggests writing something, you should keep this brief and to the point; this is not a marked or graded exercise and you should only spend as much time on the activity as you feel necessary to understand the information being taught. At the end of each lesson are comments on the activities that will help you assess your work.

Following the summary at the end of each lesson are a number of self-study questions. Note that these self-study questions are designed to help you review the material in this module. They are not intended to be graded or marked exercises. You should complete as many of the questions as you feel will help you to understand the concepts presented. External assessments, such as assignments or exams, will be included separately when this module becomes part of a graded educational programme.

ADDITIONAL RESOURCES

Students working through this module should have access to a information about emergency planning in general, if possible. Does your archival institution have anyone experienced with emergency planning? Does your records office or records centre have close links with anyone in the organisation responsible for emergency planning, so you can discuss records and archives situations with him or her? Whenever possible, it is ideal to draw on real examples, particularly in a module such

as this one, which focuses specifically on the physical protection of records and archives.

Manual

Associated with this module is the MPSR manual *Planning for Emergencies: A Procedures Manual*. This manual defines the procedures involved with developing policies and strategies to prepare for and respond to emergencies. As well as outlining instructions for developing an emergency plan, the manual provides sample forms and specimen documents, to help demonstrate the principles and practices outlined. The manual should be studied closely in relation to this module. Note that the forms and samples included in the manual are not included in this module; cross-reference are provided instead.

Case Studies

The following case studies are useful additions to this module.

Case Study:

9 Roger Craig, Cayman Islands, 'A Disaster Preparedness Plan for the Cayman Islands National Archives'

23 Ann Pederson, Australia, 'Storage/Preservation Case Study: Responding Effectively to a Disaster'

LESSON 1

IDENTIFYING RISKS TO RECORDS AND ARCHIVES

What hazards could endanger an institution's records and archives? How much damage could be done in the event of a disaster? All organisations should identify and assess all possible risks to buildings, facilities and records. They should then consider the possible impact of these dangers on the institution and its holdings.

A 'risk assessment' identifies possible disasters and emergencies that might occur in the region or within the organisation itself. It then considers how damaging these emergencies or disasters might be to the organisation.

Remember, many emergencies cannot be prevented, but their effects can be minimised: an emergency does not have to become a disaster. For example, a leaking pipe may be an emergency, but if the pipe leaks at 4:00 in the morning and no one is there to shut off the water, it can become a disaster.

A risk assessment identifies possible disasters and emergencies.

This lesson examines how to identify risks, how to determine how seriously they could affect the institution and how to minimise danger. These tasks are known as risk assessment and impact analysis. This lesson considers

- identifying risks
- determining the impact of possible emergencies or disasters
- conducting assessments and analyses
- making recommendations and taking actions to reduce risks
- protecting records.

It is important to remember that the first priority in emergency planning is to protect people and ensure their safety. While this lesson focuses on protecting records and archives, it must not be forgotten that information resources are not as important as human lives.

IDENTIFYING RISKS

An organisation can be threatened by hazards ranging from fires to power failures, from earthquakes to actions by disgruntled employees, from computer viruses to political insurrections. Threats may be deliberate or inadvertent, and they may be caused by either human intervention or natural occurrences or disasters. They need to be protected from such dangers. Records also have to be protected against more everyday threats, such as mildew, pests, rodents, mould, light, dust, hazardous chemicals and improper humidity and temperature controls.

Whatever the threat, records need to be protected and plans developed to ensure risks are minimised and recovery actions are taken immediately. A risk can become an emergency if it happens unexpectedly. An emergency can become a disaster if advanced planning has not been done and immediate action is not taken.

Emergency: Any unexpected occurrence requiring immediate action.

Disaster: An unexpected event with seriously destructive consequences.

As mentioned, a leak that is stopped early is an emergency; a leak that leads to flooding throughout the building becomes a disaster. An earthquake of magnitude 2.5 might lead to an emergency; an earthquake of magnitude 6.5 would be likely to lead to a disaster.

An emergency is not a disaster unless its consequences cannot be controlled.

Types of Emergencies

Emergencies and disasters can be classified as natural or human caused. Natural disasters come from natural phenomena, such as earthquakes, hurricanes, typhoons, cyclones, volcanic eruptions, drought or flood. Human disasters include water leakage, explosions, terrorist actions and war. When determining the possible risks to the organisation and its records, it is necessary to identify the possible emergencies that might occur, then assess their likelihood and the potential damage they could bring. Types of risks include

- **natural,** such as earthquake, fire (includes destruction by water or chemicals used in fire fighting/containment), flood (includes broken water mains, mould and mildew), hurricane, tornado, winter storm

- **environmental,** such as an aircraft crash, hazardous material or chemical spills (including acids and their fumes), building collapse, nuclear fallout, radiation, explosion, transportation accident, dust, light, rodents and insects
- **political,** such as civil disturbance, labour dispute, riots, strikes, insurrections
- **incited,** such as arson, bomb threats, theft, sabotage, security leaks, vandalism
- **technology related,** such as a malfunction of hardware and/or software, viruses from damaged or corrupted computer files, electromagnetic interference, power failures and/or fluctuations, theft of computer hardware/software.

Some common dangers are discussed below.

Water and Weather Damage

Damage from leakage, flooding and severe weather can be great. Water damage can include flooding from heavy rains, high tides or overflowing rivers. Water damage can also come from weak building structures, poor water-carrying systems and poor drainage. Even leaky office sinks or malfunctioning air conditioners can lead to water problems. Both types of water damage can harm records and archives not only immediately but also later, if the materials are not dried and mould starts to develop. Flood water that is contaminated by sewage or chemicals may also constitute a health hazard. Other weather damage can include building damage from strong winds, landslides or rockslides.

Fire

Fire is one of the most damaging dangers to records and archives. Fires can be caused by natural occurrences such as earthquakes, or they can be started by power failures, lightning strikes, electrical faults or arson. Fires result in heat and combustion damage as well as smoke and water damage. A great threat in a records centre or archival institution is not the fire itself but, if the fire is suppressed, the water damage caused by the attempts to extinguish the flames.

Earthquakes

Earthquakes are more common or more severe in some parts of the world than others, depending on the location of geological faults. Earthquakes can cause damage to buildings, such as collapsing or tilting of structures, collapse of shelving or storage units, movement of archives or records from storage containers, computer damage and lost data from power losses, water damage from pipe collapse. Earthquakes can also lead to tsunami, or tidal waves; these can lead to water and flood damage or can collapse or seriously damage buildings. Fire is a great hazard in the aftermath of an earthquake, and the water used to extinguish those fires is yet another hazard.

Armed Conflict

A nation's recorded heritage, particularly its archives, may be exposed to great risk in countries or regions facing war or armed conflict. Records may be destroyed or damaged beyond repair. Other dangers include lost communications and power sources, theft, vandalism, sabotage, building damage and fire and water damage.

Armed conflict can be particularly hazardous because archival materials are often a prime target in war, in order to destroy ethnic records and so damage the strength of a particular ethnic group or nation. In spite of war conventions to prevent damage to heritage materials, archives are often a particular target for attack.

For information on protecting records against armed conflict, see Lesson 4, particularly for information about the International Blue Shield.

Power Failures

Many institutions experience occasional disruptions in power. Indeed, records offices, records centres, and archival institutions often experience power failures, and many people do not consider these an emergency. They are often simply a way of life. However, power failures, even for short periods, can have disastrous consequences. Electronic data and computer programmes can be affected; information may be lost or corrupted. Environmental controls may be disabled, leading to fluctuations in temperature and humidity. The loss of lights could endanger people in the institution if they cannot find their way to exits safely and speedily; darkness is also and unwelcome invitation to those wishing to damage or steal property.

Loss of Staff

If people are not available to continue the work of the institution, services may not be provided and, in some situations, this absence of action could become an emergency or even a disaster. In some countries, governments have declared as 'emergency services' such duties as fire protection, police work, hospital workers, air traffic controllers and so on. Strikes or other labour disputes are common reasons people cannot do their jobs, but weather disruptions, floods, or natural disasters can also keep people from work. Records should be kept identifying people who work for the institution, who can step in an emergency and how to contact senior people for guidance. These records should also be protected against loss or damage.

Activity 1

Have you experienced any emergencies or disasters such as those described above? Briefly describe the situation and the damage done to property, records or the local environment. Was there anything that could have been done to limit damage?

Conducting a Risk Assessment

The best way to identify possible risks is to undertake an assessment. What could happen to the institution or in the geographic area in which it is located? How likely is an earthquake? A flood? A power cut?

When conducting risk assessments, records and archives managers should classify potential risks according to the likelihood that they might happen. For example, an earthquake in many Pacific rim countries is 'almost certain'; in the central United States it is 'unlikely.' A chemical spill might be a 'moderate' risk in a city with freight train services or chemical plants nearby; it might be 'rare' in a rural area far from any chemical storage facilities.

> *Risks should be classified according to the likelihood that they will happen.*

The activity below will help you understand the processes involved with determining risks and allow you an opportunity to think of possible hazards for your institution. When actually conducting such an examination, it is useful to consult with the national disaster or emergency preparedness department, as they can offer valuable advice about risks and about emergency planning in general.

Activity 2

For each of the 'risks' below, indicate the likelihood of it happening in your geographic area or within your institution.

Under 'likelihood', use the following terms:

almost certain / likely / moderate / unlikely/ rare

Risk	**Likelihood**
Earthquake	
War or armed conflict	
River or ocean flood	
Leaking pipes/drains	
Chemical spill	
Vandalism or theft	
Power failure	
Computer breakdown	
Strike or labour unrest	
Other (indicate)	

DETERMINING POTENTIAL IMPACT

Once the risk assessment has been done, an impact analysis helps to determine the potential threat brought by the hazards identified. It is important to consider the effect of each possible type of potential emergency or disaster on records and information sources. (Again, an impact analysis can also consider the effect on the institution as a whole and the staff and clients, but for this discussion only records and archives are being examined.)

This part of the risk assessment, often called an 'impact analysis,' helps identify how damaging an emergency or disaster might be for the institution. For example, a war may very well cause damage across a country. A flood may only affect a small part of the country but may have devastating effects. A power cut may affect only part of an organisation and damage may be negligible.

The effect of a hazard on records and archives will also depend on the quality of the facilities and the nature of protective measures in place. An earthquake could be devastating, but records might be better protected if the institution's shelving has been built to earthquake standards. A water leak could cause damage, but if records have been stored off the floor and away from water outlets or pipes, the danger to them diminishes.

Thus an impact analysis not only considers how a hazard might affect the institution but also helps the organisation identify what steps it should take to protect its assets, including records. Can records be moved off the floor if flooding is a concern? Can shelves be strengthened in the event of an earthquake? Can security systems be installed to reduce the chance of theft or vandalism?

When determining the impact of an emergency or disaster, it is necessary to consider both the tangible and intangible consequences that could result from a loss of business operations. Damage to records and property are obvious consequences. But there may be other tangible consequences that might not be considered right away. What about the loss of revenue from lost business? What about an increased quantity of backlogged work owing to disruptions in the business schedule or lack of information sources? The organisation may also find itself unable to meet legal obligations; it may lose customers; or there may be a danger to staff or client health and safety.

Intangible consequences should also be considered. These might include damage to public image or credibility, loss of taxpayer's confidence or political embarrassment. For example, a government archival institution that experiences a theft may not be considered 'safe'. Other agencies in the government may hesitate to transfer their records to the archival institution, which will have to do a lot of public relations work to build back its reputation and credibility.

An impact analysis involves reviewing the risks identified and determining if the potential threat to the institution – in this instance to its records and archives – is extremely serious, very serious, moderately serious or of minimal concern.

Activity 3

For each of the 'risks' below, indicate the potential impact on the records and archives held by your institution.

Under 'potential threat', use the following terms:

extreme/ very high / medium / low / negligible

Risk	**Potential Threat**
Earthquake	_____
War or armed conflict	_____
River or ocean flood	_____
Leaking pipes/drains	_____
Chemical spill	_____
Vandalism or theft	_____
Power failure	_____
Computer breakdown	_____
Strike or labour unrest	_____
Other (indicate)	_____

Emergencies and disasters can have both tangible and intangible consequences.

Once the institution has completed the risk assessment and the impact analysis, it will have a clearer sense of the possible hazards it might face and the possible effect those dangers might have, particularly for records and archives. The risks and their effects can be charted, such as in the matrix shown below. Such a matrix can help show graphically what risks the institution faces and the level of impact.

Preparing a matrix can help identify when the likelihood of risks is high and the consequences severe, allowing staff to outline appropriate responses in the emergency plan.

For example, if staff conducted a risk assessment and impact analysis and identified an earthquake as almost certain to happen, and its impact to be severe, the emergency plan should definitely address in detail the institution's response. Who would be responsible for what actions? What resources will be allocated? Are contingency plans in place? The emergency plan would need to be detailed on this point.

On the other hand, if the risk assessment and impact analysis identified a flood from the local river as unlikely and its impact negligible – perhaps the building is built high on a hill well removed from the river – then the ultimate damage would be trivial and would require no more than regular procedures to handle it. The organisation would not need to developed detailed actions in the emergency plan, but should mention the possibility and indicate in general what would be done and who would be responsible.

What if the organisation identified a computer breakdown as unlikely and the consequences negligible? If the organisation had no computers, the risk would be non-existent. It need not be detailed in an emergency plan. However, if the organisation were to obtain computers, the plan would need to be revised accordingly.

