DRJ's Sample Plan

By Web Editor

February 13, 2008

INTRODUCTION

This INTERNET DRP is for the low end type of disaster planning. It is for the people that have a PC or a small network. It also can be used as a check list to run against the product or plan already in use.

This version of the Plan is a result of years of rewriting and fine tuning the original Plan. Sections have been added and existing sections have been expanded. The forms found in some of the sections can be used to capture and recover vital information of your organization. One section contains a comprehensive checklist that is used to alert you to the overall contingency needs for your organization. Some pages have fill-in-the-blanks areas and other pages specify that you need to insert some technical information about your company.

Remember, you can use it with a PC or a small network or use it as a check list to run against the product or plan already in use.

MIS CONTINGENCY PLAN

As your MIS Contingency Plan is developing through its many phases, it will be printed and distributed to applicable people in your organization. After reviewing the document, people generally tend to tile it away with other work-related material. If a major disaster should ever occur, the data center could be totally destroyed along with copies of the MIS Contingency Plan that were kept in desks and file cabinets. If the disaster occurred outside office hours, the key personnel would probably be at home.

To plan for various situations that could occur, copies of the MIS Contingency Plan should be safeguarded both at the office and at the employees' residences. An adequate number of copies should be maintained at the data center and at a minimum, additional copies should be located at the following locations:

MIS director's home
Operations Manager's home
Special Projects Manager's home
Technical Support Manager's home
Data Administration Manager's home
Systems and Programming Manager's home
Disaster Planning Coordinator's home
Other team captains' and alternates' homes
Computer room
Tape library
Offsite storage
Backup recovery site

If you maintain your MIS Contingency Plan on a personal computer using some type of a word processing package, you should back up your Plan after it is entered. After each time it is updated, keep a copy of the diskette stored in a secure location offsite. Having copies of the Plan at various residences may be thought of as unnecessary and redundant since the diskettes are also stored offsite, but, should a disaster ever happen, your

(x) matters
Roberta Witty
Troy McAlpin
Watch this video featuring Gartner Analyst Roberta Witty as she discusses how to improve mass notification.
GARTNER Analyst Roberta Witty discusses how to improve mass notification.
(click here view video)

unnecessary and redundant since the diskettes are also stored offsite, but, should a disaster ever happen, your rime can be better utilized in disaster recovery than in locating a PC, printing multiple sets of the plan, and separating the continuous paper into usable documents for distribution.

MIS CONTINGENCY PLAN DISASTER RECOVERY MANUAL

Modified
by:____
_________/____/_____

Reviewed
by:____
_________/____/_____

Reviewed
by:____
_________/____/_____

Approved
by:____
_________/____/_____

Approved
by:____
_________/____/_____

OBJECTIVES OF THE MIS CONTINGENCY PLAN

Organizations are becoming more dependent on the service and record-keeping of the data processing department. The overall objectives of the MIS Contingency Plan are to protect corporate resources and employees, to safeguard the organization's vital records of which the data center has become the custodian, and to guarantee the continued availability of essential MIS services. The role of this Plan in these objectives is to document the preagreed decisions and to design and implement a sufficient set of procedures for responding to a disaster that involves the data center and its services.

A disaster is defined as the occurrence of any event that causes a significant disruption in MIS capabilities. The central theme of the Plan is to minimize the effect a disaster will have upon on-going operations. This Plan responds to the most severe disaster, the kind that requires moving off site to a backup facility. Occurrences of a less severe nature are controlled at the appropriate management level as a part of the total Plan.

The basic approach, general assumptions, and sequence of events that need to be followed will be stated in the Plan. It will outline specific preparations prior to a disaster and emergency procedures immediately after a disaster. The Plan is your roadmap from disaster to recovery. As you follow it, you may choose at any time to take detours for various management reasons. However after the detour, you get back on the main road to recovery. The Plan

will be distributed to all key personnel, and they will receive periodic updates. The general approach is to make the plan as threat-independent as possible. This means that it should be functional regardless of what type of disaster occurs. In order to limit your loss, it must provide for the logical restoring of all critical systems to a production status within 24 hours after the equipment is operational at either the home location or a backup site. By performing a risk/impact analysis, you can determine your potential dollar loss that will result from a major disaster.

For the recovery process to be effective, we have organized the Plan around the team concept. Each team has specific duties and responsibilities once the decision is made to invoke the disaster recovery mode. The captains of each team and their alternates are key MIS personnel. The Plan contains the phone numbers of the team members and represents a dynamic process that is kept up-to-date through updates, testing, and reviews. As recommendations are completed or as new areas of concern are recognized, the Plan will be updated reflecting the current status.

ASSUMPTIONS OF THE MIS CONTINGENCY PLAN

No matter how many precautions are implemented and to what extent they are enforced, most people in the data processing held agree that there are no completely secure computers. The operations of a data center could be suddenly disrupted by events we have little or no control over, involving people, mechanics, electronics, or natural disasters. It is important that you realize the exposure to your organization chat the loss of your data center would be, and that you take steps to minimize the costs resulting from loss or damage to its resources and capabilities, and the costs to the departments and customers it serves by their losses or a reduction in computer services. The computer room is the heart of a data center. Any threat in or near the computer room can affect the critical flow of information from this nerve center. The location of the disaster could be more important than the amount of damage it causes. A small problem at a critical location could cripple a data center and require it to reestablish operations at a backup facility.

This Plan assumes that a catastrophic event has severely crippled the data center, forcing it to reestablish full operations at a fully equipped backup facility. As soon as hardware can be installed in a cold site, processing will be moved from the backup facility to the less costly cold site. All applications will eventually be processed at the backup location, even those not classified as critical. Concurrent with the backup facility processing is the reconstruction of the original or alternate permanent facility, and the planning for the final move back to this site. Although this Plan follows the assumption of a catastrophic disaster, the Plan can be quickly altered to handle a less severe emergency as determined by management.

Two types of backup facilities are available, a cold site (shell) and a hot backup site. A cold site is an empty computer room normally equipped with raised floor, air-conditioning, electric power, and fire protection that is ready for the installation of computer hardware. The problems in relying only on a cold site for your backup are usually locating and installing the hardware. This generally takes the most time. A hot backup site, on the contrary, is a fully equipped and operational computer center, ready to be used by its members in the event of an emergency. The computer room is normally equipped with up-to-date hardware. The member schedules hands-on resting to process its applications on the backup hardware to ensure the validity of its Plan.

Many commerical hotsites offer many Disaster Recovery Services . It provides a number of scheduled testing periods each year as part of its contracted services agreement. These testing periods help keep the member’s Plan up-to-date by assuring that its applications process correctly at the backup facility.

Many companies subscribe to both a hot backup site and a cold site. If the two backup facilities are adjacent to each other, it will enhance the recovery process. However, it is not necessary that both sites be at the same location. While emergency processing would be started and continued for a short time at the hot backup site, replacement hardware would be configured and delivered to the cold site. When the cold site becomes operational, processing would be switched from the hot backup site to the cold site. As soon as the member’s permanent facility is available, the hardware would be moved from the operational cold site to the member’s own facility.

As part of the initial start-up at the backup site, those systems defined as “critical” batch processing would be run first. Testing would be expanded until total recovery per your Plan is achieved.

By taking advantage of both the hot backup site and the cold site as outlined in the guidelines of the Plan, MIS personnel can restore production operations at their own facility in the shortest possible time following a catastrophic event.

DATA PROCESSING ENVIRONMENT

INSERT HERE A BRIEF DESCRIPTION OF YOUR DATA CENTER. INCLUDE A GENERAL DESCRIPTION OF THE KIND OF PROCESSING AND SUPPORT MAINTAINED AT YOUR MAIN DATA CENTER AND ANY PROCESSING AND SUPPORT AT ANY OF YOUR OUT- SIDE LOCATIONS.

MIS CONTINGENCY PLAN INDEX

SECTION TITLE

1. Emergency Management Team notifies other teams

2. Establish Control Center

3. Begin Disaster Recovery Team operations and Disaster Recovery Logs

4. Timed events
a. 1 to 6 hours after being notified
b. 6 to 12 hours after being notified
c. 12 to 24 hours after being notified
d. 24 hours after being notified

C. Establishment of Full Recovery at Backup Site

1. All planned software, hardware, and resources in place at backup site, and the

applications tested

2. Communications network and other equipment fully operational

3. Disaster Recovery Team checklists

D. Restoration of Facilities and Operations at the Original and/or Alternate Site
II. DISASTER RECOVERY TEAMS

A. MIS Organizational Chart
B. Description and Responsibilities
1. Disaster Planning Coordinator

2. Emergency Management Team

3. Operations Team
a. Computer operations
b. Facility preparation
c. Replacement hardware
d. Cold-site preparation
e. Computer support equipment
f. Supplies

4. Data Entry and Control Team
a. Data input
b. Data control

5. Special Projects Team
a. Transportation to/from backup facilities
b. Training
c. Administrative services

6. Technical Support Team
a. System software
b. Communications network

7. Data Administration Team: Database Restoration and Integrity

8. Systems and Programming Team
a. Application systems restoration and recovery
b. Application programs

9. Insurance Department Team: Insurance and Salvage

10. Internal Audit Department Team: Verification of the Integrity of Restoration Operations

C. Team Pre-planning and On-Going Functional Responsibility
1. Disaster Planning Coordinator

2. Emergency Management Team

3. Operations Team

4. Data Entry and Control Team

5. Special Projects Team

6. Technical Support Team

7. Database Team

8. Systems and Programming Team

3. Insurance Department Team

10. Internal Audit Department Team

III. DATA CENTER REQUIREMENTS

A. Computer Room and Tape Library Layout

B. Power Requirements, Cable Diagrams, and Plug Connectors

C. Air-Conditioning, Fire Protection, and Security

D. Computer Equipment and Vendor by Location and Serial Number
1. Computer room

2. Data entry

3. Other areas: Programming/systems/technical services/offices

E. Teleprocessing: Configuration Information

1. Line flow chart drawing

2. Communication controller (3705)

3. Satellite 64

F. Terminal Configuration Charts

1. Local terminal configuration

2. Remote terminal configuration

IV. SUPPLIERS

A. New and Used Hardware Suppliers

B. Software Suppliers

C. Communications Suppliers

D. Special-Equipment Suppliers

E. Office-Support Equipment Suppliers

F. Computer Custom-Forms Suppliers

V. PRIORITIZE ALL APPLICATIONS

A. Rate All Systems with Their Priorities

B. Assign Responsibility for All Applications

C. Designate Systems Requiring Detailed Recovery Plans

VI. MEDIA PROTECTION

A. Protection and Retention of Vital Records

B. Protecting the Database

1. Database backups

2. Updates

3. Database definitions

4. Software modification source code

C. Standard Backup Procedures

1. Daily processing
2. Weekly processing
3. Monthly processing
4. Annual processing
5. Application cycles
6. Disk volume backups

D. Off-Site Storage
E. System and Program Documentation
F. Data-Entry Backup
G. Microfiche Procedures
H. Personal Computer File Backup
I. Computer Custom Forms

VII. COMPUTER ROOM OPERATION PROCEDURES

A. Power-Up Procedures

I. CONTINGENCY PLAN FOR MAJOR DISASTERS

The cycle from the occurrence of a disaster to the full restoration of normal processing has four phases initial response, preparation for temporary; backup sire operations, backup site fully operational, restoration and return to permanent facility.