Activity 4

For the risks and possible impact or consequences you identified in the activities earlier, draw them graphically into a matrix like the one shown in Figure 1.

Then, identify two actions you would take to protect records and archives in your institution against the most severe risks you identified in your activities and charted in the matrix document. Explain your reasons.

Consequences					
Likelihood	extreme	very high	medium	low	negligible
almost certain	severe	severe	high	major	significant
likely	severe	high	major	significant	moderate
moderate	high	major	significant	moderate	low
unlikely	major	significant	moderate	low	trivial
rare	significant	moderate	low	trivial	trivial

TERMS USED:

Severe: Necessary responses should be outlined in detail in an emergency plan; at the time of the emergency senior management must participate in all critical decisions

High: Necessary responses should be outlined in detail; at the time of the emergency senior management must be responsible for critical decisions and oversee actions as needed

Major: Necessary responses should be outlined in detail; at the time of the emergency senior management must be involved with or aware of actions required

Significant: Necessary responses should be outlined in detail; senior managers can delegate authority in the emergency plan so that others can carry out required tasks as outlined

Moderate: Necessary responses can be outlined in general terms in the emergency plan and staff can be assigned responsibility to act as required

Low: The organisation's regular procedures should cover any necessary actions, which can be performed by staff as required, and senior management could be notified after the fact

Trivial: The organisation's regular procedures should cover any necessary actions, which can be performed by staff as required, and senior management could be notified as part of regular reporting procedures.

Figure 1: Risk Assessment Matrix

Source: Adapted from *Guidelines for Managing Risk in the Australian Public Service,* MAP/MIAC**,** 1996.

When preparing a risk assessment and impact analysis, it is wise to consider the following issues. (The institution should expand on this list of concerns in order to conduct as comprehensive an analysis as possible.)

- What would happen to the organisation if its operations were disrupted by a disaster or emergency? (Would it keep operating on a limited basis, would it have to shut down completely?)
- How long could the organisation be non-functional before the loss of services started to affect customers and the rest of the organisation? (Can it stay 'closed' for a day, a week, longer?)
- What would be the cost to the organisation if its vital records were lost? (Are there actual financial losses, loss of reputation, loss of business?)
- Which activities are truly vital? (Can the organisation do without payroll services for a week or month if computers are not working?)
- What internal and external factors will affect the continuation of vital business functions by the organisation? (Is the organisation dependent on another agency for light or power? Are the building's security systems adequate against possible vandalism or sabotage?)
- What other organisational activities would be affected if a vital activity were interrupted or vital records lost? (If all payroll records were destroyed, who else in the organisation would be affected?)
- Are there any legal repercussions as a result of a failure to conduct business? (Can people sue for loss of income, physical damage, and so on?)
- How long would it take to reconstruct lost records and how much would it cost? (Is the cost prohibitive or worth the expense?)
- Would any contracts be in danger of operations were interrupted? (Are people presently involved with projects in the organisation and would they not be able to continue in the event or aftermath of an emergency?)
- How much money in accounts receivable would not be collected? (What lost revenue would the institution have to anticipate?)

It is also important to examine the computers and related information technology systems in place. How would they be managed in the event of an emergency?

- What organisational functions depend on computer or other systems to function?
- What is the maximum, allowable downtime (time a computer is not working) for a system that supports critical functions or processes?
- Is the computer application a 'commercial-off-the-shelf' software product or a customised application? Is there any danger that a customised application could be lost and not replaced if computers were damaged or power interrupted?
- Would it be possible to revert to a manual process to complete tasks?
- Does the computer system have built-in recovery capabilities?

REVIEWING THE RISK ASSESSMENT

To ensure the validity of the risk assessment and impact analysis, it is wise to review them both regularly. It is particularly important to review the risk assessment whenever any new functions or processes are implemented by the organisation. Has the institution started a new activity resulting in new records and information sources? Has the archival institution just received an extensive new collection of records, of high value and requiring particular care? It is especially important in organisations or institutions such as national or state governments, where reorganisation and restructuring occurs on a regular basis, to review all potential hazards regularly and ensure steps have been taken to protect against them.

It is also important, when determining risks and their effects, to remember that a record that is important and valuable today may be less valuable tomorrow or in five years. Some records have less ongoing value than others. The steps taken to protect records should focus on those materials of critical importance – the vital records – so that resources are not misspent on records of lesser value.

Because the value of records changes over time, any risk assessment should be updated regularly, ideally yearly, or any time major changes have occurred, and it should be linked directly to the organisation's retention and disposition schedule, which identifies the agency's records and their scheduled life span in the institution.

For more information on scheduling, see Organising and Controlling Current Records *and* Building Appraisal Systems.

Activity 5

Identify three occasions when you should review or redo your institution's risk assessment and impact analysis.

One way to review the threats to the organisation's records and information on a regular basis is to conduct ongoing security and safety checks. The following one-page form can be adapted for use; it will help you identify and document any issues that should be addressed.

Ongoing safety checks can help the organisation identify risks.

Remember too, these inspections should be conducted frequently, and they should be done at various times. For example, it is important to inspect areas at night and on weekends or holidays, not just during office hours. The situation in the area can be

very different when staff are not in the building, and conditions may be more hazardous at night or when the building is not as busy.

Activity 6

Using the form provided below, conduct two safety checks, one in each of two areas of your organisation where records or archives are kept or used. For example, you could assess the archival repository, and you could assess the records centre. Or you could examine two offices in the organisation, each with its own current records registry or storage area.

What three things could be done to improve safety and security in each area? How might you adapt the form to suit your own institution's needs?

Security and Safety Report Form

Date:

Person Reporting:

Problem Location (Building, floor, & room no.)	**Problem information** (Checklist Code No. and description)	**Corrective Action Completed** (Briefly describe type of action)	**Date/ Initial**

Figure 2: Security and Safety Report Form

Reproduced with permission from Ann Pederson.

METHODS OF CONDUCTING ASSESSMENTS

Interviews, questionnaires and discussions with focus groups are the three common methods used to carry out a risk assessment and impact analysis. The method chosen will depend in part on the organisation's resources, its priorities, its size and staff and other factors. Interviewing is the most comprehensive method of conducting a business impact analysis; however, it is time-consuming and would not be practical in all situations. Questionnaires may produce uneven results because not all respondents actually fill out questionnaires completely, and some people may respond inadequately. Meeting with focus groups – small groups of people representing different departments or responsible for different activities within the organisation – can help planners understand specific functional areas, such as a particular department or office. Focus groups usually provide good analytical results without being too time consuming.

Interviews, questionnaires and discussions with focus groups are the three common methods used to carry out a risk assessment and impact analysis.

The information should be matched with the planners' assessment of which business processes are more 'vital'; then the results of the assessment can be analysed to determine just how vital each business function or process is to the organisation. Then the vital functions and processes can be addressed in the vital records programme. It is not practical or cost-effective to address all business functions in the plan; rather, it is best to describe only those necessary to support the organisation in the event of a business disruption or failure.

For more information on issues related to establishing project teams and conducting evaluations, see Strategic Planning for Records and Archives Services.

Activity 7

For your institution, identify three benefits and three drawbacks to each of the methods available for conducting a risk assessment and impact analysis: interviews, questionnaires and meetings with focus groups.

Which method would you choose for your institution, based on the benefits and drawbacks you have identified? Explain your reasoning.

RECOMMENDATIONS FOR ACTION

Once you have completed the risk assessment and impact analysis, the next step is to determine what should be done to protect records and information. Recommendations can be divided into long term (over several years), medium term (over three to five years), short term (within a year) and immediate (within the next few weeks). For example, a risk assessment might have identified water leaks as a probable hazard for the archival institution, because the pipes are aging and starting to crack. The potential threat could be extremely serious because the records are presently stored directly under the water pipes.

Once the risk assessment and impact analysis are completed, the next step is to develop recommendations for action.

The recommendations might be as follows:

- **long term:** seek new storage facilities
- **medium term:** replace pipes throughout
- **short term:** repair pipes in worst condition
- **immediate:** move records away from underneath pipes
  cover tops of shelves with plastic sheeting
  (to allow water to flow off in the event of a leak)

It is possible also to consider actions in terms of priority. It is not useful to box records if they are stored on the floor of a basement that is highly susceptible to leaks: to do so would probably just mean the boxes as well as the records would be damaged by water. Instead, it might be a better priority to move the records out of the basement or find a way to minimise the chance of leaks.

In general, records are best protected when the following protection is in place in the order presented below.

1. The building is located in a safe area.

2. The building is of high quality.

3. Adequate security systems are in place.

4. Adequate warning systems (such as fire or water detectors) are in place.

5. The building, equipment and records are well maintained and well managed.

6. Records are boxed and shelved adequately.

7. Fire suppression systems are in place.

Remember, though, that even if the building's location is not ideal or security systems are not in place, any actions that can be taken to protect are worthwhile. The best short-term solutions do not have to be expensive or complicated. Moving records off the floor, placing plastic sheeting over shelves or moving boxes away from windows or doors can be as effective in an emergency as installing expensive water detectors or drainage systems.

PROTECTING RECORDS AND ARCHIVES

Regardless of the long-term actions required or the level of emergency planning underway, it is possible to take steps to prevent a potential emergency from becoming a disaster. A number of changes can be instituted to protect records, ensuring their safety on a day-to-day basis as well as in the event of an unforeseen circumstance. These measures range from the simple and quick to the expensive and time consuming.

> *Actions can be taken to prevent potential emergencies from becoming disasters.*

Each institution will have to determine the best course of action to take, depending on its resources, needs and potential risks. The common actions involve protecting records from damage caused by water, fire, hazards such as armed conflicts and abuse or mishandling.

For more information on the physical protection and care of records in general, see Preserving Records.

Protection from Water

Water damage can severely hinder the materials in the care of a records office, records centre or archival institution. All buildings will have some sort of water system in them, whether it be heating and cooling systems, washrooms or drainage systems. To reduce the risk of water damage, the following steps can be taken.

- Do not store records or archives directly next to or under water pipes.
- Inspect and repair water systems regularly.
- Ensure water control systems are easily accessible and their location known to all staff so water can be turned off in the event of a leak or flood.

- Make floors waterproof whenever possible, and keep all materials off the floor and on shelves. In particular, ensure that records are kept at a level higher than water could reach in the event of a flood.
- Install drainage direct to the exterior or away from records storage areas, even if this means directing water drainage into other part of the building.
- Install water alarms if possible to detect the presence of water, but do not rely exclusively on alarms and stop inspections.
- Store materials in containers such as boxes whenever possible, to reduce the impact of water damage.
- Take particular care when building construction or repair work is underway that records are protected from accidental water damage.
- If materials are damaged by water, take all necessary steps to dry them and reduce the chance of mould growth.

For more information on mould damage, see Preserving Records.

Activity 8

Inspect a specific records storage area in your institution and indicate if you feel the records or archives in that area are at any danger from water damage. Using the terms used in this lesson, identify if the risk is extreme, very high, medium, low or negligible. Then, name four actions you could take right away to reduce the risk of water damage.

Protection from Fire

Fire is a great risk to records and archives because it is so fast moving and its effects so serious. As mentioned earlier, fire also brings with it the potential for water damage, from the water used to douse the flames.

The risk of fire damage can be reduced by taking a variety of actions, from improving fire detection systems to installing fire suppression systems. Following are general suggestions for reducing the risk of fire.

- Install an automatic fire detection system with detectors in key locations throughout the facility; the system should have smoke and heat detectors and be linked to a central monitoring panel if possible.
- Install manual fire alarms, even if an automatic fire detection system is in place, as a backup in the event of power breakdowns.
- Ensure fire alarms are connected to local fire departments if possible so that alarms are registered immediately.

- Compartmentalise holdings by installing vaults, fire doors, or fire walls to separate areas of the office. For example, records storage areas could be separated from office areas with fire walls, so that records are more secure in the event of a fire.
- As mentioned above, it is very wise to store materials in containers such as boxes whenever possible; if records are in boxes the likelihood that fire will spread from file to file is reduced considerably. Files kept on open shelves will burn much faster because the paper will lift as it burns, exposing the paper underneath and strengthening the flames.
- Remove all unstable or dangerous materials from areas near records. This includes cleaning solutions, chemicals or easily ignited items.
- Check electrical systems regularly to ensure there are no damaged wires or poor circuits.
- During construction or repair work, ensure that records are protected from accidental fires caused by flame- or heat-producing equipment.
- Enforce a 'No Smoking' policy in all areas where records or archives are stored or handled.

Activity 9

Inspect a specific storage area in your institution and indicate if you feel the records or archives in that area are at any danger from fire. Using the terms discussed earlier, identify if the risk is extreme, very high, medium, low or negligible. Next, name four actions you could take right away to reduce the risk of fire.

Fire suppression systems can be installed, if the institution can afford them. There are two types of systems, gas-based and water-based systems. Gas systems can control fires in confined areas but they are not useful in large spaces, since the gas disperses too quickly in a large room to be effective. Water sprinklers can leave water damage, but they are the most efficient fire suppressant and so are considered a reasonable method. In spite of the possible damage from water, it is recommended that most institutions consider water sprinkler systems for large areas.

Fire extinguishers should be installed in the building and checked annually to ensure they work properly.

Portable fire extinquishers should also be installed in the facility, ideally one extinguisher for each 200 square metres of floor space. There should be at least two extinguishers on each floor of a building. Carbon dioxide extinguishers are best for use on electrical fires; water extinguishers can be used on regular fires. Extinguishers

should be checked annually to ensure they are still charged adequately, and records should be kept of each inspection.

Activity 10

Does your institution have fire extinguishers? How many? What type: carbon dioxide, water, or other? Are they inspected regularly or at all? How often?

Security Measures

Security systems are critical for the protection of records and archives. They are particularly important to protect against theft or arson. The organisation should ensure that the following steps are taken, if at all possible.

- Restrict entry in records storage areas to authorised personnel only.
- Ensure all access points to buildings or storage areas are fitted with locks, and ensure the doors are locked and keys only provided to authorised personnel whenever possible.
- Institute a programme for issuing and wearing security passes that clearly identify and distinguish different categories of staff (permanent and temporary) and visitors (contractors' staff, regular users, casual visitors).
- Ensure that all visitors are supervised all the time they are on the premises.
- Install intruder alarms to warn of unauthorised entry.
- Hire a twenty-four hour security service.
- Ensure that all security measures apply not only to visitors but also to staff.

One of the most important security measures that can be taken is simply to ensure all doors and windows are shut when no one is in the building, so that people cannot enter without authorisation.

Activity 11

Inspect a specific storage area in your institution and indicate if you feel the records or archives in that area are at any danger from a breach in security. Using the terms used earlier, identify if the risk is extreme, very high, medium, low or negligible.

Next, name four actions you could take right away to reduce the security risk.

Special precautions should be taken when contractors are working in a building, so that security measures are not breached. Unfortunately, contractors can be the primary cause of disasters and emergencies. For example, they might be using open flames for welding or construction; they may use hazardous chemicals; or they may be moving heavy equipment in and around records and archives.

Contractors should also be monitored for any activities that might damage or harm materials, such as mishandling of water systems, smoking, eating or drinking in high-risk areas or the use of dangerous equipment such as open flame torches or items with heat sources. The use of such equipment should be considered a possible risk to the materials, as torches or open flames can easily ignite papers. Ideally, contractors should be supervised at all times to ensure they do not do anything that might harm records.

For more information on security issues, see Preserving Records.

Protection against Armed Conflict

Organisations in countries or regions at risk for armed conflict, terrorism or other dangers should take particular precautions to protect material. UNESCO and the International Committee of the Blue Shield (ICBS) have developed a range of recommendations and instructions for action.

For more information on UNESCO and ICBS, see Lesson 4.

Among the key actions are the following.

- Prepare lists of vital records (this action is discussed later in this module).
- Establish priorities for the protection of records.
- Copy inventories and store copies in various locations, including off site.
- Make copies of critical records on microform or another medium and store the copies securely in a separate location.
- Evacuate vital records to secure storage if an emergency is imminent.
- Organise cooperative programmes with other institutions in the country to protect records or archives.
- Raise awareness of the importance of records and archives among the military, security forces and police, so that they may take steps to protect records and archives during a conflict.

Activity 12

Is your country or region under threat of any possible armed conflict? If so, what steps has your institution taken to protect its information resources in the event of confrontation?

Improving an Existing Facility

If the measures outlined above are not sufficient or if the institution is able to put resources into improvements, it is possible to upgrade the existing facility in order to improve standards for the storage of records or archives. General improvements might include the following.

- Waterproofing the building to reduce possible flood or water damage.
- Reinforce the structural strength of key areas in the building.
- Construct walls or external barriers to prevent accidents such as vehicles hitting the building.
- Strengthen shelving to stabilise it in the event of earthquakes or similar disasters.
- Repair or recover water and other pipes to prevent leaks.
- Install security bars on windows and doors.

Activity 13

Name three steps you would take to improve the facility for storing records or archives in your institution. Explain the priority in which you would do this work and why.

Constructing a New Building

If the institution's risk assessment has determined that the existing facilities are inadequate, the ideal situation would be to construct a new, purpose-built facility, whether for office space or for semi-current or archival records storage. While building a new facility is very expensive, it is within the realm of possibility for some institutions. However, the success of a new building will come from good planning before it is built.

A new building should be well planned and well designed.

When constructing a new building, the choice of site is extremely important; a good geographical location will help manage risk. When determining a location for a building, the following potential dangers should be avoided:

- natural water or flooding hazards
- soft or fragile earth (if there is a risk of earthquake)
- industrial activities that might pose a risk of fire, pollution or armed conflict (such as strategically important sites)
- aircraft flight paths
- highways or locations where travelling vehicles might cause damage through accidents, pollution or vibrations.

Ideally, sites should be examined by architectural or engineering specialists with knowledge of disaster planning, and the highest possible standards of construction should be applied to new buildings whenever possible.

For more information on facilities management, including such issues as constructing buildings, see Resource Management for Records and Archives Services.

Activity 14

Name three elements you would include in the construction of a new building to ensure it could protect vital records in an emergency. Explain your reasons for choosing those three elements.

SUMMARY

A risk assessment and impact analysis is usually carried out in four stages: identifying records and assets, determining threats, assessing their impact and recommending action. A risk assessment is critical to identifying the specific dangers an institution might face. An impact analysis helps to examine the effect those dangers might have on the institution, particularly its records and information sources.

- **Identifying records and assets** involves determining what to protect by defining the mandate of the organisation and which functions are vital to the continued operation of the organisation, thereby identifying which records support those vital functions and are considered 'vital' records. This step was discussed in Lesson 1.
- **Determining risks** involves determining the types of interruptions, disaster or emergencies an organisation may experience and the likelihood of those threats occurring.
- **Assessing the impact of risks** involves analyzing the impact of the threats on the organisation, its clients and its records and information sources.
- **Recommending action** involves identifying what should be done in the long term, medium term, short term and immediately.

As well, it is possible to take more immediate action to protect records, and this lesson has outlined some options for protecting records against water damage, fire and armed conflict. It has also considered actions that might be taken to improve existing facilities or construct a new building.

STUDY QUESTIONS

1. What types of risks can affect any organisation?

2. What types of risks are specific dangers to your organisation?

3. What is the difference between a disaster and an emergency?

4. What are the steps involved in conducting a risk assessment?

5. What are the steps involved in conducting an impact analysis?

6. Name four questions you should consider when conducting a risk assessment and impact analysis.

7. Name four questions you should consider when specifically examining the risks associated with computerised information technology systems?

8. What methods can be used to gather information for an assessment and analysis. What are the benefits and drawbacks of each method?

9. What environmental conditions can be changed to protect records?

10. When determining the location of a new building, what potential hazards should be considered?

11. What steps can be taken to improve existing facilities?

12. How can the organisation protect itself from water damage?

13. How can the organisation protect itself from fire damage?

14. What key security measures should be in place in the organisation?

ACTIVITIES: COMMENTS

Activity 1

Every part of the world may experience different types of emergencies or disasters. In all instances, however, it is likely that some steps could have been taken to limit the damage experienced. This exercise helps you consider the situation in your own region and the effects of such emergencies on yourself and your own immediate family, friends or colleagues.

Activity 2

All parts of the world will have a greater or lesser likelihood of the risks identified. It is important to be realistic about dangers, without becoming overly concerned about those emergencies that are highly unlikely to occur in your region. This exercise helps you think about those potential disasters that really might occur and give them a higher priority than unlikely events.

Activity 3

The impact of disasters will depend in large part on the current state of your institution. Do you have a good quality storage area? Is your building secure and well constructed? The risks are perhaps uncontrollable but it is possible to assess the threats and then take steps to minimise dangers.

Activity 4

Each institution will select different actions. However, priority should always be given to those risks that are more likely and those that will cause the most damage to the institution and its records and archives.

Activity 5

There are many reasons to review or redo an institution's risk assessment and impact analysis. Consider for example:

- acquisition of a large body of new records
- expansion of or changes to the institution's mandate or responsibilities
- addition of a large quantity of new staff, whose needs should be considered in any vital records plan
- physical reorganisation of buildings, offices, storage areas or staffing areas.

Activity 6

Each institution should find identify safety and security concerns. The value of using a form is that the process ensures complete documentation and the capturing of information in a systematic format. How would you adapt this form to suit your own organisation's needs?

Activity 7

There are benefits to each method. For example, interviews allow for a comprehensive analysis; questionnaires save time, and focus groups allow for detailed discussions with a group of people.

However, there are also drawbacks to each method. Your institution might be too large to allow for interviews of all staff. Questionnaires may not be completed if the institution does not understand the important services provided by the records office, records centre or archival institution. People may be assigned to focus groups but perhaps not prepare for meetings by discussing issues with their colleagues.

The method or methods chosen must suit the particular needs of the institution at the time. Remember, it may be best today to conduct interviews; in two years it may be more appropriate to work with focus groups. It is necessary to consider the best methodology each time you prepare to conduct assessments and analyses.

Activity 8

A number of simple actions can be taken to protect records from water damage, including lifting boxes off the floor, covering shelves with plastic sheeting and not storing records near pipes or water intakes or outlets. The module *Preserving Records* discusses preservation measures in more detail.

Activity 9

A number of simple actions can be taken to protect records from fire damage, including removing flammable items, chemicals or other fire hazards from the storage area, using metal shelving instead of wooden, storing records in boxes, not allowing open flames in the records storage areas and installing fire extinguishers and alarms in key areas. *Preserving Records* discusses preservation measures in more detail.

Activity 10

All institutions should have an adequate number of fire extinguishers. If possible, as your local fire department officials to visit the facility and offer advice on the best type of extinguishers for the needs of the institution. The extinguishers should be checked at least monthly; annual checks are not enough to ensure they are working adequately. The fire department may also advise on the proper placement of extinguishers; they should be located so that they are easy to remove and use.

Activity 11

A number of simple actions can be taken to protect the security of records, including restricting access to storage areas, returning used materials to storage immediately after use, checking the materials for completeness after use and monitoring public and storage areas regularly. *Preserving Records* discusses security measures in detail.

Activity 12

Armed conflict is an unfortunate reality in many parts of the world. It is important to take steps to protect records and information, as well as people, from harm. Lesson 4 offers advice on where to seek information about protecting records in an emergency.

Activity 13

A number of suggestions for improving storage facilities are included throughout this lesson and this module.

Activity 14

Any new facility should be physically secure, should be constructed to reduce the danger of vandalism or theft and should operate with the best environmental and physical controls possible. Measures might include installing vaults, installing metal bars over windows or doors or ensuring the building is strong enough to withstand as much as possible the effects of an earthquake or flood.

LESSON 2

PREPARING AN EMERGENCY PLAN

Once an assessment has been made of the possible risks to an organisation's records and the possible impact of lost or damaged information, the next step in protecting records is to prepare a plan to manage emergency situations. It is useful to repeat the definition provided earlier.

> ***Emergency plan**:* Policies and procedures developed by an organisation to be used during an emergency or disaster to prevent or minimise damage to an organisation, its people and its resources.

Such a plan is usually called an 'emergency plan'; it might also be referred to as an 'emergency management plan', a 'business resumption plan', a 'disaster plan', or a 'disaster management plan'. The term 'emergency plan' is used in this module.

Emergency planning involves three distinct activities:

- readiness: developing a combination of preventive measures to forestall emergencies or disasters, and strategies for dealing with disaster should it occur
- response: adhering to procedures to deal with any emergency situation that arises
- recovery: restoring records and facilities to their usual condition and resuming normal activities.

> *An emergency plan involves readiness, response and recovery.*

An emergency plan will ensure the right measures are taken at the right time in the event of an emergency or disaster. An emergency plan helps the organisation to be ready: that is, to take steps to remove the threat of damage to records and archives by identifying preventive measures that can be taken to improve the stability and security of records. It also helps the organisation to respond: to establish procedures to protect undamaged materials and to stabilise the condition of damaged materials so they may be recovered. It also outlines the work involved with recovery: the tasks of salvaging materials and cleaning and protecting them.

This lesson outlines the steps involved in preparing an emergency plan. These steps include

- preparing an emergency management document
- ensuring adequate supplies are available
- obtaining senior approval for the plan
- establishing emergency response teams
- testing and revising the plan.

When studying this lesson, it will be useful to review the associated manual, *Planning for Emergencies: A Procedures Manual*, at the same time. Sample forms and examples given in the manual are not included in this module; cross-references are included instead.

DEVELOPING AN EMERGENCY PLAN

Ideally, the emergency plan will be a written and widely disseminated document, updated, reproduced and circulated as necessary. Since the document will serve as tool for communicating the disaster prevention and recovery plan to people within the organisation, it must be developed in coordination with all the players involved with handling emergencies within the organisation. Refer back to the discussion in Lesson 1 about who should be involved in preparing an emergency plan.

The plan may be more or less detailed depending upon size of organisation and type of records. The emergency plan should contain the following information:

- introduction and objectives of the plan, including a policy statement from the director of the records and archives institution
- a brief description of possible emergencies or disasters
- a description of preventive measures that can be taken
- emergency procedures, including initial response
- a list of key contacts
- a description of items of special concern that should be rescued or protected
- a description or graphic plan of the building layout, to help people orient themselves
- a list of emergency equipment and supplies that should be available, including information about possible external suppliers
- guidelines for salvage of records after an emergency
- the date the plan has been reviewed, revised and approved (to ensure superseded versions are replaced).