A. Detection and Reaction

As soon as an emergency situation happens, the on-site personnel should contact the appropriate emergency

As soon as an emergency situation happens, the on-site personnel should contact the appropriate emergency authorities and then take the necessary steps to minimize property damage and injury to people in the vicinity. Following these procedures, they will then contact the MIS Emergency Man agement Team so that the team can personally make an on-site evaluation of the disaster.

1. Identitying the problem; Notifying the authorities
a. Emergency services

Telephone the following numbers to reach local authorities for emergency situations such as fire, explosion, earthquake, tornado, etc.:

Non-Emergency Numbers
Fire Department (emergency-_____-___) _______________
Police Department (emergency-_____-___) ________________
Paramedics (emergency-_____-___) ________________

b. Environment

If a problem is detected concerning the computer room environment, such as electrical, water damage, excessive heat, cold, or humidity, contact the following authorities:

Office Home
Operations Supervisor ___________ ________- ________________
Operations Manager ___________ ________- ________________

If neither of the above can be contacted, notify:

Office Home
MIS Director ___________ ________- ________________

After contacting one of the above, make the decision as to who should be contacted based on the problem encountered: air-conditioning, water exposure, or electrical.

Office Home
Maintenance Manager ___________ ________- ________________
Maintenance Supervisor ___________ ________- ________________
Maintenance Supervisor ___________ ________- ________________

c. Physical security

If you are aware that an unauthorized person is in a secured area of the computer complex, notify one of the following:

Office Home
Security Guard ___________ ________- ________________
Security Company (continuous service) ___________ ________- ________________
Security Officer ___________ ________- ________________

2. Reducing your exposure

Following the procedures below will help to reduce the organization’s exposure to additional losses because of actions not taken by on-site personnel. These actions are targeted at emergencies concerning air-conditioning, fire, or electrical or water damage.

a. Air-conditioner failure

Normallv a graphic temperature-and-humiditv monitor is located in the computer room and operates 24 hours a dav. The temperature should be checked each morning and periodically if a heat increase is noticed. The watchman must check the temperature on each round he makes. If the computer room has two air-conditioning units, the fans in both units will normally operate at all times to maintain the proper air now. If one unit fails, the second unit can usually carry the load for most processing, but only for a limited amount of time. The failing unit needs to be repaired as soon as possible to take the strain off the only operating unit.

The normal temperature for a computer room is between GS and 76 degrees. If the temperature rises above 76 degrees, take the following precautions:

1. Advise the Operations Supervisor that the temperature is above the normal operating range. He will notify the Maintenance Department for corrective action and then notify the Operations Manager.

2. If the temperature rises above 84 degrees, the hardware vendor must be notified. The Operations Supervisor must decide which noncritical applications may continue to be processed.

If the Operations Manager decides to power down the computer or if the computer powers down by itself because of excessive heat, it should not be powered up until approval has been received from the hardware vendor.

Maintenance Department personnel normally perform maintenance for the air-conditioning units each month. They will clean the fiiters, check the freon, check the belts and hoses, and do normal visual inspections. If any problems occur between scheduled maintenance operations, the Maintenance Department should be notified.

b. Fire alarm procedures

Various fire alarm systems can detect and suppress fires within the first few seconds. They can auto matically close fire doors, control elevators, shut off equipment and circulation fans, and notify the local fire department through 24-hour, central-station monitoring. If automatic controls are inappro priate or nonexistent, local smoke alarms should alert you, and fire extinguishers can be used. Water sprinkler systems are activated depending on the type of controls installed. Some sprinkler svstems are dry systems, controlled by smoke/heat detectors that will open valves allowing water to flow to a whole series of sprinkler heads. Other svstems are wet svstems, with water alwavs in the pipes. In a wet svstem, each sprinkler head is equipped with a link that will melt and fall aside when exposed to high temperatures, activating that particular sprinkler head. The wet system helps to limit water damage to lust those areas where the fire occurs.

Should tire or smoke be detected in the computer room, do the following:

1. Immediately power-down the computer.

2. Take the hand fire extinguisher and attempt to put out the fire. NOTE: A fire extinguisher should be mounted on the wall next to the door of the computer room.

3. If unable to extinguish fire:
-Pull the fire alarm or call the Fire Department at_____--____________________(emergency___________).
-Call the guard at extension____________________.
-Call the Operations Supervisor, who will call the Operations Manager and other office management.
-Ensure that the vault door is closed and locked.
-Take a copy of the MIS Contingencv Plan with you.
-As you exit the computer room, push the emergency power-off button located at the computer room door.

4. If time permits:

-Remove current tapes from computer room to a safe place.
-Cover all hardware with large plastic sheets.
-Remove as many tapes as possible.

5. Notify the MIS Emergency Management Team. c. Eledricalltailure procedures

Most computer rooms have battery-powered emergency lighting. Some also have UPS systems and generators to provide continuous electrical power to the computer room. If no backup power is available, emergency procedures need to be initiated. If your computer room and tape library do not have emergency lighting, we suggest that you provide your operational people with pocket penlights. They should carrv the penlights with them while at work, and, if there is a power failure. your people will be less likelv to have an accident while trving to fnd their wav out of a blackened room. A small penlight is a safer soiution than the open flame of a cigarette lighter.

Should an electrical problem be detected in the computer room, the following steps should be taken:

1. Immediately notify the Operations Supervisor, who will contact the Operations Manager and Maintenance Department.

2. Power-down the computer if this hasn't been done already.

3. The Operations Supervisor will advise IBM or other hardware vendors of electrical failure. He will also advise the Database Administrator and Software Section so they can verify that all files are properly restored. If there is a Help Desk staff that screens calls from users, he will also notify them of the expected time the system will be up.

d. Flood and water damage.

Some managers believe that water will never be a problem because no rivers or streams run near the facilitv. or because the facilitv is located on high ground and the possibility of flooding is remote. This mav be true with regard to rivers and streams, but water damage is not always caused by natural disasters such as foods. Water damage can be caused from a discharge or leak in the sprinkler system, broken pipes, bathroom facilities, the flow of water into the computer room from another area of the building because of fire, etc. The following steps should be followed if there is a water problem from the sprinkler system or other leakage:

1. If a fire is not apparent, but the sprinkler system discharges:

Alternate__________ ________-
____

Captain__________ ________-
____

a. Power down thecomputer. b. Push the Emergency Power Off switch next to the door of the computer room. c. Cover all hardware with plastic covers stored in the computer room. d. Call the security guard text) and tell him that the sprinkler is discharging and no fire is apparent. Have him turn off the sprinkler system and notify the necessary maintenance people. e. Make sure that the vault is secured. f. Contact the Operations Supervisor, who will call the Operations Manager, the Maintenance Department, and the hardware vendor. The hardware vendor must inspect the equipment for water damage before it is powered up again.

2. If the water damage exposure is not caused by the sprinkler system, but has affected the computer hardware:

a. Powerdown the computer. b. Push the Emgrgency Power Off button to stop electric power to the computer rcom. e. Place plastic covers over all equipment if water is coming from above. d. Close and lock the vault door. e. Notify the Operations Supervisor, who will call the Operations Manager and Maintenance Su- pervisor. The Maintenance Department will determine the source of the water and take cor- rective action. f The Operations Supervisor will contact the hardware vendor to have the equipment checked for damage before the equipment is powered up.

3. Evacuation of the facility.

Most organizations have procedures for the orderly evacuation of a building. These procedures include the conditions for determining if evacuation is justified and who is authorized to initiate the evacuation. Evacuation because of various threats to human life such as fire, earthquakes, floods, explosions, and bomb threats may be initiated by anyone, but other threats may require an executive to authorize the evacuation. If your organization is not the only occupant of the building, business interruption for other companies may create certain legal problems if no just cause exists.

Employees should be trained in emergency procedures and should know the evacuation routes from various parts of the building. Drills should be conducted periodically to refresh the memory of long term employees and give instructions to new employees. The drills will inform the employees as to which people are responsible for directing the evacuation and checking that all areas have been properly cleared.

4. Advising the Emerllency Manallement Team of the situation.

As soon as possible after a disaster, notify the Emergency Management Team. It is the responsibility of the Operations Supervisor or Operations Manager to make sure the team is advised of the situation. if the on-site person was unable to contact the operations management, that person will now be responsible for contacting the Emergency Management Team. The team members will be phoned in the following sequence until someone is reached. The person reached will continue to call the remaining team members.

____ ______-- ____________________

____ ______-- ____________________

____ ______-- ____________________

The team will personally visit the site and make an initial determination of the extent of the damage. Based on their assessment, all or part of the MIS Contingency Plan will be initiated. The team will decide:

____ ______-- ____________________

Name	Ext	Home phone

a. If the computer operation can be continued at the site and repairs can be started as soon as possible. b. If the computer operation can be continued or restarted with the assistance of only certain recovery teams. c. If a limited computer operation can be continued at the site and plans started to repair or replace unusable equipment. d. If the computer center is destroyed to the extent that the backup recovery facility must be used and the full MIS Contingency Plan initiated.

The Management Team will decide on its plan of action and then notify senior management. If the action plan requires the assistance of other recovery teams, those teams will be notified.

5. Creating a flow chart for the detection and response

The following flow chart lists the recovery steps in the MIS Contingency Plan for Phase 1: Detection and Response.