The format of the plan should be easy to read and understand. As well, the format should allow for any updates or additions to be added and for existing pages to be removed easily. Key people should receive a copy of the plan and all updates. A list of these people should be included in the document itself so that everyone knows who has the plan. At least one copy of the plan should be stored off site, such as in the home of the emergency planning coordinator, so that it is accessible during an emergency, even when personnel are not allowed into the building.

> *An emergency plan will be a written, accessible and widely disseminated document.*

Following are descriptions of the key elements in a written emergency plan.

Introduction and Objectives

The introduction explains the nature and purpose of the plan, a detailed list of the contents of the plan, who is responsible for its development, who has approved it and its scope. (For example, does it address emergency issues for the entire government records operation, the records centre or just the archival institution?). Also included should be the terms of reference for the emergency response team, a description of any applicable legislation, policy and management support for the plan as well as a policy statement from the director of the institution outlining the importance of emergency planning.

As well, this part of the plan should outline the specific objectives to be achieved through good emergency management. The organisation should ask itself why it wants to ensure its essential records are protected. Objectives might include the following:

- facilitating effective and efficient methods of preventing damage to or destruction of records
- facilitating the effective and efficient coordination of recovery tasks
- minimising interruptions to normal business operations of the organisation
- limiting the extent of the damage and preventing the escalation of disaster
- establishing alternate means of operation
- providing smooth and rapid restoration of essential services and operations
- preventing injury to the organisation’s personnel
- preventing damage to the organisation’s property or facilities
- minimising any economic impact
- ensuring the continuation of organisation.

The introduction explains the purpose of the plan.

The purpose of outlining objectives is to help ensure that the duties and activities identified are truly relevant to the key records needs of the organisation; framing objectives helps the organisation remain 'on track' with its emergency planning.

See Appendices 1, 2 and 3 in Planning For Emergencies: A Procedures Manual *for a sample terms of reference document, an outline of staff responsibilities, and a policy statement about emergency planning.*

Activity 15

Based on the activities you did in Lesson 1, where you considered possible risks to your institution's records, identify two of the most important objectives for emergency planning for your institution. Explain your reasoning.

Possible Emergencies or Disasters

The next part of the plan is a review the information gathered in the risk assessment and impact analysis, discussed in Lesson 1. The emergency plan should include a brief description of the possible emergencies or disasters that might befall the organisation and the potential impact of those disasters. For example, if an institution is in an earthquake-prone area but is never subjected to tornadoes, then the emphasis in the emergency plan should be on management of earthquake-related tasks, not tornado-related work. Of course, all plans should include discussion of the common and potentially most hazardous threats, such as floods, leaks, power cuts or fire.

The information gathered in the risk assessment and impact analysis will be included in the written plan.

Activity 16

Based on the risk assessment and impact analysis exercises you completed in Lesson 1, indicate in order of priority the top five emergencies that could affect your institution's records and information sources. Explain your reasoning for selecting those emergencies over others and placing them in the order you chose.

Preventive Measures

This section of the plan should include an outline of the steps to be taken to minimise or prevent disruptions in normal business operations. For example, it may be wise to shut off water supplies in the building over weekends or holidays, to reduce the chance of leaking or flooding. It may also be important to turn off all lights when leaving a storage area, or to replace materials on shelves, and not leave them on the floor, when leaving for the night. Such preventive measures will be specific to the needs of the organisation but many of them will reflect practical common sense practices.

Refer back to Lesson 1 for a discussion of preventive measures that can be taken. See also Preserving Records.

Activity 17

Name two preventive measures that could be taken to reduce the negative effects of each of the top five emergencies you identified for the last activity.

Emergency Procedures

The next step in the emergency plan is to outline the emergency procedures to be followed. The very first information provided here should be a description of initial responses to be taken in an emergency, including the list of key emergency personnel and their responsibilities. You should also include an explanation of how to set up a 'command centre' and provide information about any other steps that should be taken immediately after a disruption or emergency. After the initial response, it is important to outline the rest of the emergency procedures to take, in order.

Remember, access to the area may be restricted by fire officials, police or others until it is safe for people to enter. The first priority should always be human safety.

For example, in the event of a fire, the first action would be to sound the alarm; after which the senior staff member identified as responsible in emergencies will take charge, with assistance from other staff as assigned. All people will be evacuated safely from the area, then the senior staff member will ensure emergency calls or contacts are made, to notify external suppliers or assistants and to advise senior management in the organisation. Next, action will be taken to suppress the fire and remove or retrieve materials either before they are damaged or after.

Specific actions taken to deal with materials will depend on the nature and extent of the fire, but options will be outlined in the emergency plan. In general, early actions to be taken will include conducting an assessment of the organisation's facilities, including documenting details necessary for insurance purposes, taking photographs for fire or police reports and so on. Another early action will be to stabilise materials, in order to prevent further deterioration or damage. Stabilisation includes packing records and moving materials to secure storage. Detailed instructions should be provided for those tasks. Interim processing should also be described; that is the specific procedures to undertake during the recovery phase.

This section should of the plan be printed in large type and highlighted, as it will be the section most people turn to first during an emergency. The section may also be copied and made available to all staff as part of their general procedures documents. As well, the procedures could be posted on cardboard or enclosed in plastic and posted on the wall in appropriate parts of the facility, such as near water outlets, fire extinguishers, emergency exits and so on. There could also be an emergency area established, where the procedures are posted for quick reference.

Emergency procedures should also be distributed separately from the plan so everyone has access to this information.

Procedures should be extremely simple and clearly laid out. All staff should be able to follow the instructions given even if they have never seen them before. Remember, the procedures are designed to provide first-response information for staff: what they should do immediately in the event of an emergency. Dealing with the actual records issues, such as moving records or undertaking salvage operations, is a more specialist activity and selected people in the institution will be trained to perform those jobs.

Activity 18

What do you consider should be the first three steps your institution should take in an emergency? Why?

Identification of Key Contacts

The next part of the plan will identify all senior staff and other authorities to be contacted in the event of an emergency. These people will include the director of the organisation, the individual in charge of preservation management, anyone responsible for emergency planning and so on. The chain of command during an emergency should be clearly outlined here, with alternates and out-of-hours contact information identified in the event one individual is not available. This outline of the command structure will help everyone proceed with work by avoiding confusion about who is responsible for what task.

Key people inside and outside the organisation need to be contacted right away in an emergency.

The plan will also identify external suppliers or advisers, such as people who might supply storage space or materials, moving trucks or other equipment. These local resource people can be critical to the success of emergency planning. The organisation should consider establishing reciprocal agreements with other organisations, so that each can help the other in the event of an emergency. It is also advisable to establish relationships with suppliers such as butchers or dairies, or anyone with large walk-in freezers, as it is often necessary during a salvage operation to freeze wet papers until such time as they can be dried out and repaired. It is also very important to establish contacts with national or regional emergency or disaster relief organisations. If possible, representatives of the records or archives institution should join the committees of these external organisations in order to ensure that information needs are considered in the process of national or regional emergency planning.

See Appendix 4 in Planning For Emergencies: A Procedures Manual *for sample forms that may be used to maintain contact lists.*

It is wise to establish formal relationships with such external suppliers. A memorandum of agreement can ensure no confusion during an emergency about who has agreed to do what.

See Appendix 6 in Planning For Emergencies: A Procedures Manual *for a sample memorandum of agreement.*

Activity 19

Name four people (by position title, not personal name) within your organisation who should be notified first in the event of an emergency.

Name four organisations or businesses in your area that could be contacted to share resources such as freezers or emergency supplies. How would you go about contacting them and discussing a possible reciprocal arrangement?

Identification of Items of Special Concern

The plan will also identify areas of the building where materials of particular concern are kept, as well as specific lists of records to be rescued. For example, if the organisation's key financial documents are in the safe in the records vault, this location should be identified so that the records may be removed safely. If areas are locked or otherwise protected by keys, combinations or passwords, it is imperative that enough people have the ability to access the area, so that the records are not at risk if one particular person is not available. For example, staff should not take the only available

set of keys home with them each night. Rather, a master set of keys should be stored in a safe area and then staff may take copies home if necessary.

> *Key documents should be listed separately so they can be identified quickly and rescued in an emergency.*

Within the storage areas themselves, particularly in records centres or archival repositories, it is common to label high-priority records, so that they can be easily identified in an emergency. For example, a large yellow sticker can be placed on the outside of a storage box identifying the fact that essential records are stored within. Then people need only look for the yellow stickers and move the boxes, rather than have to read labels or otherwise identify items for transfer.

Description of the Building Layout

The plan should include floor plans for the building. Of particular importance is information about sources of water and power, so these may be turned off if required. Also important is the location of drainage points. As well, the floor plans should identify emergency storage locations within the building where materials might be transferred in anticipation of salvage and repair.

> *The emergency plan should include a detailed but clearly readable floor plan.*

Specifically, the floor plan should outline the location of

- plumbing, gas or electricity outlets and shutoffs
- heating or ventilation sources
- fire extinguishers and alarms
- emergency equipment
- elevator or escalator operating systems
- emergency lighting
- high-priority materials
- salvage and emergency equipment and supplies
- temporary or emergency storage areas.

List of Emergency Equipment and Supplies

The plan should include a list of key equipment and supplies needed for emergencies. Some equipment is highly specialised and expensive and could be obtained from, or shared with, other departments within the organisation. Other equipment is commonplace but still valuable. Equipment should be held in strategic locations in the building or, better yet, outside of the building. If the facilities are large it may be necessary to house duplicate sets of equipment and supplies in different locations.

Figure 3 is a list of all the ideal equipment and supplies to have on hand. It may not be possible for many institutions to acquire this long list of equipment. However, it is suggested that institutions keep this list on hand and endeavour over time to build up the store of emergency equipment and supplies. Figure 4 is another list of essential equipment and supplies; it may be more realistic for many institutions to obtain the items on this list.

> *Emergency equipment may have to be acquired over a long period; it should be kept secure and used only in emergencies in order to prevent loss.*

Whenever possible, emergency equipment should be used only for emergency purposes. Staff should not take equipment or supplies for everyday use, and items should not be 'borrowed' and not returned. It is wise to take stock regularly of emergency equipment and perhaps even to lock these materials away. If they are locked in a storage cupboard, it is important to know who holds the keys and ensure key staff involved with emergency planning can gain access to the cupboard if necessary.

These equipment lists are repeated in Appendix 5 in Planning For Emergencies: A Procedures Manual.

Ideal Emergency Equipment and Supplies

aprons
axes
batteries for lights or flashlights
bolt cutter
brooms
clean unprinted newsprint
coveralls
crowbar
dehumidifiers
detergents and cleaning solutions
disinfectants
dollies or handcarts
drills
drinkable water
dust masks
dust pans
extension cables
eye protectors
fans, electric
first aid kits and medical supplies
flashlights
food supplies for emergency use
fume masks
generator
glue
hammers
hard hats
jack
kitchen towels
labels (self-adhesive, waterproof)
latex gloves
lumber
mops and buckets
nails, screws, fasteners
note pads
pencils
permanent markers
pipe cutters
plastic bags
plastic crates
plastic sheets
pliers
plywood (for replacing or covering windows)
portable lighting systems
protective boots
protective clothing
pumps, hand and electric for water
radio, battery-operated
rope
rubber boots
saws
scissors
screwdrivers
shovels or scoops
silicone paper
sledgehammer
sleeping bags or blankets
sponges
staplegun and staples
string
surgical gloves
tape (masking or duct tape)
tape measures
thermohygrographs
thermohygrometers
tin snips
utility knives
vacuums, wet/dry
water hoses
water spray bottles
waterproof clothing
wire
wire cutters
wrenches

Figure 3: List of Ideal Emergency Equipment and Supplies

Essential Emergency Equipment and Supplies

batteries for lights or flashlights
brooms
crowbar
dollies or handcarts
drinkable water
eye protectors
first aid kits and medical supplies
flashlights
food supplies for emergency use
hammers
hard hats
mops and buckets
nails, screws, fasteners
note pads
pencils
permanent markers
plastic bags
plastic crates
plastic sheets
pliers
rope
saws
scissors
screwdrivers
shovels or scoops
sponges
tape (masking or duct tape)
utility knives
wrenches

Figure 4: List of Essential Emergency Equipment and Supplies

Activity 20

Review both lists shown here and find out as best as possible how much of the equipment and supplies listed are available to your institution. Are they all in one location or scattered throughout the building?

Write a brief description of where in the building you would put such equipment and how you would go about acquiring necessary items over time. How would you ensure the equipment remained available for emergency use only?

This activity could take some time; only spend as much time as you feel necessary to get a general sense of the equipment available. When an emergency plan is actually developed or revised, it will be necessary to conduct this investigation more thoroughly.

Guidelines for Salvage

The plan will also explain the steps to take during salvage operations. The plan should emphasise the key rules for salvage, which are

- do not open or close wet books
- do not separate single sheets if stuck together
- do not remove book covers
- do not press wet books or papers
- do not wipe off mud or dirt
- do not blot soluble media such as bleeding inks or watercolours
- do not unpack or disturb wet boxes, artwork or photographs.

Salvage guidelines should be included in the plan to help people know how to handle materials in different media.

Each different type of medium should be handled according to appropriate specific salvage guidelines.

See Lesson 4 about where to find information on salvaging records. A description of recommended salvage treatments is also contained in Appendix 7 in Planning For *Emergencies*: A Procedures Manual.

OBTAINING APPROVAL

In order for the disaster management plan to proceed, it is necessary to receive approval and commitment from senior management. This support is usually gained through the process of completing the risk assessment and impact analysis, both of which help explain the need for and benefits of a well-planned system for disaster management. The risk assessment and impact analysis were discussed earlier.

Activity 21

Who in your organisation (by position, not individual person) should be approached to approve the emergency plan? Why did you choose those positions?

ESTABLISHING EMERGENCY RESPONSE TEAMS

Once a plan has been prepared, selected staff will be assigned duties as part of emergency response teams. The number and type of teams chosen will depend upon the size and scope of the organisation. In a large institution several people might join each team; in a small organisation one person may have to take responsibility for many activities. Regardless of how many people are available, the responsibilities of the members of the teams selected should be clearly defined and the members should be comfortable with their roles.

Even if emergency response teams consist of only one person, they still have specific duties and responsibilities.

Following is a list of the types of emergency response teams that could be established, as well as a brief explanation of possible responsibilities.

- **Administrative Team:** responsible for initiating salvage; providing liaison with an insurance company for damage assessment; procuring supplies; estimating time for repair and/or replace operations; establishing a command post; providing clerical and administrative support.
- **Support Services Team:** responsible for procurement of housing and office space for personnel; arranging for transportation of supplies, equipment and personnel during recovery time frame.

- **Backup/Offsite Storage Team:** responsible for establishing control of offsite records; providing human resources; verifying procedures to be followed at backup site.
- **Security Team:** responsible for establishing and maintaining security at backup or alternative site; enforcing security at damaged site.
- **Finance Team:** responsible for establishing and distributing funds during recovery time frame.
- **Public Relations Team:** responsible for dealing with media, staff, customers and public during disruption to normal business operations.
- **Facilities Restoration Team:** responsible for starting restoration; preparing new facility (if required).
- **User Liaison Team:** responsible for coordinating restoration efforts with users; identifying what transactions may be lost or temporarily suspended during recovery time frame.
- **Information Technology Systems Team:** responsible for the installation of software, hardware and applications.
- **Communications Team:** responsible for the installation of communications systems (telephone lines) at recovery facility; examination and restoration of communication systems at damage facility.

In reality, the 'teams' may consist of one person or perhaps two people. In smaller organisations, all the responsibilities identified here may fall to only one or two people. But no matter how few people are involved, or whether people have to combine responsibilities, it is important to recognise the different duties, such as communications or facilities restoration. If each of those duties is assigned formally, everyone will know what he or she is responsible to do.

Staff Awareness and Training

Once teams are identified, staff need to be trained in their respective duties. As well, all staff need to be trained in safety measures; everyone needs to understand the importance of protecting themselves and the assets of the organisation. All employees should be prepared to deal with emergencies in a planned and careful manner, and they must know the necessary procedures well in advance of an emergency.

All staff should be trained in safety measures.

One of the most important aspects of emergency planning is staff training. Team members must understand their roles and functions and they must be comfortable with those tasks. Their response needs to be automatic; there is no time in an emergency for people to wonder what they should be doing. As well, people need to be able to perform their jobs without any one person around, such as a senior manager or the

person who developed the plan. People have to be able to act independently and according to the duties outlined. Such skill requires continuous training and testing.

Knowledge of procedures for personal safety are of the highest priority. Staff should know the location of and use of fire extinguishers; the location of and use of alarms; the need to keep staff calm and reduce panic or disorientation. They should be familiar with the entire emergency management plan and particularly with those areas within their responsibility. Employees should receive training and updates on a regular basis.

TESTING, EVALUATING AND REVISING THE PLAN

In order to ensure that the emergency plan works, it must be tested and then exercised or practised on a regular basis. Testing the plan helps to identify weak areas or procedures that might not otherwise be known until the plan in put into action in a real disaster. Exercises will highlight any deficiencies in the plan that may have occurred as a result of operational or organisational changes. Revisions must be done promptly to ensure that an effective plan is in place at all times.

The plan must be tested, evaluated and revised regularly.

Testing the plan will also determine if the alternative site is useable and compatible. If the agency is depending upon other organisations or vendors to provide an alternative site, testing the plan will help show weakness in those dependencies, as well as determining what details have been overlooked. Testing will also help determine if information technology system back-ups are adequate and easily installed when required.

If possible, the organisation should initiate 'dry-runs' or simulations of various types of business interruptions and emergencies. The plan may be adequate for a major emergency, such as a fire, but may be overly complicated for a short disruption in operations, such as a water leak. Simulations will help smooth out the details. As well, in the event of a real emergency, the plan should be reviewed after to ensure all went according to plan.

The following points should be reviewed during testing or after an actual emergency.

- Were the right people notified in the right order?
- Who took responsibility for starting the emergency response process? Was this the same person designated in the written plan?
- How long did it take to complete initial responses and emergency procedures?

- Were members of emergency teams able to simulate their tasks and respond appropriately?
- How long did it take for the members of the teams to simulate their tasks? Was the time taken too long?
- Was communication between team members and between the various teams effective?
- Was there a duplication of effort between the various teams?
- If emergency storage areas were identified, were they available during the test? If not, why not?

Upon completion of the simulations, an appropriate individual should document the results of the testing and provide recommendations for senior management on how to improve the plan. Senior management will want to know what worked, what needs to be altered and if the plan is viable and relevant to the organisation.

If the plan needs to be revised, this work should be done as soon as possible and the plan tested again to make sure all revisions are suitable. The plan should then be reviewed annually to ensure all information is up to date. If changes take place in the organisation, such as reorganisation of the physical layout of the building, relocation of priority materials or the changes in the importance of records, the plan must be updated as soon as possible. Superseded copies should be destroyed. It is easiest to keep the plan in three-ring binders and replace only those pages requiring updating.

Activity 22

Does your institution have an emergency plan in place? If so, review the contents and identify where what information might be added to incorporate recommended elements outlined in this lesson.

If your institution does not have an emergency plan, outline briefly the steps you would take to begin the process of developing such a plan.

INCIDENT REPORTS

After an actual incident occurs, it is important to examine what happened and take steps to improve the emergency plan as required. The following specific actions should be taken.

- Determine the causes of the emergency or disaster by holding post-mortem meetings.
- Prepare an incident report or similar briefing notes for agency heads on the emergency or disaster.

- Take action to prevent the same emergency happening again, such as by repairing damaged pipes, removing combustible items and so on.
- Modify the emergency plan in light of any possible improvements or changes that have been made or needed to the emergency planning process.
- Ensure that emergency supplies are replenished and make any additions as appropriate.
- Notify the clients and general public of any changes in operations that may result from the emergency.

A sample incident report is in Appendix 8 in Planning for Emergencies: A Procedures Manual.

SUMMARY

This lesson has outlined the steps involved in preparing an emergency plan. These steps include

- preparing a written emergency plan, which includes

  introduction and objectives of the plan

  a brief description of possible emergencies or disasters

  a description of preventive measures that can be taken

  emergency procedures, including initial response

  a list of key contacts

  a description of items of special concern that should be rescued or protected

  a description or graphic plan of the building layout, to help people orient themselves

  a list of emergency equipment and supplies that should be available

  guidelines for salvage of records after an emergency

  the date the plan has been reviewed, revised and approved (to ensure superseded versions are replaced).
- obtaining senior approval for the plan
- establishing emergency response teams
- testing and revising the plan
- preparing an incident report.

STUDY QUESTIONS

1. What is the purpose of an emergency plan?

2. What information should be included in an emergency plan?

3. Explain the purpose of the introduction and objectives section of an emergency plan.

4. What information about the building should be included in the emergency plan?

5. Name ten different types of emergency equipment and supplies and their purposes or uses for emergency management.

6. What are the key rules for salvaging damaged records?

7. Why should the organisation receive approval for and commitment to the plan from senior management? How can this approval be obtained?

8. What types of emergency response teams should be established?

9. Explain the purpose of staff training in emergency management.

10. Explain the purpose of testing the emergency plan.

11. What actions or information should be verified during the test?

12. Why should the plan be reviewed after and actual emergency?

13. Why should an incident report be completed?

ACTIVITIES: COMMENTS

Activity 15

Objectives for emergency planning will differ from institution to institution. At the heart of emergency planning, however, must always be the protection of human life and health. This priority is followed, when dealing with recorded information, with the protection of records and archives.

Activity 16

The emergencies you identified will depend on the assessments you have done. Each institution will be different. Again, the critical issue is protecting people and then ensuring vital records are safe.

Activity 17

Could the institution have stored records more safely? Made copies of critical materials? Covered shelves with sheeting or protective covers to prevent damage?

Activity 18

The first step should always be to ensure people are safe. Then it is important to notify appropriate officials such as the police or fire department. Shutting off water or electricity may also be critical to preventing the spread of danger.

Activity 19

Senior officials in your organisation should be actively involved in any emergency, but it is also important to involve those people 'on the ground' such as technicians or security staff who have day-to-day knowledge of the building, its security systems and its physical layout.

Organisations that might be contacted include butchers, bakers, restaurants and supermarkets. You may also develop a cooperative arrangement with the museum, library or other institutions in your area.

Activity 20

It is wise to try to put all emergency equipment in a central location, one close to an exit and not buried within the centre of a building, where it will be inaccessible in a fire or flood. The storage room should be locked if possible, with specific people holding the keys. It may be advisable to keep this equipment outside of the building itself, if the building is not stable or environmentally safe.

Equipment can be purchased over time, or acquired through donations. It may be valuable to contact government or other suppliers and ask for surplus items to complete your inventory, so that you have as much equipment as possible at limited cost.

Activity 21

The people who approve the plan should be the same people who were involved in overseeing the entire vital records management programme, discussed in Lesson 1.

Senior approval is critical as is continuity and shared understanding of the activities of the organisation.

Activity 22

The steps you identify to begin developing a plan should mirror the suggestions offered in this lesson and the rest of this module.

LESSON 3

IDENTIFYING AND PROTECTING VITAL RECORDS

As mentioned earlier in this module, not all records can necessarily be saved in an emergency. It is important not to misuse resources or energy protecting records of little value when high-value records are at risk. While it is difficult, if not impossible, to place a monetary value on the information contained within the records of an organisation, the information is nonetheless irreplaceable. It is not really possible to 'insure' information against loss, but a vital records programme provides a form of 'insurance' that the information is not lost or damaged.

> ***Vital records programme:*** A systematic approach to identifying, protecting and having available the vital records of an organisation, especially in the aftermath of an emergency or disaster.

It is possible to identify those records that are crucial to an organisation's operations and then outline procedures to protect those records from loss or damage. This protection might be by safe storage or copying, or a combination of both. It is always important to remember that it is the information in records that is important, not necessarily the records themselves. In many instances, copies of records may be as valuable in an emergency as originals. There are situations where only the original will suffice, such as in the case of documents with seals or original signatures. However, even copies of signed documents can be identified as 'true copies', making the copy as authentic as the original in an emergency.

Vital records should be protected from loss or damage.

As well as identifying vital records, it is very useful to identify other assets held by the organisation, including those that affect the work of records or information management. For example, it is important to identify and describe computer equipment, particularly those machines providing a vital service to the organisation; historical documents or records with significant cultural or heritage value; negotiable materials, including cash, stocks, certificates and so on; contracts; radios, televisions, recording devices or other such equipment; attractive items with high monetary value.

Another asset to identify, of course, is the personnel of the organisation. Full information should be kept about all people working in the institution, so that in the event of an emergency they can be identified and protected. It is also useful to maintain information about personnel so that they can be contacted in an emergency.

It is important to protect vital records not only in the office environment but also in the records centre and the archival institution. Regardless of whether the programme relates to current records, semi-current materials or archives, the records and archives institution should play a lead role in developing the programme and ensuring its maintenance. The archival facility, above all other agencies, will have the knowledge and expertise to understand the issues involved with protecting records and the information in them. As well, it is critical to work closely with other agencies within and outside the organisation that may support emergency planning work, including emergency services organisations, police, fire departments and so on.

This lesson discusses the steps involved in identifying and protecting vital records and the means of formalising these tasks as part of a vital records programme, including

- identifying vital records
- listing vital records
- handling and storing vital records
- copying vital records
- protecting vital electronic records.

Activity 23

Think back to the work you did in Lesson 1 and consider two types of natural disasters or emergencies that might happen in your particular geographic area. What kinds of records would you need to protect the rights of citizens or help the organisation continue its business in the event of those types of emergencies or disasters?

IDENTIFYING VITAL RECORDS

Vital records are critical to the ongoing operations of the organisation.

A record is 'vital' if the organisation – or a particular office within the organisation – cannot function without it. The personnel department may consider its employee files vital because all critical data about each employee is recorded in one central location.

On the other hand, the payroll department may hold copies of employee records; these records may not be vital to the payroll department, since they are just reference copies and could be replaced by originals from the personnel department, as long as the personnel records have not been lost or damaged.

Similarly, an archival institution may consider its accessions registers vital, as they are the primary evidence of what has been received by the institution. The records centre may maintain copies of the same registers; because these are not originals they may not be considered 'vital'. But they may in fact be the only security copies, making them even more valuable than the originals.

In general, it can be said that vital records are those records that support the 'vital' functions of the organisation. Without those records, the organisation would have great difficulty continuing its core business.

A functioning vital records management programme must begin with an understanding of what is a vital record to that organisation. It is useful to repeat the definition included at the beginning of this module.

> ***Vital records*:** Records considered critical to the ongoing operations of an organisation or the re-establishment of operations after an emergency or disaster. Also known as essential records.

Who Identifies Vital Records?