MIS Contingency Plan-Detection and Response: Phase 1

Heading Name	Executed by	Action Taken
Detection and Response	Operations personnel	Call Operations Management
	Security guard	Call Emergency Services
Reducing your Exposure	Operations personnel	Follow Emergency Procedures for fire
	Security guard	power, air-conditioning, water damage
Evacuation	All occupants	Leave building
Advising Emergency Management Team	Operations personnel	See list below
	Security guard	

Emergency Management Team: Initial Response

- Coordinate initial response using office procedures to protect life and minimize property damage.

-Assess the damage.

- Determine extent to which MIS Contingency Plan will be utilized.

..Minor Damage—Processing can be restarted in a short time with no special recall of personnel. Anticipated downtime is less than one day. Damage could be to hardware, software, mechanical equipment, electrical equipment, or the facility.
..Major Damage— Selected teams will be called to direct restoration of normal operations at current site. Estimated downtime is two to six days. Major damage to hardware or facility.
..Catastrophe— Damage is extensive. Restoration will take upwards from one week. Computer room or facility could be completely destroyed. All team leaders will be called to begin a total implementation of the MIS Contingency Plan.
— Notify senior management.
— Notify users.
— Prepare regular status reports for senior management.
— Notify users of projected time for becoming operational.

B. Initiation of Backup Site Procedures

1. Emergency Management Team notifies other teams
Following an emergency at the computer center, the operational personnel on site will take the appropriate initial action and then contact a member of the Emergency Management Team starting with the first name on the list (Form 12). When a member is located, that member will contact the remaining members of the Emergency Management Team. The members will meet at or near the disaster to make a firsthand assessment of the damage. They will determine the action to take and will notify senior management. If a determination is made to notify all other teams, the Emergency Management

Team will phone the other teams using a predefined pyramid contact system. A brief message will be dictated over the phone and the called person will write down the message. At the end of the message, the called person will read back the message to verify that all critical information is stated. This same procedure will be used for all calls in the pyramid. It will ensure that all contacts have the same information. Form 12 contains the names of all team members and their phone numbers.

2. Establish Control Center

The first task for the Emergency Management Team is to establish a control center. The location of the control center should be in close proximity to the data center. It can be in another office or another building in your complex. If nothing is available or usable, a nearby hotel/motel affords excellent accommodations. The Control Center should be close to other departments in your organization for maximum communication during this hectic period. The phone number should be made available to all departments and users so that all information can be channeled through the center. If a location is not available in your own facility, the first choice in public facilities is_________________________
____.

An alternate is____.

3. Begin Disaster Recovery Team operations and Disaster Recovery Logs

The captain of each Disaster Recovery Team will document the team's activity by posting it on the Disaster Recovery Log (Form 18). This will be used by the Management Team to prepare status reports for management and will become a historical document for your organization. The Management Team will also use the log to coordinate the concurrent activities of the various teams. The Disaster Recovery Log (Form 18) will be used by all teams.

Disaster Recovery Teams

Form 12

Name	Station	Home Phone
Disaster Planning Coord:		
______	______	_____-- ______
Emergency Management Team:		
______	______	_____-- ______
______	______	_____-- ______
______	______	_____-- ______
Operations Team:		
______	______	_____-- ______
______	______	_____-- ______
______	______	_____-- ______
Data Entry and Control Team:		
______	______	_____-- ______
______	______	_____--

		--

Special Project Team:		
		--
		--
		--

Disaster Recovery Teams

Form 12

Name	Station	Home Phone
Technical Support Team:		
		--
		--
Database Team:		
		--
		--
		--
Systems and Programming Team:		
		--
		--
		--
Senior MIS Management:		
		--
		--
		--
Insurance Department Team:		
		--
Internal Audit Department		

Department Team:		
______________	____________	_____-- _______________

Contingency Plan for Major Disasters

C. Establishment of Full Recovery at backup Site

**1. All planned software, hardware, and resources in place at backup site,
and the applications tested.**

2. Communications network and other equipment fully operational.

Make arrangements with the telephone company and other communications vendors for delivery and installation of temporary equipment. Vendors that specialize in used equipment can deliver their equipment in a very short time. Conduct a complete series of tests to ensure full recovery of the communication network capabilities. Provide for full restoration of service at the original or new alternate facility.

3. Disaster Recovery Team checklists

The checklists below (Form 21) are to be used by each team captain to keep track of the many activities that will be performed simultaneously by his team. The Management Team will collect these checklists

and prepare a detailed report of daily progress. The lists will also be used to coordinate all events from the Control Center.

______________________Company, Inc.
Disaster Recovery Checklist

Form 21
TEAM: MANAGEMENT Date:____/_____/______

Team Captain:____

Alternate:____

Timed Events	• Assigned To	Begin Date ......Time mm//dd/yy hh:mm	Completed Date Time mm/dd/y hh:mm
Coordinate initial response using office procedures to protect life and minimize property damage.			
Assess the damage.			
Notify senior management.			
Make decisions on implementation of Disaster RecoveryPlan.			
Notify team captains and start recall process.			
Give formal notification for request to use backup facilities.			
Arange for emergency funds to cover extra expenses.			
Establish a Control Center at or near original site and coordinate			

Establish a Control Center at or near original site and coordinate the recovery. Use the central telephone number or guard's phone as primary contact.			
Start Disaster Recovery Logs.			
Give senior management scheduled status updates.			
Review corporate policy, department budget, and cost-limit guidelines with other teams.			
Give users scheduled updates on status.			
Produce report on damages.			

______________________Company, Inc.

Disaster Recovery Checklist

Form 21

TEAM: MANAGEMENT (page 2)...... Date:____/_____/______

Team Captain:____

Alternate:____

Timed Events	• Assigned To	Begin Date ......Time mm//dd/yy hh:mm	Completed Date Time mm/dd/y hh:mm
Gather Disaster Recovery Logs from all teams. Produce daily status reports.			
Arrange for any additional professional help..			
Coordinate interviews to fill any vacancies.			
Keep status charts of recovery efforts.			

______________________Company, Inc.

Disaster Recovery Checklist

Form 21

TEAM: OPERATIONS...... Date:____/_____/______

Team Captain:____

Alternate:____

		Begin Date	Completed

Timed Events	• Assigned To	......Time mm//dd/yy hh:mm	Date Time mm/dd/y hh:mm
Asscess damage and the necessary replacement equipment.			
Obtain necessary computer equipment and data-handling equipment from those on the Emergency Vendor Contact list.			
Notify vendor Field Engineering management to review plan for repair of equipment and installation of delivered units.			
Meet with Operations Team members and schedule duties for preparing the backup recovery facilities for any additional equipment.			
For backup cold site (shell), review and ensure availability of required power, hearing, telephone lines, and air-conditioning; work with maintenance personnel to ensure best service from utility companies.			
Obtain needed recovery tapes and documentation for use at backup site.			
Assess status of processing and point of recovery for the entire system and/or individual systems. Develop plan to restart operating schedule.			
Establish a Control Center at or near original site and coordinate the recovery. Use the central telephone number or guard's phone as primary contact.			
List restart plans for high priority systems and notify all users.			
Review list of requirements for supplies.			
Arrange for transportation and/or purchase of replacement supplies.			
Notify vendors of status and give address of backup site.			
As soon as backup site is operational, begin to clean up and restore original site.			
Check on requirements for cables and connectors and other start-up requirements at the original site.			
Schedule testing with maintenance personnel.			
Determine the damage to PC, office equipment, data entry, and other units; then schedule replacements.			

______________________Company, Inc.

Disaster Recovery Checklist

Form 21

TEAM: DATA ENTER AND CONTROL Date:____/_____/______

Team Captain:____

Alternate:____

Timed Events	• Assigned	Begin Date ......Time	Completed Date Time

	To	mm//dd/yy hh:mm	mm/dd/y hh:mm
Determine the starting point for recovery.			
Match the latest backup files that Operations plans to use for restoration with user data for rekeying.			
Obtain original documents to rekey to bring files up to current status.			
Determine when equipment will be available.			
Arrange for setting up temporary office space.			
Notify users of status and inform them on details of restart plan and how to handle input.			
Obtain the backup documents and establish revised schedules in conjunction with users and Operations.			

_____________________Company, Inc.

Disaster Recovery Checklist

Form 21

TEAM: SPECIAL PROJECTS Date:____/_____/______

Team Captain:____

Alternate:____

Timed Events	• Assigned To	Begin Date ......Time mm//dd/yy hh:mm	Completed Date Time mm/dd/y hh:mm
Establish transportation to/from backup facilities; arrange scheduled shuttle.			
Arrange transportation for materials, people, supplies, and equipment.			
Train employees who may be working outside their areas of responsibility.			
Administrative services: serve as a clearinghouse for expediting payments, facilitating the process for all team leaders.			
Establish internal mail delivery between locations.			
Deliver any needed furniture to the backup site.			
Deliver any needed office equipment to the backup site.			
Set up any telephones at the backup site.			

_____________________Company, Inc.

Disaster Recovery Checklist

Form 21

TEAM: TECHNICAL SUPPORT Date:____/_____/______

Team Captain:____

Alternate:____

Timed Events	• **Assigned To**	**Begin Date ......Time mm//dd/yy hh:mm**	**Completed Date Time mm/dd/y hh:mm**
Provide the operating systems as well as other control systems software.			
Restore the system in priorty sequence using bacjup tapes and verfying continuity.			
Work with vendor technical staff as needed.			
Determine damage and requirements to restore communications network.			
Work with telephone company to restore full service and place order as needed for replacement telecommunications facilities.			
Notify and inform users of disruptions in services.			

_______________________Company, Inc.

Disaster Recovery Checklist

Form 21

TEAM: DATABASE Date:____/_____/______

Team Captain:____

Alternate:____

Timed Events	• **Assigned To**	**Begin Date ......Time mm//dd/yy hh:mm**	**Completed Date Time mm/dd/y hh:mm**
Restore the database from backup tapes using recovery documentation.			
Restore intermediate data to ensure current integrity.			
Perform tests and verify these against user listings.			
Ensure continuity by working with users.			

______________________Company, Inc.

Disaster Recovery Checklist

Form 21

TEAM: SYSTEMS AND PROGRAMMING Date:____/_____/______

Team Captain:____

Alternate:____

Timed Events	• Assigned To	Begin Date ......Time mm//dd/yy hh:mm	Completed Date Time mm/dd/y hh:mm
Coordinate with Operations and Data Control to verify proper restart point. Verify application software programs and libraries			
Restore files and ensure continuity of data by testing and comparing results to users' listings.			
Process critical applications.			
Establish full processing schedule.			