Vital records are linked directly to the organisation's business. Therefore, it is necessary to involve senior managers – those people responsible for defining the organisation's business – in the task of identifying vital records. Senior managers should review and confirm the organisation's mandate statement before any vital records are identified. Senior managers should also be involved with reviewing lists of proposed vital records and confirming which records should be protected as vital and which are less crucial to the organisation.

But senior management has a more important role to play than simply defining the organisation's business. A vital records programme will succeed only with strong and visible support from the organisation's senior management. A comprehensive plan requires broad participation and a commitment of resources. Senior management support is paramount to ensure that business resumption planning and a vital records programme can compete for financial and personnel resources.

> *Senior management needs to participate actively in the identification and protection of vital records.*

Senior management should actively support the vital records plan as it is being implemented and then on an ongoing basis, to ensure its general acceptance and,

ultimately, its success. Such support could be in the form of memos to staff on the necessity and importance of the vital records plan, reference to the plan in staff briefings, or by any other means of communication with employees of the institution.

Activity 24

Identify who in your institution (by position title, not personal name) should be involved with the development of a vital records programme. Indicate briefly why you selected those positions.

The group responsible for actually developing a vital records management programme should include both people responsible for records management and people involved with emergency preparedness. The key users of the records should also be involved in the process of identifying vital records, and legal, financial and technical experts may also be consulted. Senior management should be involved from the beginning of the process to ensure that the programme is established in its entirety and is kept up to date. The archival institution should participate throughout the entire process in order to provide both technical and management input into the decision-making process.

Which Records Are Vital?

It is not possible to present a pre-determined list of records and say that 'x type of record is always vital' and 'y type of record is never vital'. Each organisation must determine what constitutes a vital record according to its own requirements, jurisdictions and responsibilities.

Every organisation will identify different records it believes are vital.

The mission statement, legislation and policy documentation of the organisation can provide information that will help define the organisation's vital services and responsibilities. The determination of those vital services and programmes will then determine which records are vital. However, as a general rule, it is possible to say that vital records will have at least one of the following three qualities.

- They will be crucial to the operations of any organisation

  or

- they will be required to protect the rights of individuals or the organisation

  or

- they will be absolutely integral to the reconstruction of the organisation in the event of an interruption or termination of services.

Activity 25

Name three records that you consider absolutely crucial to the operations of your organisation.

Name three types of records essential to protecting the rights of individuals involved with your organisation (such as employees, or the general public, or users).

Name three types of records that you would have to have access to in order to re-establish your organisation's operations in the event of an emergency.

For each type of record you identified, indicate why you thought it was important.

Appraising records in order to determine if they are vital requires a knowledge of the functions of the organisation, the records required to carry out those functions and the life cycle of records. All of those responsible for the information holdings of an organisation should be involved in determining which records are vital. The records manager, librarian, electronic records manager and the emergency planner or security person should work closely with each other and with the users of the information in order to determine which records are vital.

Managing Vital Records

When identifying and protecting vital records, the following diverse issues must be considered.

- In order to determine which records are vital, the roles and responsibilities of the organisation must be clearly defined. Then it is necessary to consider which records are required to ensure the ongoing legal, property and other rights of individuals and corporate bodies. The selection of vital records must also be based on ensuring the continued delivery of the organisation's programmes and services.
- Some vital records keep changing, such as data bases, registration records, and so on. These 'active' records must be kept current. If not, the safeguarded records will be of little use in the event of a disaster or emergency. A procedure for consistently updating vital records must be part of the organisation's records management programme. It is also important to remove records that have been superseded or are no longer applicable, in accordance with a records retention and disposition schedule, in order to keep the vital records programme current and relevant.
- Vital records should be kept in a secure location. Ideally the vital records storage site should be geographically separate from the offices of the organisation, in the

event that the building and surrounding community is destroyed or is inaccessible for a period of time.

- It is necessary to verify that vital records are not already held by another organisation and that any duplicated records are vital to the organisation holding them. If shared or duplicate records are determined to be vital by another organisation, that organisation should identify and properly store and protect those records as part of its own vital records programme. Consider, for example, records of state-national joint activities. Who would be responsible for the official records?
- It is important to consider the technologies used to create records. For instance, if some vital records happen to be in electronic format only, it may be necessary to keep print copies, since the electronic technology needed to use the records may be destroyed in an emergency. Power or utility systems may not be available, for example. Paper is the only record media that is totally technology independent.

Changeable versus Static Records

Some records change regularly. For example, client database records may be updated daily or weekly; accounts payable records may change with every update in payments. If these changeable records are identified as 'vital', they need to be replaced regularly to ensure the most up-to-date version is retained.

> *It is important to identify those vital records that keep changing, to ensure the most current version is kept.*

Static records are those records that do not change or that change minimally. Examples include the original mandate of the organisation presented in an order-in-council, or the annual financial report, which might be approved yearly. Some static records may in fact be archival and may reside either in an archives or in a records storage centre.

If a record is considered 'vital', then it needs to be protected so that the business functions or operations of the organisation can be maintained or resumed as quickly as possible in the event of a disruption in business. To protect static vital records, it may only be necessary to make copies and store these securely. To protect vital records that change regularly, an organisation may have to establish a programme of backups or copies that ensure the most recent version of the record is captured automatically, so the constantly changing information is not lost. It is important to note when copies, backups or revisions are made and to develop a regular process to ensure this work is not left to chance but becomes a part of the ongoing routine of the organisation.

Activity 26

Look again at your list of vital records, identified earlier. Identify whether each type of record you identified in each category changes regularly or remains the same. Explain why the records change or do not change.

LISTING VITAL RECORDS

Once vital records have been identified, they should be listed. Vital records can best be identified in a file classification system or records inventory. They can also be identified in records retention and disposal schedules.

For more information on schedules and inventories, see Organising and Controlling Current Records *and* Managing Archives.

A list of vital records will identify vital records for each division or office of the organisation. The list will also identify the operation or process that the record supports, and it will provide information concerning the procedures needed to protect the records. The records office should maintain a complete set of these lists, and copies of the lists should be kept with the vital records wherever they are stored.

The list should contain the following information:

- the name and file number of the record
- the office responsible for the creation and use of the record
- the purpose of the record
- a description of the record, including information about its purpose and the type of information it contains
- media type(s)
- storage location (both off site and on site)
- an indication of whether the record is classified for security purposes
- the retention period for the record
- steps taken to protect the record (offsite storage, copying and so on).

Vital records should be listed so they can be identified quickly and easily.

Remember, the 'vital' nature of records should be tested periodically. If the information contained in the records is no longer vital, the records should be deleted from the vital records programme. This type of spot-check and testing would help identify any missing or excluded vital records.

Activity 27

Choose three of the vital records you identified in the activity earlier in this lesson. Write a list of these records, including for each record the information provided in the list above.

HANDLING AND STORING VITAL RECORDS

Once vital records have been identified and listed, procedures should be established for handling and storing vital records, so that they are protected under normal circumstances and during hazardous conditions. Records can be stored on site or be transferred to safe storage such as an offsite vault, another office within the organisation with good environmental controls, the records centre or the archival institution

Procedures must be developed, documented and circulated to all divisions responsible for transferring vital records, so that the protection of these records becomes part of the ongoing routine of the organisation. For example, vital records may have to be transferred or copied on a daily, weekly, monthly, bi-annual or annual basis, depending upon the records and the normal operating procedures for the handling of the records in each division.

Procedures should be developed to handle and store vital records so that they are protected.

The procedures developed to handle and store records should clearly indicate the responsibilities of the people who care for the records; the procedures should be tested and modified as required. One person within each division should be made responsible for the transfer of vital records according to the established procedures; he or she should also be responsible for maintaining an accurate and up-to-date list of transferred records. The procedures should also include instructions in the event of an emergency during working hours as well as after working hours.

In order to identify vital records quickly, it may be useful to flag them or otherwise identify the boxes, shelves or bays. It is best to use a marking system that is understood only within the institution; to label records specifically as 'vital' will invite unwanted attention or possible theft or damage.

Onsite Storage

Some essential records may be stored on site in a designated area, such as a special record building, vault or records office. If kept on site, the records should be in a building or storage facility that can handle large volumes of vital records, that is as secure as possible against fire, flood or other hazards. The physical security of the records must be paramount. Records must be kept in a secure environment and, if used during the day, must be returned to safe storage as soon as possible.

Vaults can be used for small volumes of vital records required for ongoing reference; Vaults are secure containers, ideally constructed of fire-proof material that resists flames and heat. Note, though, that fire-proof vaults are not necessarily water tight; therefore, they should be located in an area free of possible water damage, flooding, fire or other hazard. In order to protect all records, no combustible material, chemicals or flammable materials should be permitted within the records office or other storage area.

Activity 28

Does your institution have any vaults? If so, survey one and briefly describe its strengths and weaknesses as a location to store vital records. If your institution does not have any vaults, write a brief description of where you might install one and how you might go about constructing one. What materials would you use? How would you ensure the vault was safe and secure?

Remote Storage

Vital records can also be stored remotely; that is, out of the regular office environment in an offsite storage facility. Remote storage of vital records is usually more economical, efficient, flexible and secure than onsite storage. In some countries, private companies have developed commercial records centres for the storage of vital records. Access to records in remote storage locations should only be gained with proper identification. There are many advantages to using remote storage facilities for protecting vital records, including the following.

- In the event of a disruption in normal operations, it is easier to retrieve vital records because they are all stored in the same location.
- Remote storage facilities are usually designed to store vital records and have the appropriate environmental controls for temperature, humidity, air control and circulation, as well as other detection and monitoring devices when required.
- The staff of this type of storage facility are usually trained in records management.
- This type of storage facility usually has extremely good security and access to the records is restricted to authorised personnel.

When considering whether to use a remote storage site, it is important to consider the following:

- The records should be at a safe distance from the offices of the organisation, but as near as safely possible to allow for a reasonably quick retrieval. At least 10 or more kilometres away from the main facility is considered by many experts to be the minimum distance for remote storage facilities.
- The records should be in a location controlled by the organisation and available for use in the event of an emergency as well as for regular maintenance.
- The location should provide a site where officials of the organisation could establish emergency operations for a short period of time.
- Operating personnel should receive the highest possible security clearances.
- The operating personnel should be able to provide all necessary records management services.
- There should be emergency communication facilities available, in addition to regular communication facilities.
- The facility should be self sustaining, for example, with a generator to provide power, water, humidity control system, air-conditioning facilities to heat and de-humidify the air and an ongoing security system.
- The facility should be as safe and secure as possible with its own emergency plan to protect people and records.
- If essential records are machine-readable, the hardware or machinery required to read those records must be available at the facility.

For more information on the care of current records, see Organising and Controlling Current Records.

Activity 29

Are there any commercial remote records storage organisations in your country or region? If so, try to visit one or enquire about their facilities and services. Compared with the checklist above, what facilities does the facility have and what facilities does it lack?

Developing Reciprocal Relationships

It is not always possible to use a commercial agency for offsite storage; in many countries such businesses do not exist or are not yet well established. However, it is possible to consider other options for offsite storage. A range of reciprocal relationships can be established if the organisation seeks creative solutions to the challenge of protecting vital records. One option to develop reciprocal relationships with other agencies in the country. For example, the archival institution and the museum might agree to store each other's vital records. Or the records centre might establish a liaison with the library. If each is located in a different part of the city, this

arrangement might be very beneficial. If the facilities sit next to one another, the chance of protecting records diminishes; an emergency in one building might easily move to the other. Similarly, a records office might establish a relationship with other records offices around the country, or vital records might be stored in provincial records centres. Universities might exchange materials so that each cares for the other's vital records.

Organisations may develop reciprocal relationships with each other in order to protect each other's vital records.

Activity 30

If there is no commercial organisation in your area, name three options you might consider for developing reciprocal relationships to protect vital records.

COPYING VITAL RECORDS

Copying involves the creation of a second or duplicate copy of a vital record. Ideally, copying should only be done when no more changes are expected to the records. The copy should be stored in a safe place, removed from where the original is kept. This may be in a building or area completely separate from the general records storage area. Alternately, the copy may be used for general reference and the original stored in a safe offsite location. Remember, if a copy is used for reference, it should not be the 'master' copy but a copy of the copy. In other words, the original and one copy should also be protected from use so that one or the other is available in the event of an emergency.

Vital records can be copied, but the master copy should also be protected so that one or the other version is available in an emergency.

Copies do not have to be in the same format as the original record. The duplicate can take the form of a photocopy, carbon copy, electronic tape, floppy disk, microform or optical disk. The method selected should be made on the basis of the needs of the organisation and the equipment and facilities available.

Before copying records, you should ask yourself the following questions.

- Do duplicates already exist? If yes, where and in what form?
- When should duplicates be made? When the record is created, or at a pre-set or scheduled time?

- Where should duplicates be made? If duplication occurs at an offsite storage area, equipment must also be provided at that location. What considerations have been made for access to the duplicates?
- How often should updates be made? A schedule must be maintained and consideration should be given to the fact that the longer the period of time between scheduled duplication, the greater the risk of not having copies of the essential records in the event of a disruption in business or an emergency. A log could be maintained to identify those records that have been altered after copying.
- What are the costs involved with the creating and filing of duplicate copies?
- Does the duplicate copy have the same legal value as the original signed document? Is this a relevant consideration?