.

______________________Company, Inc.

Disaster Recovery Checklist

Form 21

TEAM: INSURANCE DEPARTMENT Date:____/_____/______

Team Captain:____

Alternate:____

Timed Events	• Assigned To	Begin Date ......Time mm//dd/yy hh:mm	Completed Date Time mm/dd/y hh:mm
Review the site and determine the severity of damages.			
Photograph the site if possible.			
Prepare report that details damage and outlines disposition of hardware.			
Contact insurance companies and do follow-up with adjusters.			
Initiate insurance claims.			
Advise other teams of the replacement provisions in the existing insurance policy and the allowance for renting and leasing necessary equipment.			

____________________Company, Inc.
Disaster Recovery Checklist

Form 21

TEAM: INTERNAL AUDIT DEPARTMENT Date:____/_____/______

Team Captain:____

Alternate:____

Timed Events	• Assigned To	Begin Date ......Time mm//dd/yy hh:mm	Completed Date Time mm/dd/y hh:mm
Verify restoration process to ensure integrity and continuity			
Audit financial files to ensure recovery process is complete.			
Monitor file restoration, controls, and security during the recovery period.			

D. Restoration of Facilities and Operations at the Original and/ or Alternate Site

Now that your backup facility is functioning as your data center, it is time to turn your attention to rebuilding your permanent data center. Reconstruction plans should already have been in progress, but now it is time to devote more effort to this area. The full reconstruction is normally a two-step process. The first step is to use a cold site as a replacement of the high-cost, hot, backup site. The permanent replacement hardware that will eventually be used at your permanent facility is ordered and installed at the cold site. Once it is tested and operational, the production processing is moved from the hot backup site to the now-operational cold site. A lot of hotsites also provides both a hot backup site and a cold site. Reconstruction at your permanent facility may not require a totally new building but only repair of the existing facility. Once the permanent facility is ready for use, the hardware at the operational cold site can be moved to the permanent facility.

SECTION TITLE

II. DISASTER RECOVERY TEAMS

A. MIS Organizational Chart
B. Description and Responsibilities
1. Disaster Planning Coordinator
2. Emergency Management Team
3. Operations Team
a. Computer operations

b. Facility preparation

c. Replacement hardware

d. Cold-site preparation

e. Computer support equipment

f. Supplies

4. Data Entry and Control

a. Data input

b. Data control

5. Special Projects Team

a. Transportation to/from backup facilities

b. Training

c. Administrative services

6. Technical Support Team

a. System software

b. Communications network

7. Database Team: Database Restoration and Integrity

8. Systems and Programming Team

a. Application systems restoration and recovery

b. Application programs

9. Insurance Department Team: Insurance and Salvage

10. Internal Audit Department Team: Verification of the Integrity of Restoration Operations

II. DISASTER RECOVERY TEAMS

A. MIS Organizational Chart

Except for the Insurance Department and the Internal Audit Department teams, all of the team members belong to the MIS Department. Therefore, it is important to note the organizational responsibilities and authority the remaining members have. Your organizational chart will identify the normal chain of command.

YOUR MIS ORGANIZATIONAL CHART SHOULD BE PLACED HERE

B. Description and Responsibilities 1. Disaster Planning Coordinator

______________________________has been given the responsibility of Disaster Planning Coordinator and will coordinate the activities stated in this Plan.

As the Plan is being formulated, he will be responsible for accumulating all of the information that needs to be included. Most of the data already exists in the organization but is not in a useful form. As people are assigned their duties, their names, addresses, and phone numbers have to be entered in the various parts of the Plan, As the addresses and phone numbers change, the master copy of the Plan is updated, and, every six months to a year, updates are distributed.

After the original version of the Plan is completed, copies are made and distributed to team captains and their alternates. Copies are also secured at all locations named in the Plan. The copies are to be kept at the employees' homes and not in their desks at the office. If a major disaster occurs, their offices may be destroyed.

All activities in the Plan need to be tested. This not only ensures that the procedures work, but also acts as a training exercise for the various teams. The Coordinator will schedule testing and document the success or failure. He will prepare reports for management and for the Internal Audit Department. When tests fail, he will work with the team captain to resolve the problem and schedule another test.

Numerous seminars and meetings on disaster recovery are available, and the Disaster Planning Co ordinator represents his organization at these meetings. He will stay current with state-of-the-art information and procedures and will present this information to his organization. As hardware, software, and communications are updated at his facility, he will communicate with the hot backup site to ensure that it can adequately support all critical systems.

2. Emergency Management Team

Team Captain: MANAGER SYSTEMS AND PROGRAMMING—
____

Alternate:____

Responsibilities:

—Supervise the initial reaction to the disaster and ensure that organizational property and lives are secured.
— Make an assessment of the damage.
— Determine to what extent the MIS Contingency Plan will be implemented.
— Notify senior management.
— Call team captains and begin the disaster recovery plan.

Team Members:
— Manager of Computer Operations—____

— Database Administrator—____

— Manager of Technical Support—____

— Manager of Special Projects—____

— Disaster Planning Coordinator—____

Disaster Recovery· Functions:

— Set up a Control Center per the instructions of the Plan so that all operations will be channeled through one area.
— Distribute the phone number to all teams and emphasize the use of the phone only for necessary information.
— Notify the backup facility of your intentions to use it.
— Start using the Disaster Recovery Logs for all operations.
— Supply senior management with scheduled updates on status.
— Notify all users of the status of the computer facility.
— Arrange for any additional professional help.
— Coordinate interviews to ~ill any vacancies.

3. Operations Team

Team Captain: MANAGER COMPUTER OPERATIONS—____

Alternate:____

Responsibilities:
— Restore files and operate system at the hot backup site.
— Prepare operations schedule at hot backup site.

— Prepare operations schedule at hot backup site.
— Coordinate activities necessary to restore facility at the existing or new permanent location.

— Order and install computer hardware necessary for normal processing at permanent location.
Team Members:
— Operations Supervisor—____
— Computer Operators—As assigned
— Tape Librarian
Disaster Recovery Functions:

a. Computer operations

— Operate or give assistance to computer operator at hot backup site.
— Obtain backup tapes and restore files at hot backup site.
— Determine restart point for critical systems.
— Test critical systems for production processing.
— Establish an operations schedule at hot backup site.
— Inform users of processing schedule at hot backup site.
—Arrange for shipment of backup supplies to hot backup site.
— Arrange for shipment of off-site tapes to hot backup site.

b. Facility preparation

— Coordinate the repair or construction of the new permanent facility at the original location or new location.

c. Replacement hardware

—Contact hardware vendor to determine if current hardware is repairable. If hardware must be replaced, get proposed time-frame for delivery. If time-frame is not satisfactory, get proposal from used-hardware vendor.
— Check on requirements for cables, connectors, and other start-up requirements.
—Arrange for procuring any other data-handling equipment.
— Schedule testing with maintenance personnel.

d. Cold site preparation

— Review cold-site facility to ensure that the environment can support the hardware that will be temporarily operating there.
— Provide for adequate power, cables, and connectors.
— Provide for communications requirements.
— Provide for security guards and limited access to computer room.
— Provide for off-site storage.

e. Computer support equipment.

— Determine the need for other support equipment: PC, data-entry office equipment, paper-handling equipment. Order all required equipment.

f. Supplies.

— Review list of requirements.
— Contact vendors on Emergency Vendor list.
—Arrange for shipment of existing supplies or purchase of replacement supplies.
— Notify remaining vendors of disaster and give shipping address of backup site.

4. Data Entry and Control Team

Team Captain: MANAGER I/O CONTROL

Team Captain: MANAGER I/O CONTROL____

Alternate:____

Responsibilities
: — Restore the Data Entry and I/O Control operations at the backup facility or at an alternate site. Team Members: — Data Entry Supervisor—____

— I/O Control Supervisor—____

— Data Entry Personnel—As assigned
— I/O Control Personnel—As assigned

a. Data input

—Work with Operations to determine the starting point for recovery. Match the latest backup files that Operations will use to restore, with the data from the users. Obtain original documents needed to rekey to bring files up to current status.
— Determine when equipment will be available for keying, or make arrangements with service bureaus or other outside services for keying.
b. Data control

— Notify users of the disaster and advise them of the temporary procedures for handling input and output.
— Arrange for temporary office space either at backup facility or somewhere close to original facility.
— Obtain the backup documents and establish revised schedules in conjunction with users and Operations.

5. Special Projects Team

Team Captain: MANAGER SPECIAL PROJECTS—____

Alternate:____

Responsibilities:

— Provide transportation for people, supplies, and equipment between sites.
— Provide administrative and office support for the recovery activity.
Team Members
: — Special Projects personnel
Disaster Recovery Functions:
a. Transportation to/from backup facilities
— Provide for transportation to and from backup facility. Set up a shuttle service between the airport and the backup site.
—Arrange for shipments of material, supplies, and computer equipment.
b. Training
— Provide for training of employees who may be assigned duties other than their normal duties.
c. Administrative services
— Establish an interoffice mail service between locations.
— Provide all necessary administrative services such as the payment of bills, processing of the payroll, handling of employee insurance claims, issuing of critical invoices.
— Arrange hotel accommodations for personnel stationed at the backup site.
— Provide for additional office facilities, including furniture, phones, and office equipment.
6. Technical Support Team

Team Captain: MANAGER OF TECHNICAL SUPPORT—____

Alternate:____

Responsibilities:
— Install operating system software at the backup site allowing the minimum required operations and communications to be restored.
Team Members:
— System Programmers
Disaster Recovery Functions:
a. System software
— Supply the required operating system as well as other control systems.
— Restore the systems in priority sequence using backup tapes and verifying continuity.

— Work with backup site and vendor technical staff as needed.
b. Communications network
— Determine damage to communications network and provide for replacement equipment.
—Work with telephone company to restore full service and order telecommunications facilities as needed.
— Notify and inform users of disruptions in service.

7. Database Team

Team Captain: Database Administrator—____

Alternate:____

Responsibilities:
— Full restoration of the database and verification that the files are current.
Team Members:
— Data Administration personnel
Disaster Recovery Function: Database Restoration and Integrity
— Supervise restoration of the database from backup tapes.
— Restore intermediate data to allow files to be updated to a current status.
— Run tests and check them against user listings. Ensure that future processing is accurate by working with users.

8. Systems and Programming Team

Team Captain: MANAGER OF SYSTEMS AND PROGRAMMING—
____

Alternate:____

Responsibilities:
— Ensure production systems are restored and verify continuity of ongoing processing.
Team Members:
— Systems and Programming staff
Disaster Recovery Functions:
a. Application systems restoration and recovery
— Coordinate with Operations and Data Control to verify proper restart point.
— Verify application software programs and libraries.
—Supervise file restoration and ensure continuity of data by testing and comparing results to users' listings.
b. Application programs
—Supervise the processing of critical applications at backup site or arrange for processing at service

bureau.

9. Insurance Department Team

Team Captain: MANAGER INSURANCE DEPARTMENT___________________________________

Alternate:____

Responsibilities:
— Review the damage and notify the insurance company to request appraisal process.
— Provide detailed accounting of the damage to senior management.
— Process all claims.
Team Members:
—As assigned Disaster Survival Functions:
Insurance and salvage
— Contact insurance companies and do follow-up with adjustors.
— Review the damage and determine hardware that can be repaired.
— Prepare report that details damage and outlines disposition.
— Initiate insurance claims.
— Advise other teams of the replacement provisions in the existing insurance policy and the allowance for renting and leasing necessary equipment.

10. Internal Audit Department Team

Team Captain: MANAGER OF Internal. AUDIT____

Alternate: ____

Responsibilities:
— Assure that data and file restoration is accurate and on-going processing is proper.
Team Members:
—As assigned
Disaster Recovery Function: Verification of the Integrity of Restoration Operations
— Verify restoration process to ensure integrity and continuity.
—Audit financial files to ensure recovery process was complete.
— Monitor controls and security during recover): mode.

C. Team Preplanning and On-going Functional Responsibility

1. Disaster Planning Coordinator
a. Keeps Plan documentation updated; correcting names, addresses, and telephone numbers.

b. Ensures Plan is properly distributed to team members.
c. Develops testing schedule of all phrases of Plan.
d. Works with Internal Audit to validate procedures.
e. Distributes literature on safety and disaster recovery.
f Periodically checks backup facilities.
g. Formally updates Plan every six months using input from teams.
2. Emergency Management Team
a. Team leader schedules quarterly meetings, discusses current status.
3. Operations Team
a. Keeps computer room floor plans current for both main location and backup facilities.
b. Keeps organizational charts current.
c. Keeps copy of all company hardware configurations.
d. Keeps updated copies of vendors who supply hardware, software, communications, supplies, and custom forms.
e. Keeps current emergency procedures for fire, water damage, and other potential hazards.
f. Keeps off-site backup tapes current.
g. Stores current microfiche of critical historical records.
h. Keeps Operations run-book information stored off site.
i. Keeps contingency plans operational.
4. Data Entry and Control Team
a. Keeps a current listing of systems and documentation used by both departments.
b. Keeps copy of keying instructions off site.
c. Makes contingency agreements with local users and/or vendors for mutual emergency use of each

c. Makes contingency agreements with local users and/or vendors for mutual emergency use of each others' equipment.

5. Special Projects Team

a. Keeps current listing of transportation companies to be used in emergency.

b. Sets up contingency plans to deal with distribution of emergency funds.

6. Technical Support Team

a. Ensures operating system and communications software are off site.

b. Keeps current list of disk files and layout identification.

c. Ensures communications network information is current, including teleprocessing-line now chairs, terminals, and controllers.

d. Prepares a full recovery capability using off-site backup tapes.

7. Database Team

a. Ensures database off-site backup arrangements are complete.

8. Systems and Programming Team

a. Reviews all systems to ensure adequate arrangements for off-site backup have been provided for programs, files, and documentation.

b. Verifies that proper retention is being maintained as noted in retention policy in company records.

c. Lists all systems, users, processing priority, and responsible programming staff.

d. Identifies critical systems and prepares detailed recovery plans.

9. Insurance Department Team

a. Reviews insurance coverage and verifies adequacy of Plan.

b. Reviews coverage to verify that insurance is in conjunction with MIS Contingency Plan and that premiums reflect backup efforts.

10. Internal Audit Department Team

Reviews MIS Contingency Plan to gain a thorough understanding, checks for control points, and verifies for completeness.

IV. SUPPLIERS

Not all of the suppliers that you actively work with in your normal business environment will be listed in this section. This section is designed to identify only those specific vendors who need to be contacted to repair or replace equipment or supplies critical to the operation of the data center and required as part of the recovery effort.

Information on vendors should include names and addresses of key sales representatives and technical personnel and lists of all local and central emergency phone numbers (Form 30).

List vendor policy as to response time and stated position on reacting to emergency situations in delivering replacement equipment.

List the major equipment units that are key to this vendor. Details will be part of the installed equipment list. Specify if this equipment can be obtained from vendor as part of current production or if available from used-equipment vendors. If so, list availability.

List alternate backup installations or disaster recovery facilities that offer availability of equipment.

A. New and Used Hardware Suppliers

MIS management often focuses recovery planning efforts on computing equipment. Since computing equipment is more readily interchangeable than people, is more portable than plants, and has shorter lead times than communications, this focus can be very misleading. Nonetheless, it often happens because the DP manager sees his equipment as being the most unique asset.

Today, the population of computer hardware, even of any given type or model, is quite large. Job streams are portable from one system to another. Components are portable and can be readily moved from one location to another. Vendors are particularly responsive to emergency situations and usually have a detailed description of the installed hardware. As a result, most data processing installations can expect to be able to find replacement hardware faster than they can find adequate space to put it in.

A complete list of all equipment and specifications is essential in a recovery situation. A list of used-equipment vendors and their specialties should be part of this section of the plan.

B. Software Suppliers

A complete list of any special software, whether operating system or application system, should be kept. Special considerations for backing up these packages should become part of the plan.

C. Communications Suppliers

Communications facilities normally have long lead times, which can generally be shortened only slightly even in an emergency. These lead times should be kept in mind when the vendor list is determined. When the required lead time of the desired facility is greater than the objective recovery time, a strategy must be prepared to substitute a slower or higher cost, but available facility. For example, dial-up lines may be substituted for leased lines, voice facilities for data facilities, or mail for telephones.

D. Special Equipment Suppliers

For the most part, computing equipment is modular and portable, and, at least in emergency situations, has short lead times. On the other hand, if there is old, unique, or obsolete equipment, or if there are hardware-dependent applications, then special strategies should be part of the Plan. If an upgrade or reconfiguration is already planned, it may be wise to accelerate the schedule.

E. Suppliers of Office-Support Equipment

Office-support equipment should be listed, along with alternate devices or plans to obtain services from a second source.

F. Computer Custom-Forms Suppliers

A complete list of vendors that are providing custom forms should be part of the Plan. Samples and specifications are helpful in describing requirements to a vendor. Forms can often have a long lead time if they must go through the entire cycle from draft artwork to finished product. It is helpful to have more than one vendor that can supply the same form. A single supplier with a heavy work load may not be able to react quickly enough to your needs in an emergency situation. To speed up the entire process, we suggest that your suppliers maintain camera-ready samples of your custom forms, even if they have not previously produced the form for you. This will also provide the off-site protection for sample custom forms that your plan requires.

Form 30 Updated

Vendor Name____

Address of Local Office____

Phone Number____

Contacts:
A Sales Representative:____

B. Technical Representatives:____

1. Hardware____

2. Software____

C. Emergency Phone No.____

Vendor Response

Equipment

Alternate Facility

V. PRIORITIZE ALL APPLICATIONS

A. Rate All Systems with Their Priorities

The principal Real of MIS is to provide the ability to quickly restore service for critical applications when there is a serious failure or disruption of regular operations because of fire, natural hazards, power failures, or other causes. The purpose for identification of critical systems is to establish an approach to disaster-recovery planning that will outline functions both before and after a disaster leading to full restoration of services. The planning must be sufficiently detailed so that major decisions will be made prior to, and not immediately after, a serious situation occurs. If a disaster or serious failure does occur, there will be enough confusion and stress without worrying about who does what and how.

The continuation of a large percentage of the MIS operations at an alternate site immediately after a disruption is rarely logistically, technically, or economically feasible. It is seldom essential, since the tasks performed are not all of equal importance. This relative importance of the various functions must be analyzed. The following procedures are designed to step through the business functions in priority order.

It should be assumed that some reduced level of MIS operations must be endured during the primary post-disaster recovery period. For planning purposes, two key issues need to be determined: for which applications is post-disaster survival critical, and which critical applications need urgent attention when the recovery effort begins.

The following information will help in these evaluations. The process will help identify the critical standing of an application within the business. The technique uses seven factors that can help identify an application's vulnerability to performance degradation when a disaster occurs as well as the con straints that may be present when the application must be restored.

The seven factors are:
1. The time that can elapse before the application recovers after a disaster
2. The unique resources required if the application is to be restored
3. The application's ability to withstand relocation during restoration
4. The MIS Operations staffs experience in testing the restoration process
5. The limits on loss that can be tolerated if application restoration is delayed or not possible
6. Structural or operational defects that may be present in the application
7. Security considerations regarding structure or performance
Collectively, these factors establish the relative importance of the post-disaster recovery of specific applications. Individual factor ratings are developed as follows:

Ratings: Time
5 Required to reach median operational level 4 to 6 hrs after disaster
4 Required to reach median operational level 7 to 12 hrs after disaster
3 Required to reach median operational level 13 to 24 hrs after disaster
2 Required to reach median operational level 25 to 48 hrs after disaster
0 No time constraints

Ratings: Unique Resources
5 Adequate restoration requires full recovery of a unique database and/or custom software/hardware and/or non-dial-up telecommunications facilities
4 Can operate adequately on dial-up basis if all other unique resources are available
3 Can be restored to an adequate operational state with only partial recovery of key resources (i.e., by using the current/backup version of the database)
2 No unique resources required for restoration
0 Can operate during the post-disaster recovery period with some features/subsystems disabled

0 Can operate during the post-disaster recovery period with some features/subsystems disabled

Ratings: Relocatability
5 Application cannot be successfully restored at other than the prime processing/operating site
3 Application can be relocated successfully but with a delay exceeding the application time factor
0 No difficulty anticipated in application relocation

Ratings: Experience
5 Currently assigned MIS operations staff has not successfully tested application restoration process
3 Application has been successfully restored in test after a significant delay
0 No delays or other problems encountered during successful recovery testing

Ratings: Loss Toleration
5 Failure to restore within time/feature constraints will likely lead to dollar loss exceeding established management tolerance
4 Failure to restore within time/feature constraints will create problem with major customers/suppliers/union groups/regulators that would exceed management/operational tolerance
2 Must be restored successfully, but loss problems associated with incomplete or delayed restoration can be tolerated
0 No loss problems anticipated through delayed or incomplete restoration

Ratings: Operational Defects
5 Successful restoration and “normal” operation requires direct involvement of key programmer and operator
4 Application lacks current documentation and/or is scheduled for major overhaul
3 Application has demonstrated sensitivity to changes in data input volume, mix, and/or quality, and/ or has evidenced significant failure rates
0 No known defects

Ratings: Security Considerations
5 Application contains corporate-sensitive and/or proprietary and/or employee/customer “personal privacy” data
4 Application controls funds disbursement or otherwise affects custody over assets
0 No special security considerations required beyond exercise of due care during restoration processing
Using this assessment technique will result in a ranking of application systems in terms of relative importance. The maximum score for any application, 35, identifies the most critical systems. The ranking provides a guide for proper allocation of limited resources during the post-recovery period. Form 24 can be used to complete the evaluation of all applications.