If copies of records are kept off site, the probability of having the same records stored in two or more locations are unlikely to be destroyed at the same time. Storage of copies off site does not necessarily provide a consistent procedure for ensuring duplicates of all vital records, unless detailed logs are kept of which records are where, when they have been updated or replaced and if they are still considered vital.

Activity 31

Does your institution have a plan for copying records? If so, are copies or originals stored off site? If not, write a brief explanation of how you would develop a copying programme, what resources you would need, whether you would store originals or copies off site and why and what priorities you would establish for your copying programme.

PROTECTING VITAL ELECTRONIC RECORDS

Many records today are created in an electronic format, and there are several different types of alternative methods for dealing with vital electronic records. The type of information technology system used by the organisation, and its dependence upon that system will determine what type of alternative storage site or facility chosen. If an office only produces word processed documents using computers, it might just consider printing out copies of vital records and not keeping the electronic versions . However, if the organisation creates more complex electronic records, such as payroll or personnel data, it may be important to prepare electronic copies -- back ups -- of the data and store these in a secure location.

The care of electronic records is discussed in more detail in Managing Electronic Records.

Ideally, the best way to protect vital records in an electronic format is to make back up copies on a regular basis and store these copies in locations separate from the original. Regardless of what else the organisation does, it should establish a procedure for copying electronic records regularly and completely.

Ideally, three 'generations' of electronic copies should be kept. For example, if a payroll database is considered vital, it may be copied every week. The institution should keep

- one copy of the most recent data, copied this week
- one copy of the data from last week, now superseded by the most recent copy
- one copy of the data from the week before, superseded by both this week's and last week's.

Each of the copies should be kept separately from each other and separately from the original data. For example, the originals may be kept in the payroll office; one copy might be kept in the records centre, another in the archival repository, and the third in a business some kilometres away, as part of a reciprocal arrangement. Each copy should be replaced as new copies are prepared.

Keeping three generations ensures that some data are always available; even if two of the copies were lost only two week's worth of information would be at risk.

It is important to consider how to access, read and use the electronic data in the event of an emergency. It is not enough to keep a data tape without access to the equipment needed to run it. Does the office storing the data have the hardware and software needed to access the information? Remember that since many organisations are constantly modifying their information technology systems, it may be possible to access data now but in six months the technology may not be available. It is important to review regularly the availability of necessary technologies in order to maintain access to the information.

Activity 32

Does your institution have procedures in place for copying or backing up electronic records? If so, describe the procedures and suggest three steps you might take to improve them.

If not, indicate the first three actions you would take to establish a programme to copy electronic records and store them safely.

Reciprocal Arrangements for Electronic Records Care

Just as reciprocal arrangements can be established to maintain paper records, it is possible to develop reciprocal relationships to care for electronic records. It is

sometimes necessary to enter into commercial agreements; some software or hardware vendors, for example, may provide their corporate facilities as an alternative data storage site to the organisations using their products under contract. Again, compatibility between information technology systems may be an issue, but vendors who engage in this type of contract will usually ensure that they maintain the information technology system required to meet the needs of their clients. This is not the least expensive method, but is a fairly reasonable option. One disadvantage may be that the vendor may not stay in business or may change locations. Also, other organisations may have similar agreements with the same vendor, which may cause difficulties if more than one organisation needs to use the facilities at the same time.

It is possible to establish reciprocal arrangements for the care of electronic records.

In some parts of the world, businesses exist specifically to provide protection or storage for electronic records. They often only require the organisation to pay for the time that it uses the facility. One advantage is that this type of alternative storage arrangement is usually available immediately in the event of an interruption in operations. However, a hazard is that the vendor may not offer ongoing or regular service, disrupting the work of the organisation. It may also be necessary to establish special security measures to protect information held by such agencies, if they do not have adequate security themselves.

Establishing Offsite Storage for Electronic Records

The organisation itself can establish an offsite storage centre for its electronic records and data. However, when storing electronic records off site, it is necessary not only to store the records but also to ensure access to the technologies needed to read and use the records.

For example, an organisation may set aside a facility that is wired for information technology and telecommunications systems but that does not have environmental controls or hardware. Such a facility is sometimes called a 'cold storage site'. In the event of an emergency, the organisation would need to obtain and set up computers and telephones to access its data. It is possible that two or more institutions might share in the establishment of such an offsite storage location, reducing the costs. One major disadvantage to sharing is that all organisations may all require the same site at the same time, thus complicating the use of the facility.

The organisation may also create what is called a 'warm storage site.' This type of alternative site is wired for the information technology and telecommunications systems and contains the appropriate environmental controls. Some or all of the computer hardware peripherals may be on site as well. This option is more expensive than cold site facilities, but again it may be shared by two or more organisations to reduce costs. While this type of facility is good for long-term use, the sharing organisations may require the facility as the same time, thus reducing its availability.

A 'hot storage site' is a complete data centre available on a continuous standby basis. An organisation can move into this type of facility with its own information technology systems and continue operations until its own data centre is rebuilt or restored. The advantages of hot sites are that they are usually very secure and are immediately ready for use. This type of electronic storage site is very expensive. Costs can increase if the organisation chooses to locate this type of storage site outside of the city limits, a wise precaution against the damage of earthquakes, floods or other major disasters.

This most expensive type of electronic storage facility is called a 'redundant' site. This type of site is an exact duplicate of the organisation's information technology or data centre. The complete duplication of equipment and services allows for guaranteed compatibility, availability, security and ease of use. However, this is probably the most expensive option as the organisation has to keep both sites totally compatible and up-to-date.

Finally, it is also possible to protect records by a technique called 'electronic vaulting.' Electronic vaulting involves transferring critical information electronically, using telecommunication systems, to a remote storage facility. This electronic transfer of data allows for the simultaneous update of records at remote storage facilities when normal updates are done. The data in storage remains as current as the data in the office. This is an extremely expensive method of data protection, requiring a high level of technical expertise. The advantages to this method are that operations can be restored on-line within one to two hours and lost data is limited to minutes or seconds. The method also allows for direct access to information that has been transferred and eliminates the need to physically transfer back-up tapes or to load data from one back up tape to another.

The disadvantages of electronic vaulting are the high cost of having a duplicate information technology system that is constantly being updated. Security may also be a factor as equipment and telephone lines shared with other users and may be subject to security breaches.

Storing electronic records off site is a complex matter involving access to appropriate technologies and related resources.

Activity 33

Does your institution have procedures in place for storing electronic records off site? If so, describe the procedures followed and suggest three steps you might take to improve them.

If not, indicate the first three actions you would take to establish a programme to store electronic records off site.

SUMMARY

This lesson has outlined the work involved with identifying and protecting vital records. It has discussed the importance of obtaining senior support for a vital records programme, in order to protect records central to the operations of the organisation. It considered the process of identifying and selecting vital records. It discussed the concept of records that change and records that remain the same, and it has discussed various options for storage of vital records, including onsite and offsite storage, and it has examined the option of copying vital records. It concluded with an examination of the tasks involved with protecting vital electronic records.

STUDY QUESTIONS

1. Define a vital record.

2. What is a vital records programme?

3. Explain why some records are changeable and some are static; give examples of each.

4. Explain the purpose of a vital records programme.

5. Who should be involved in the process of determining vital records and why?

6. What is the role of senior management in vital records planning?

7. Explain the key guidelines that might be used to determine if records are vital or not.

8. Why should the criteria for the selection of vital records be established at the outset of a vital records programme?

9. How must vital records be managed to ensure they are current?

10. What are two recommended methods for protecting vital records? Are some measures more suitable than others for different records formats?

11. Name three issues that should be considered when duplicating vital records.

12. Name three issues that should be considered when storing vital records off site.

13. Describe the advantages and disadvantages of visible marking of vital records or their storage locations. Explain how you would approach making a decision about whether or not to mark vital records or their storage location..

14. What procedures should be followed to transfer vital records to secure storage?

15. What information should a list of vital records contain?

16. What options are available for storage of vital electronic records?

17. Define a cold site, a warm site, and a hot site.

18. What is electronic vaulting?

ACTIVITIES: COMMENTS

Activity 23

Institutions in all parts of the world may experience different types of disasters. Many of the same actions can be taken, however, to protect against those disasters. This module has discussed some of those actions. This activity is designed to help you start thinking about those records that are particularly important -- vital -- to the organisation's activities and that must be protected in the event of a disaster or emergency. The activity helps orient you as you proceed through this lesson.

Activity 24

Senior managers responsible for the civil service, for record keeping and for government operations are key to a vital records programme. It is important to ensure that other senior managers are involved with or support the process of developing a vital records programme, particularly since the programme may require time and resources that must be approved at higher levels of the organisation. It is also important to include as many people as possible who might be affected by an emergency or who can offer technical input into the planning process.

Activity 25

Each organisation will consider different records crucial, for different reasons. It is important, however, to acknowledge that some records are critical and need special protection.

Consider the following types of records; these might be considered crucial to the operations of a national government. In the event of an emergency, the government might have to rebuild buildings or bridges; it might have to move people quickly; and it might have to equip hospitals or emergency centres. The following types of records might be considered vital:

- constitution and similar legal framework documents
- legislation supporting the operations of the government or by which the government was established
- official tax records
- official minutes of parliamentary or senior government meetings
- records vital to public order, safety and public health
- rescue plans and resources
- memoranda of understanding with other organisations and other levels of government
- copies of international agreements
- records of evacuation routes

- records identifying or describing key parts of the city or country, such as details of utility systems; maps of highways and road systems; surveys and plans of public utilities, waterways and bridges; information on facilities such as hospitals, schools or nursing homes
- locations and quantities of stocks of goods or materials necessary to restore basic services to the public.

Activity 26

It is important to be able to distinguish between changing and unchanging records and to take steps to update information on changing vital records regularly so that the organisation's information is always protected.

Activity 27

Each person's list will be different but should include each of the elements listed in this part of the lesson.

Activity 28

Vaults should be fire resistant and safe from flooding or water damage. Ideally they are constructed of a strong metal with metal shelves, not wooden, inside. They will have a door that seals tightly to keep out fire or water; this door should be closed whenever the vault is not in use.

Activity 29

In many countries, such commercial remote records storage organisations do not exist. However, it is useful to bear in mind the requirements of such a facility so that if one is established your organisation can determine if you should enter into an agreement for storage.

Activity 30

As discussed in this lesson, arrangements could be made with businesses, other organisations, other offices within your organisation or with similar agencies in the country. Arrangements should be considered with organisations outside of your city, so that vital records are kept in a distant location and are not at risk in the event of a city-wide emergency or disaster.

Activity 31

Copying of vital records should be done according an established plan, to ensure all critical records are identified and copied. Priorities for copying might focus on those records that are particularly fragile, of great importance to the organisation or at most risk from loss.

Activity 32

Many institutions have no established procedures to back up electronic records. Copies should be kept of all critical electronic records, and information should be recorded about the record and the software and hardware used to produce it. The care of electronic records is discussed in more detail in the module *Managing Electronic Records.*

Activity 33

When storing electronic records off site, it is critical not just to protect the record but to ensure the technology is available to read that record again and be able to use it fully. The care of electronic records is discussed in more detail in the module *Managing Electronic Records.*

LESSON 4

WHAT TO DO NEXT?

Emergency Planning for Records and Archives Services has focused on the development of systems to protect records and information in the event of an emergency or disaster. It has outlined the steps involved in establishing and maintaining emergency planning programmes and protecting vital records. Specifically, it examined

- methods used to identify risks and determine their potential impact on records and archives
- how to develop an emergency plan
- how to identify and protect vital records

Once you understand these principles, concepts and practices, it is necessary to establish priorities for emergency planning and to know where to go to find out more about vital records issues.

ESTABLISHING PRIORITIES FOR ACTION

This module has introduced key activities in emergency planning. But which tasks should you undertake first? Which are high priority and which are low? Each institution will make different decisions based on its physical environment, environmental conditions, needs and short- and long-term plans. However, it is possible to offer some recommendations for action, to help the institution manage its vital records in a planned fashion.

Activity 34

Based on the work done in this module, outline briefly the specific steps you would take to establish an emergency programme for records and archives services. What actions would you do first? What next? Why?

It is suggested that an organisation should consider the steps involved with establishing an emergency programme in the following order.

Priority 1: Identify Threats

Conduct a survey to determine the threats that could affect the work of your institution. Are earthquakes a major concern? Is security a serious problem? Again, document all results of the threat assessment and impact analysis and consult with senior management to discuss the situation and determine actions that can be taken.

Priority 2: Protect Records

Take immediate steps to ensure records are adequately protected. Should some records be stored off site? Should they be copied? Determine immediate actions that can be taken, such as repairing leaky pipes, moving records off the floor, bracing shelves to stabilise them and so on. Establish regular environmental inspections, to check that the physical environment remains stable and records are well stored. If you decide to copy records or store them off site, keep detailed records of decision made, and store copies of those records in a safe place in the event of an emergency.

Priority 3: Identify Vital Records

Conduct a survey to determine which records are vital. Which must be protected at all costs? Document all findings and seek senior management review of the lists developed and recommendations made. Senior administrators may have a different understanding of what is vital and what is not; a collaborative approach to the identification process is critical to obtain perspectives from all key personnel. This analysis might be done as part of an overall survey of the state of records in the institution; it is important not to ignore day-to-day management in the course of developing vital records programmes.

Priority 4: Develop an Emergency Plan

Once you have taken steps to protect records from immediate danger, it is important to establish procedures for long-term protection against possible emergencies or disasters. An emergency plan will document the steps to be taken, assign responsibilities and outline detailed information that might be critical in a disaster, such as the location of emergency equipment or supplies, contact information for key personnel and steps to take to salvage materials.

GETTING HELP

Many institutions, particularly in developing countries, have limited access to resources for emergency aid, especially for the protection of records and archives. However, there are places you can go to get more information or to obtain assistance. Following are names and addresses of agencies that could be contacted for assistance.

> *Some of these agencies are also mentioned in* Preserving Records; *see that module for more information about general preservation-related organisations. Also see the* Additional Resources *document for information on other organisations and associations involved with records and archives management generally.*

International Organisations

International Council on Archives Project Group on the Protection of Archives in the Event of Armed Conflict or Other Disasters (ICA/PDP)
60, rue des Francs-Bourgeois
75003 Paris, France
Tel: +33 0 1 40 27 63 06
Fax: +33 0 1 42 72 20 65
email: 100640@compuserve.com
website: http://www.archives.ca/ICA/

This ICA committee studies and drafts guidelines and directives concerning the protection of archives in the event of armed conflict or other disasters. It works in cooperation with UNESCO and the International Committee of the Blue Cross. It also works to promote the exchange of views and experiences in this area. The ICA is the primary international agency for archival work around the world.

International Committee of the Blue Shield (ICBS)

The International Committee of the Blue Shield was established in 1996 by four non-governmental organisations: the International Council on Archives (ICA), the International Council of Museums (ICOM), the International Council on Monuments and Sites (ICOMOS), and the International Federation of Library Associations and Institutions (IFLA). The International Committee of the Blue Shield aims to advise on the protection of endangered heritage, to facilitate international response to emergencies, to encourage the protection of cultural property, to offer training at the national and regional level to manage and protect against disasters and to consult with other agencies on issues of preservation and protection. As a cooperative programme of several agencies, the ICBS can be reached through agencies such as the International Council on Archives, whose address is listed above.

International Centre for the Study of the Preservation and Restoration of Cultural Property (ICCROM)

Via de San Michele 13
00153 Rome, Italy
Tel: +39 06 585 531
Fax: +39 06 5855 3349
email: iccrom@iccrom.org
website: http://www.iccrom.org

ICCROM is an intergovernmental organisation with ninety member states concerned with conserving all types of heritage, whether movable or immovable. ICCROM serves as a clearinghouse for information and a forum for discussion. It seeks to integrate the conservation of cultural heritage by collecting, studying and disseminating information, coordinating research, offering consultancy assistance, providing training opportunities and promoting awareness of cultural heritage issues.

United Nations Educational. Scientific and Cultural Organization (UNESCO)

7 place de Fontenoy
75700 Paris, France
Tel: +33 1 45 68 10 00

Website http://www.unesco.org/webworld

The Division of the General Information Programme (PGI) publishes RAMP studies on records and archives management issues; some of these studies are available online at the website listed above. The website also contains information about other UNESCO initiatives in information, library and archival issues, including announcements about forthcoming conferences, new activities around the world and information about community and cultural activities in developing countries. In particular, UNESCO has undertaken considerable work on emergency planning.

National or Regional Organisations

Each country will be likely to have its own emergency preparedness department, which could be consulted for more information. In addition, the following national and regional organisations may offer assistance.

European Commission on Preservation and Access (ECPA)

PO Box 19121
1000 GC Amsterdam
The Netherlands
Tel: +31 20 551 08 39
Fax: +31 20 620 49 41
email: ecpa@bureau.knaw.nl
website: http://www.knaw.nl/ecpa

The European Commission on Preservation and Access was established in 1994 to ‘foster, develop and support in Europe collaboration among libraries, archives and

allied organisations, in order to ensure the preservation of the published and documentary record in all formats and to provide enhanced access to the cultural and intellectual heritage.' One of the ECPA's main objectives is to 'collect, record and disseminate specialised information relating to new developments in access and preservation.' The ECPA has an active publications programme and produces catalogues regularly, which can be obtained through the address above.

National Archives and Records Administration (NARA)

8th and Pennsylvania Avenue, NW
Washington, DC
20408 US
Fax: +1 202 208 5248
Website: http://www.nara.gov/

The National Archives and Records Administration is an independent federal agency of the United States government, responsible for preserving the nation's history and managing its federal records. NARA has a wide range of publications available on preservation and emergency planning issues. It also conducts research into preservation, disaster preparedness and storage. It's website includes extensive information about emergency planning; go to www.nara.gov/nara/preserva/

Massachusetts Institute of Technology (MIT), Information Security Office

email: gii@mit.edu
websites: http://www.mit.edu/security/
http://www.disasterplan.com

The Massachusetts Institute of Technology conducts extensive research into and maintains considerable information about disaster planning and recovery. It focuses particularly on the security issues surrounding the protection of electronic data. Its Information Security Office provides a wide range of online publications and information about electronic records and information security. As well, the website www.disasterplan.com includes a 'disaster recovery yellow pages' section with information on commercial and other agencies involved with disaster recover. The website also makes available a complete business contingency (emergency) plan, an earthquake response plan, a tsunami response plan, and a section on 'solutions for natural and man-made disasters.'

Library of Congress Preservation Directorate

110 First Street, SE
Washington, DC
20540, US
Tel: +1 202 426 5213
Email: lcweb@loc.gov
website: http://lcweb.loc.gov/preserv/

The Library of Congress Preservation Directorate has developed a number of products concerning emergency preparedness, including lists of supplies needed in an emergency, information about actions to take after a disaster and steps that can be

taken to prevent emergencies. Much information is available online and publications can be ordered.

National Archives of Australia

PO Box 34
Dickson
Canberra, A.C.T. 2602 Australia
Fax: +61 6 257 7564
Website: http://www.naa.gov.au

The National Archives of Australia offers a number of publications free, including information about various archival issues. The NAA also participates in international activities and makes many of its resources available on its website., including information about emergency planning topics.

Southeastern Library Network (SOLINET)

1438 West Peachtree Street NW
Suite 200
Atlanta, Georgia
30309-2955 US
Tel: +1 404 892 0943
website: http://athena.solinet.net/solinet

SOLINET is a non-for-profit library cooperative providing resource sharing for educational, cultural and economic advancement of the southeastern United States and the Caribbean. Founded in 1973, SOLINET has a membership of over 800 libraries of all types, making it the largest regional library network in the United States. SOLINET's Preservation Services division offers information to institutions to help them improve the physical care of their information resources. The Preservation Services division offers emergency disaster assistance to individuals and institutions, including publications, videos, leaflets and group discounts on supplies. Much information, including entire leaflets on topics such as disaster preparedness and recovery, is available on the website at

http://www.solinet.net/presvtn/disaster/disastsv.htm

Also available on the website are case studies of disaster experiences in different institutions.

Activity 35

Find out if your institution has any information about any of the agencies listed above. Does your organisation receive publications, participate in conferences or meetings or otherwise work with any of these groups?

In your opinion, which groups should your institution consider communicating with first, if any, and what would you expect to achieve by doing so? How would you go about building a productive relationship?

ADDITIONAL RESOURCES

There are many publications available about emergency and vital records planning. Some are more easily obtained than others, and some more up-to-date than others. However, older publications also contain valuable information and may be more easily found in libraries in your particular country or region than very new publications that have not yet circulated around the world. Core publications are identified with an asterisk (*).

> *Core publications are also identified in the* Additional Resources *document; refer to that document for information on more general publications on records and archives management.*

Emergency Planning and Recovery

Anderson, Hazel and John E McIntyre. *Planning Manual for Disaster Control in Scottish Libraries and Related Offices.* Edinburgh, UK: National Library of Scotland, 1985.

Balloffet, Nelly. *Library Disaster Handbook: Planning, Resources, Recovery.* Highland, NY: Southeastern New York Library Resources Council, 1992.

Brooks, Constance. *Disaster Preparedness.* Washington, DC: Association for Research Libraries, 1993.

* Buchanan, Sally A. *Disaster Planning, Preparedness and Recovery for Libraries and Archives, with a Bibliography by Toby Murray: A RAMP Study with Guidelines.* (RAMP Study PGI-88/WS/6). Paris, FR: UNESCO, 1988. Available electronically through the UNESCO website.

Fakhfakh, Moncef. *Emergency Plan for Dealing with Accumulations of Records and Archives in Government Services.* (RAMP Study CII-95/WS/4). Paris, FR: UNESCO, 1995. Available electronically through the UNESCO website.

Fortson, Judith. *Disaster Planning and Recovery: A How-To-Do-It Manual for Librarians and Archivists.* New York, NY: Neal-Schuman, 1992.

International Council on Archives. Committee on Disaster Prevention. *Guidelines on Disaster Prevention and Control in Archives.* Studies/Etudes 11. Paris, FR: International Council on Archives, December 1997.

Iowa Cooperative Preservation Consortium. *Flood Recovery Booklet.* Iowa City, IA: Iowa Cooperative Preservation Consortium, 1994.

Library of Congress. *Emergency Drying Procedures for Water Damaged Collections.* Washington, DC: Library of Congress, n.d.

Library of Congress et al. *A Primer on Disaster Preparedness, Management, and Response: Paper-Based Materials.* Washington, DC: Smithsonian Institution,

National Archives and Records Administration, Library of Congress and National Park Service, 1993.

* Lord, Allyn, Carolyn Reno and Marie Demeroukas. *Steal this Handbook! A Template for Creating a Museum's Emergency Preparedness Plan*. Columbia SC: Southeastern Registrar's Association, 1994.

New York State Archives and Records Administration. "Records Disasters and their Prevention." *In the Field* (September 1995): 1-4.

Seibert, Ann. *Emergency Preparedness for Library of Congress Collections*. Washington, DC: Library of Congress, 1996.

Shepilova, Irina G and Adriene G Thomas. *Main Principles of Fire Protection in Libraries and Archives: A RAMP Study.* (RAMP Study PGI-92/WS/14). Paris, FR: UNESCO, 1992. Available electronically through the UNESCO website.

Waters, Peter. *Procedures for Salvage of Water-damaged Library Materials.* Washington, DC: Library of Congress, 1994.

Walsh, Betty. 'Salvage Operations for Water Damaged Archival Collections: A Second Glance.' *Western Association for Art Conservation Newsletter* 19, 2 (May 1997): 12-23.

Overviews on Vital Records Management Issues

Canadian Conservation Institute. *CCI Notes* (Ottawa: Canadian Conservation Institute, various years).

Canadian Council of Archives. *Basic Conservation of Archival Materials: A Guide*. (Ottawa: Canadian Council of Archives, 1990).

Ritzenthaler, Mary Lynn. *Archives and Manuscripts: Conservation: A Manual on Physical Care and Management* (Chicago, US: Society of American Archivists, 1983). ISBN 0-931828-58-9.

Ritzenthaler , Mary Lynn. *Preserving Archives and Manuscripts*. (Chicago: Society of American Archivists, 1993).

Security Issues

Dunn, F.I. *Security: A Guide for Use in Appraising and Implementing Security Systems and Procedures in Archives Operations, covering Buildings, Staff, the Public, and Repository Management* (London, UK: Society of Archivists, 1994). ISBN 0-902886-47-9.

Thomas, David L. *Study on Control of Security and Storage of Holdings*. (RAMP Study PGI-86/WS/23). Paris, FR: UNESCO, 1986.

Walch, Timothy. *Archives and Manuscripts: Security* (Chicago, USA: Society of American Archivists, 1977). ISBN 0-931828-13-9.

Activity 36

Check your institution's library or resource centre. What books or other resources do you have about emergency planning issues? Are any of the publications listed above available in your institution? If so, examine two or three of them and assess their currency and value to your institution. If not, identify two or three publications you think would be most useful to help develop or expand your preservation library. Devise a plan outlining how you could realistically obtain copies of these.

SUMMARY

This lesson has provided an overview of the entire module, *Emergency Planning for Records and Archives Services.* This lesson has then discussed how to establish priorities for action and suggested that the main priorities for action are often as follows:

- Priority 1: identify threats
- Priority 2: protect records
- Priority 3: identify vital records
- Priority 4: develop an emergency plan.

The lesson then outlined ways to find out more information or get help with emergency management issues. The lesson concluded with a discussion of valuable information resources relevant to emergency planning and vital records management.

STUDY QUESTIONS

- In your own words, explain the reason why the priorities proposed in this lesson are offered in the order they are in.
- Indicate two of the organisations listed in this lesson that you would choose to contact first and explain why.
- Indicate two of the publications listed in this lesson that you would choose to purchase first and explain why.

ACTIVITIES: COMMENTS

Activity 34

Every institution will find itself at a different stage of development in terms of emergency planning. The priorities established will have to take into account the particular needs of that institution, and especially the possible threats to the institution, the country and the region. It is important to identify possible threats so that the institution is aware of the potential dangers it faces. Then it is important to protect records against those threats, and then identify vital records. Finally, it is also important to develop a formalised plan for emergency management, so that all policies and procedures are documented and everyone knows what to do in the event of an emergency.

Activity 35

If resources are limited, it is wise to communicate with international organisations first, as they often obtain and filter information from national or regional associations. Thus valuable information is passed on to your organisation through the international group, which can save resources for all. It is also advisable to focus on general emergency and vital records management information before obtaining specialised publications or information.

Activity 36

As mentioned in relation to the previous activity, it is important to begin with general information and ensure you have a good resource library of introductory and overview publications before developing a more specialised library.