VI. MEDIA PROTECTION

A. Protection and Retention of Vital Records

The protection and retention of vital records is a part of your normal business operation. Various records need to be made available to society or to stockholders upon request to verify the information your organization supplies as part of their business. Your company also has a legal responsibility to protect certain records for a specified number of years.
Magnetic tape is commonly used to store company records because of the amount of data that can be contained on a single reel of tape and because the tape can be easily secured in an off-site location. Storing tape at a commercial media-storage facility is usually very economical and fulfills the requirements of off-site protection for vital records.
Some records need to be stored in their original form. The data center does not normally get involved in these procedures because the center only acts as a service center for processing user information. The original forms or source documents are usually the responsibility of the users. Some users choose to copy the original form onto microfilm because of space requirements. The microfilm can be duplicated and a copy sent off-sire to a commercial media-storage facility. For some original records, multiple copies already exist because of the nature of the records themselves. When this occurs, only the controlling of

the records at each location is necessary. When there are multiple copies of a particular record but they all reside at the same location, procedures need to be established to capture one copy of the record and store it at another secure location.

When the data center has the responsibility to secure the computer records off site, it normally accomplishes this by copying the records to magnetic tape and transporting the tape to the off-site location. Copying the computer records can be a separate step in the normal processing of the information, or it can be part of an existing step. Sending the second or third generation of a tape tile off site may be considered adequate by some managers, but this may not fulfill the needs of your recovery plan. If a second or third generation tape is to be used to bring your files to a current status following a disaster, considerable processing may be necessary following the restoration of the file from the off-site backup tape.

Regardless of the method used to store records off-site, a written procedure and a scheduled pickup and delivery, with a person assigned the responsibility for supervising the procedure, needs to be pan of the complete operation.

B. Protecting the Database

1. Database backups

Complete daily backups are taken when the database is not open. If possible, copy the database to two separate tapes and send one tape off site. The other tape is kept on site for seven days.

2. Updates

A log tape is created capturing the before and after image of all modified records. These tapes are kept on site for seven days.

3. Database definition

If your database definition normally remains static, the database definition should be backed up only after it is updated. If it changes quite frequently, it can be backed up weekly along with technical support software as long as you also back up the change information. These backups should be kept off site. 4. Software modification source code

Software modification source code is stored on a source code file. The source code file is backed up weekly and rotated off site.

C. Standard Backup Procedures

Most data centers back up their files to tape and rotate the tapes off site. The tapes are created either as part of the normal processing or as a separate step. If the tape is the standard new generation of a file and it is needed for the next processing, a second tape is required so it can be rotated off site. Rotating a second- or third-generation tape instead of the current tape off site would require reprocessing to bring the file to a current status during the recovery mode. The tapes rotated off site should be as current as the processing that created them. The frequency of processing can be any of the following.

1. Daily processing
2. Weekly processing
3. Monthly processing
4. Annual processing
5. Applications cycles
6. Disk volume backups

D. Off-Site Storage

Off-site storage provides a method of protecting high-speed, machine-readable media that is an essential part of file reconstruction in a disaster recovery mode. Having the media off site reduces the risk of a single disaster destroying all copies of file backups. Disasters such as a fire, explosion, water damage, and aircraft accident will not affect two widely separated locations, and the risk is greatly reduced for area disasters such as those caused by weather conditions. When media is rotated to off-site locations, a copy of the inventory at that location should accompany the media. A second copy should remain at the data center. The listing should contain the librarian or reel number, the name or description of the file, and the time and date the file was created.

E. System and Program Documentation

System documentation should be created through the computer so the documentation can be easily maintained and easily accessed. It also assures that the information can be backed up and rotated off site. The information can also be printed and stored in a binder. If a disaster occurs at the data center, the system documentation can be recovered along with other critical files. If the documentation isonly on source documents, it must be copied or microfilmed before it can be stored off site. Maintaining these backup copies has traditionally become a forgotten or "do it later" task. Program documentation in many data centers has become the source code listing itself. If a librarian system is used to store and maintain the source code, the librarian file should have file backups scheduled at least weekly. All modifications must also be maintained until the next weekly backup.

F. Data-Entry Backup

At a data center where the keying formats are modified infrequently, the data-entry format file should be backed up each time the file is modified. A copy of the backup should remain at the data center and a copy rotated off site. If modifications occur more frequently, a weekly scheduled backup may be preferred. All changes must be maintained until the backup file is created. The formats may be designed to execute primarily in your data entry department with the equipment you use. Formats that can be used by a service bureau should be easily available so that other sources may be used in a recovery mode.

Other documentation concerning the data entry functions should be entered into some maintainable computer file so that it can also be backed up and rotated offsite. This documentation would include such items as user contacts, schedules, volumes, etc.

G. Microfiche Procedures

Microfiche is a printed report generated on film. It is an inexpensive and compact method of maintaining reports. Its value in a recovery mode is limited to source information since it is not machine-readable, When errors cause the backup file to be missing or unusable, microfiche may be the only source for reentering data. Microfiche should be stored in a temperature- and humidity-controlled environment to ensure its usability.

H. Personal Computer File Backup

Those persons having a personal computer have the responsibility to protect files important to the continuing operation of an organization. If a file is critical, it should be well documented and the responsibility for it should be shared by more than one person. Files should be backed up on to diskettes and the diskettes secured off site. An executive who keeps the only copy of a confidential diskette in his or her desk may lose this information if some disaster destroys the office.

I. Computer Custom Forms

Custom forms are the continuous computer forms designed only for your organization. Replacing these forms by ordering them from a supplier in an emergency situation may not conform to your time schedule. The suppliers measure their lead times in weeks. When the forms are needed for critical applications such as payroll, customer invoices, and production scheduling, you cannot wait for the supplier. Many companies overcome this problem by having multiple suppliers for the same custom form or by storing the same form in different locations. Sample copies of the various forms should be maintained in a secure location to improve supplier turnaround with little loss in quality in an emergency situation.

VII. COMPUTER ROOM OPERATING PROCEDURES

A. Power-Up Procedures
Include computer center procedures or identify source
B. IPL Procedures
Include computer center procedures or identify source
C. Power-Down Procedures
Include computer center procedures or identify source

Include computer center procedures or identify source

O. Schedules

Include computer center procedures or identify source

E, Operations Run-Books

Include computer center procedures or identify source

F. Application Responsibility

Include computer center list of all production systems and the name of the persons responsible for each. Also include on the list their home phone numbers and any beeper phone numbers.

VIII. OPERATING SYSTEM

A. Software Operating Environment

The optimum in processing at your backup facility is to execute under the same operating system. In order to bring up your operating system at the backup site, the computer hardware must be compatible with your current hardware. If the operating system is coded to execute only on a single mainframe, you may have to arrange with your software vendor to execute on a replacement configuration. If some hardware is different from your own hardware, you will have to do an I/O Generation. If the backup facility operates as a virtual machine, you may bring up your operating system as a sub-task under the host system.

B. Listing of All Purchased Software Packages

Most software packages are coded to execute on a single mainframe. Make any necessary arrangements with your software vendor so that your purchased software will execute at your backup facility.

Include computer center listing or identify source

C. Disk Drives and Pile Layouts

If the type and/or number of disk drives at the backup facility is different from your data center, make plans for the placement of permanent files and the placement and sizes of work areas. If job control statements will have to be altered, have a method for changing the job control language JCL) already planned out.

Include computer center listing or identify source

IX. PHYSICAL SECURITY AND ACCESS CONTROL

Physical security begins with access to Your organization’s property. Many companies have guards stationed at all access roads to the office complex. Further security is provided by personnel located at the reception desk of each building and at the reception desk of each floor and/or department. Once individuals pass the human element, their access to various areas is normally controlled by some type of access control system. An access control system prevents unauthorized persons from entering secured areas. Other than guards and guard dogs, these systems are mechanical (locks), electronic (typically, an electronic control box used with a key), electromechanical (such as push-button devices that work with electronic badge-readers), digital (devices that allow users to set any combination), and computerized (including systems that can sound alarms, record employee attendance, monitor employees’ locations, and produce operational control reports).

Access for the people in the following categories should be stated so that only those persons having the proper authority can enter the various restricted areas:

A. Computer Operations

B. MIS Staff

C. Service and Maintenance Personnel

D. Outside Company Personnel

1. Hardware

1. Hardware
2. Communications
3. Miscellaneous
E. Access Control
F. Secured Forms-Room Access
G. Vault Access
H. Non-office Hours
I. Security Duties: Guards
J. Office Security

Although access to the general office area is normally given to all employees, a few office security measures are noted here.

—Confidential information such as a password listing or payroll information should not be left unattended on a desk.
— Separation of duties should be maintained in all areas involved in the disbursement of funds, such as payroll and accounts payable.
—A rotation of duties for all people involved in the disbursement of funds should be scheduled, and these people should not be allowed to continually work through their vacations.
—A manual log to account for all checks should be established.
—A manual log for all usage of the manual check signer should be established.
— Duplicate check-signing plates should be secured off site, possibly in a safe deposit box.

X. SOFTWARE SECURITY

A. Sign-On Passwords

Most purchased software includes some type of provision for restricting use of the software to only those individuals who know the password. Signing on to the host computer usually requires a password. The password is internally checked against a table that tells the system if the terminal operator has entered a valid password. If the password is valid, the system then displays a menu screen. When the operator selects an entry in the menu, the system checks that entry against the password table to see if the operator has access to the selection. If the user has access, the access could be further restricted as to update capabilities or lust read-only access. Even the information on the screen could be masked so that only the information that the operator has authority to view will be shown. If the operator selects a different purchased software package from the main menu, he or she may have to enter a new password to have access to this new selection.

B. Maintaining Application Programs

If your application source code is managed by some type of source code librarian, some of the application programs may have password security protecting access to the code. In many organizations that do not manufacture or produce classified types of products, the only programs with password protection are those that disburse funds, such as payroll and accounts payable. Password protection will help deter people from making unauthorized changes to the software.

C. Password Maintenance

Every organization should have a formal procedure for maintaining passwords. The procedure should begin with issuing passwords to new employees. Documents need to be approved by supervisors before passwords can be issued. The approval will indicate all access authorized for the employee. The entering of the passwords is usually the responsibility of the security officer or someone in the Technical Services Department. Regardless who is responsible for entering the data, a different person should be responsible for verifying the passwords by making a spot check at least once a month. The second person does not have the ability to enter or change passwords, but only to view them and the approving document. Part of the password procedure should be the mandatory entering of a new password by all terminal operators at least once a quarter. Software can be generated to broadcast messages to all operators announcing that, by a particular date, a new password must be entered by the operator or, after that date, the operator will not have access to the system until he or she goes through a formal request procedure. This will prevent one person from using another's password to access the system.

The formal procedure should also provide for clearing a password when someone leaves the organization. Again, this will prevent the past employee or someone else from unauthorized use of a password.

XI. BACKUP FACILITIES A fully equipped backup facility where you have tested your operating system and other critical applications is your assurance that, should a disaster ever occur, you are fully prepared to make an efficient and effective recovery with minimal effect on the users you serve. These fully equipped facilities are available to paid subscribers for their use to schedule testing of their operating systems and their applications. They no longer have to depend on a hardware vendor who may supply their cold site with a mainframe and components that they have never tested with. (A cold site is an empty computer room that is equipped with a raised floor, air-conditioning, electric power, and some type of fire protection system, and that is ready for the installation of computer hardware.)

Hardware vendors will work with you as much as possible in an emergency situation, but the locating and delivery of hardware could still take as much as 6 to 10 days. After delivery, the vendor must still install and test the hardware before turning it over to you for testing.

Having both a fully equipped facility and a cold site as part of your disaster recovery plan is the most cost-effective if you ever have to move off site. The recovery will start at the fully equipped facility while preparations are being made to install replacement equipment at the cold site. When the cold site is prepared, the computer operations can be moved from the high-cost, fully equipped facility to the low-cost cold site. When your permanent facility is reconstructed, the operations can be moved from the cold site to the permanent facility.

A. Subscribing to a Backup Facility

There are many fully equipped backup facilities from which to choose. For the most part, they offer the same services. They may differ in the amount of floor space they offer, the type and size of hardware that is installed, the physical security they have for their facility, or their geographical location, but they still offer the basic solution: an operational computer ready to be used by one of their subscribers. Before you choose one facility over another, compare their services, location, and hardware, and select the facility that best meets the needs of your organization.

The contract you sign will contain many of the following items: terms and effective date, definition of contract terminology, use of the facility, fees and payment schedule, conditions concerning multiple disasters, liability, hardware changes, confidentiality, and termination of contract.

B. Facility Layout

The company you contract with should furnish you with a layout of the facility. This would include the computer room, tape storage room, office area, conference room, reception area, etc.

C. Hardware and Software

Some facilities have multiple hardware configurations. You would subscribe to the hardware that meets your needs. The operating system that has been installed on the system should allow you to process your system software and applications with a minimum of changes.

D. Communications

Communications from the backup facility to your network cannot be effected without planning and testing. If the telephone company has to install new lines in order to connect with your network, it will require weeks of delays. Preplanning with the phone company will expedite the connection of any necessary lines.

Hardware is available that can be installed between your host computer and your communications network. This same hardware can be installed at the backup facility and connected with its computer. A link can be easily made between this hardware at both locations. Once the link is made, your communications network is connected with the computer at the backup facility.

E. Supplies

Available backup supplies have to be moved from their storage areas to the backup recovery facility. Suppliers on the list of critical vendors need to be informed of the location of the backup facility so additional supplies can be sent.

F. Testing

Your Plan must be tested over and over again so it will be ready to be put into effect once a disaster occurs. Your data center, as well as the backup facility, is continually being upgraded. New software and hardware are being added, and an application that tested successfully in the past may not execute now. The only way to be assured that you can move your operations to the backup facility and know that processing can continue is to test and test and test.

Testing at the facility should be well documented. Avoid relying on a single key person to bring up your operating system and restore the necessary libraries and files. If a disaster occurs, that key person may not be available to function as he or she ;lid in the testing phase.

1. Initial testing

Initial testing should be concerned with bringing up the operating system, testing job control language JCL), restoring files on disk drives that could be different from the drives that you have in your data center, testing communications, and testing a simple batch job that uses purchased software. Future testing would require testing all applications that were classified as critical to the operations of your organization. It would not be unusual for you to be unsuccessful in your first test attempt. In your first test, you may not even be able to bring up your operating system. The key to success is noting your failures and successes and making changes in your Plan so that your next test is successful.

2. Restoring your tiles and libraries

If you were able to restore some of your disk files and libraries in your first test attempt, you are that much ahead in your testing. In future testing, you should restore your files from tapes that would have been rotated off site from your data center. If the disk drives at the backup facility are different from yours, plan ahead for the way you will download your files, how much space will de allocated to work areas, etc.

3. Testing critical applications

All critical applications should be eventually tested. This is the only way you will know if they will execute at the backup facility. Prepare a schedule for testing all critical' applications and note your successes and failures.

4. Testing communications

Communications may be required in testing some of your critical applications. If communications is not part of the testing of the first couple of applications on the schedule, it should be tested as soon as possible so that any necessary line requirements can be initiated.

5. Mock disasters

Although you schedule testing at the backup facility, your management should approve a surprise test using a mock disaster. With scheduled testing, your people know ahead of time which kind of testing is using a mock disaster. With scheduled testing, your people know ahead of time which kind of testing is going to he accomplished and they can prepare for it, even though they may be told not to. Using a mock disaster, you can better evaluate the effectiveness of your Plan.

6. Testing program compilations

Support at the backup facility for the programming staff is an essential part of the recovery plan. The programmers must be able to access their source statement library, recompile their programs, and then relink them. They also need access to all of their programming and debugging aids. Compilations should be tested for all languages used in your shop. Test systems should be available unless management has decided to eliminate the test systems because of a lack of sufficient disk space at the backup facility.

XII. RECIPROCAL AGREEMENTS

Reciprocal agreements are mutual aid agreements between two or more data centers that state that if Center A has a disaster, Center B will allow Center A to share time on Center B's computer. This approach was popular years ago to comply with management directives to have a disaster recovery plan. At that time, the computer was not an essential part of the organization as it is today. Back then, the applications were primarily financial and were all batch. The computer was not being used 24 hours a day; at many centers, it was idle even during the prime shift. Hardware configurations were similar and so was software. This is not the environment we operate in today.

The computer is the driving force that dictates what we build, when we build it, and how we build it. It generates shop orders, production schedules, purchase orders, shipping schedules, and tracts material, and tracks orders from the time they are entered into the system until the finished product is ready for shipment. The computer is on line 24 hours a day seven days a week. When is Center B going to have time to share its resources with Center A, which had a disaster? When each center is operating at 80 percent capacity on its own computer, how can they both operate on a single computer? How can one center supply all of the disk capacity for both centers? With reciprocal agreements, Center A's disaster will create a disaster for Center B.

Reciprocal agreements are still a viable alternative to subscribing to a fully equipped backup facility but only for small data centers that still fit the mold of centers of years ago. A reciprocal agreement normal" consists of the following:

—A letter of understanding is exchanged specifying any costs, hours of availability testing arrangements, and a general agreement of response each company expects to offer and or receive during an outage.
—A configuration questionnaire is filled out covering current hardware and software and a schedule is set for updating the questionnaire to ensure comparability.

XIII. INSURANCE PROTECTION

Information is a business asset and, as such, warrants the same protection as other assets. Management has the obligation to stockholders to ensure that all assets are protected. The computer center is as important to an organization as is electricity. A company could not survive if it lost its computer center because of a disaster.

Insurance can cover the cost of replacing or repairing equipment or facilities damaged by some disaster. Optional business-interruption insurance can protect you from the extra expenses incurred during the recovery period.

Some large organizations have umbrella-type insurance that has extensive coverage for multiple companies at multiple locations. Whatever type of insurance your organization has, it must be consistent with the provisions of the Plan. Having a well-documented and continually tested Plan can help reduce your insurance premiums.

A. Data Processing Property Protection Coverage Include any insurance coverage or identify source

B, Insurance on Computer Hardware Include any insurance coverage or identify source
C. Insurance on Other Data Processing and Office Equipment Include any insurance coverage or identify source

D. Business-Interruption Insurance Include any insurance coverage or identify source
XIV. POLICING THE PLAN Once the Plan has been established, there is a continual process of maintaining and policing the Plan to ensure that it is being kept up-to-date and that its recommendations and provisions are being adhered to. The maintenance responsibility belongs to the Disaster Planning Coordinator, but the policing is everyone's responsibility. The MIS Director has total responsibility for the entire Plan, but his or her full staff should be aware of the contents of the Plan and should notify the supervisor if any action or lack of action as specified in the Plan is noticed. Staff members should not look upon notification as a form of "telling on someone," but as a more positive method of ensuring that their jobs will be there tomorrow because they are following protective measures today.

One of the so called watch dogs of the organization is the Internal Audit Department. The department's responsibility is not to make policy but to make sure that all departments are following the policy that management has already established. In many cases, it is one of the recommendations of the Internal Audit Department that pushes the data processing management into formalizing the disaster recovery plan. Many times, people in the data processing department had some ideas about what they would do if a disaster occurred, but they never formalized it. Now that they have a plan, it is up to everyone to make sure that the Plan is being closely followed.

XV. MAINTAINING THE CONTINGENCY PLAN

A. Disaster Planning Coordinator's Responsibility

To help prevent the Plan from becoming out of date, establish a schedule for formal updates to the Plan (see form below). Scheduled updates are in addition to any other intermediate updates that are entered as they occur. Such as address changes, hardware updates, software purchases, etc. Six months has been determined as the time between formal updates.

Assigned Date-------- Disaster Planning Coordinator-------------------- Completion Date

____
__01/01/yy_____ ____
__07/01/yy_____ ____
__01/01/yy_____ ____
__07/01/yy_____ ____
__01/01/yy_____ ____
__07/01/yy_____ ____
__01/01/yy_____ ____
__07/01/yy_____ ____
____
____

B. Team Captain's Responsibility

Each Team Captain also has the responsibility to review and update his section of the Plan at least every six months (see form below).

Team Captains---------------------------------Date------------------------------------Initials
Operations Team ____
Data Entry and Control Team ____
Special Projects Team ____
Technical Support Team ____

Systems and Programming Team ______________________________

Insurance Department Team ______________________________

Internal Audit Department Team ______________________________

DISASTER PLANNING CHECKLIST

Now that your organization has completed an impact/risk analysis and has realized that a disaster recovery plan is essential if you are to survive a major disaster, you need to take an inventory of your current environment and any future planned improvements. It is essential for you to have full knowledge of your present situation and your plans for the future so that you can organize and schedule your future tasks. The checklist below will help you note some of you; existing controls, which are already protecting your organization's assets. Other items on the checklist may prove to be good business practices and easily incorporated into your present operation.

The MIS Contingency Plan is a very comprehensive plan. It has been written in generic terms and Functions so that it can be tailored to any organization's environment. It uses a standard framework that is effective in any phased-development approach to major projects. In order to prepare for the Plan, you must answer a multitude of questions. No single person in your organization will have the answers to all of these questions, but it will require the input from many areas in the data center. This will not only give you a more accurate picture of your status, but also it will generate a feeling of ownership by the entire staff. Any plan, good or bad, will have a better success rate if all parties are eagerly working for the good of the plan.

The checklist has been broken down into major categories: General Overview, Data Center Facility, Data Entry, Data Control, Computer Room, Tape Library, Telecommunications, Systems and Programming,

Technical Support, Database Administration, Internal Audit, Insurance, Backup Facility, and Reciprocal Agreements, Many of the categories relate directly to sections in the MIS Contingency Plan. After each question is space to answer "YES," ''NO" or "Work in Progress (WIP)." There is also a place to enter a notation as to who is assigned to complete the item or what action is planned. The checklist is designed to be a working paper that can be updated as events occur.

Questions-------------General Overview

	YES	NO	WIP	-------- ASSIGN/ACTION
1. If a major disaster to your data center occurred today, could your organization survive'				
2. Have you recently completed an Impact/Risk Analysis?				
3. Do you know the total dollar amount of your exposure?				
4. Have you prioritized all of your programs?				
5. Have you listed the maximum downtime for all of your systems?				
6. Have you listed the objectives of a disaster plan and the assumptions it includes?				
7. Do you have a disaster plan, and is it current?				
8. Does the Plan include backup facilities? Hot backup site? Cold site? Reciprocal agreement?				
9. Does the backup facility inform you when there is a change in hardware or software!				
10. Have you determined the cost of a disaster plan including: Initial cost?				

Development cost? Maintenance cost?				
11. Has the plan been approved by top management?				
12. Do you have a Disaster Planning Coordinator!				
13. Is someone assigned to update the plan?				
14. Does the plan use a team approach?				
15. Do you have people assigned to lead each team?				
16. Is the same person assigned to lead more than one team?				
17. Are names and phone numbers updated regularly?				

Questions-------------General Overview

	YES	NO	WIP	-------- ASSIGN/ACTION
18. Has the plan been reviewed by the Internal Audit, Security, and Insurance Departments?				
19. Does the plan provide for recovery from a major disaster, and can it be adjusted for a less severe occurrence!				
20. Has the plan been tested using only material stored off-site?				
21. Is the plan tested at least every 6 months?				
22. Has the plan been updated as a result of the testing?				
23. Have you ever initiated a surprise test!				
24. Does the plan provide instructions for: Emergency procedures? Organizational structure following a disaster? Off-site storage for all recovery material!				
25. Does the off-site storage have 24-hour access, physical security, vaulting, fire protection, courier service, round trip travel time of less than 1 hour, access only by authorized persons?				
26. Are the tapes secured in a separately controlled room within the secured area?				
27. Is all system documentation, except program listings, kept in fireproof storage when not in use?				
28. Are there written instructions that define the responsibilities that personal computer (PC) users have for backing up and protecting their files?				
29. Have these instructions been given to all PC users?				
30. Have all data center personnel been advised about the confidentiality of all information they work with?				

Questions------------- DATA CENTER FACILITY

	YES	NO	WIP	-------- ASSIGN/ACTION
1. Fire there signs outside identifying the data center?				
2. Is the building protected by security guards, fences, alarm systems, and/or closed-circuit monitoring!				
3. Is wiring for all security and alarm systems passed through conduit?				
4. Do the guards make scheduled rounds of the building!				
5. If no guards are used, are the people responsible for security trained by security professionals?				
6. Has someone been assigned the responsibility for security of the data center,				

company, or building?				
7. Are security personnel or computer room personnel on site at all times?				
8. Is there card access to the facility and various areas in the facility?				
9. Are identification badges worn by all employees?				
10. Are visitors required to sign in and sign out?				
11. Is there security at the receiving area?				
12. Is there an Office/Building Emergency Booklet published that includes: Medical emergencies? Fire emergency procedures? Evacuation procedures? Bomb threats? Security violations? Electrical failures?				
13. Has someone been assigned to provide information, instruction, and supervision for the list in Item 12?				
14. Are evacuation route drawings posted in all hallways?				
15. Have all occupants been instructed and trained in emergency procedures?				

Questions------------- DATA CENTER FACILITY

	YES	NO	WIP	-------- ASSIGN/ACTION
16. Are fire drills conducted on a regular basis under the supervision of your local fire marshal!				
17. Is there a written termination procedure that includes a checklist of items to be returned to the company, such as keys, ID badges, card access, etc.!				
18. Are all employees required to take vacation time so others can perform their duties?				
19. Do all areas of all buildings have a fire alarm system!				
20. Has the tire detection and extinguishing equipment been tested and/or inspected in the past 6 months?				
21. Does the insurance company or fire department make annual fire inspections!				
22. Is the storage area for forms and supplies protected with sprinklers?				
23. Are smoke detectors located in the storage area?				

Questions------------- DATA ENTRY

	YES	NO	WIP	-------- ASSIGN/ACTION
1. Are there alternatives for entering input normally keyed on-line?				
2. Have you made provisions to have keying done on the outside in emergencies!				
3. Is a copy of the keying instructions stored off site?				
4. Is a software package used for keying, and is it available to outside services?				
5. Have arrangements been made to have your affiliates or divisions key your input?				
6. Are all manual procedures performed by data entry documented and a copy stored off site?				
7. Are source documents batched and controlled by another department?				
8. Are source documents stamped with date, time, and operator after keying?				
9. Are source documents maintained in their original batches for a short time so they can be re-keyed if necessary?				
10. Are source documents returned to the data control department after keying!				

10. Are source documents returned to the data control department after keying?				
11. Can the data entry department be reestablished in another location in a reasonably short time if necessary?				

Questions------------- DATA CONTROL

	YES	NO	WIP	-------- ASSIGN/ACTION
1. Is access to the data control department restricted?				
2. Are ail source documents and computer reports routed through this department for control and balancing?				
3. If communication fails for transmitted reports, has an alternate method for sending reports to users been established?				
4. Is this department responsible for the control of check forms?				
5. Is there a written procedure for issuing a supply of blank checks outside the computer room?				
6. Are checks signed by a different person from the person balancing and distributing them?				
7. Can the check signer be replaced overnight?				
8. Is there any special office equipment critical to the operation of the data center, that provisions For a substitute have not been made?				
9. Are backup signature facsimiles secured off site?				
10. Is there a formal custom-form system that identifies all forms, their reorder point, their supplier, and an alternate supplier?				
11. Is a small supply of all critical custom forms maintained oh site?				
12. Is a copy of all form specifications and a copy of the final proof maintained off site?				
13. Is a fact sheet maintained on all suppliers of office equipment and forms?				
14. Has an alternate point-to-point pickup and delivery been planned for if the primary method is not operational?				
15. Is there an output distribution report form for every printed report defining: number of copies, decollate, burst, method of shipping, recipient name, and recipient phone number?				

Questions-------------COMPUTER ROOM

	YES	NO	WIP	-------- ASSIGN/ACTION
1. Is access to the computer room restricted?				
2. Are only the computer operators allowed to operate the computer?				
3. Is the room protected by Halon, CO,, or sprinklers!				
4. Are smoke detectors located: In the ceiling? Under the raised floor! In the air conditioning ducts?				
5. Will the smoke detectors operate even if there is a power outage!				
6. Are fire extinguishers located at all exit doors?				
7. Are water detectors located under the floor?				
8. Are waterproof covers stored in the computer room for emergencies?				
9. Is a UPS system installed for short power outages?				

10. Is a generator available for extended power outages?				
11. Is there emergency lighting in the computer room?				
12. Is there an emergency Power-Off switch located at the exits?				
13. Is there more than one cooling system that will support the computer hardware should one system fail?				
14. Will an alarm sound if the air conditioning system is turned off?				
15. Is the temperature and humidity monitored?				
16. Will some type of visible or audible alarm sound if the limits are exceeded?				
17. Are fire doors installed at all entrances to the computer room?				
18. Are check forms stored in a secured room!				

Questions-------------COMPUTER ROOM

	YES	NO	WIP	-------- ASSIGN/ACTION
19. Are there written instructions for powering up and powering down the system?				
20. Are there written instructions for actions to take in an emergency!				
21. Is there a copy of the MIS Contingency Plan in the computer room!				
22. Is a procedure library used that contains all the job control necessary to execute job streams?				
23. Is there a formal scheduling system, either computerized or manual?				
24. Is someone assigned to review the schedule and enter all control record information!				
25. Is the entering of control records and similar job control Functions eliminated from operator intervention?				
26. Are tape mounts controlled by a tape- librarian system!				
27. Does a supervisor review reasons why an operator overrides the tape-librarian system?				
28. Does operations management review the console log and error listing to ensure that identifiable errors are corrected and recurring errors are prevented?				
29. Are there written restart procedures for all production systems?				
30. Do the restart procedures indicate that other systems may have to be reprocessed even though they completed successfully!				
31. Do all high priority systems have detail recovery procedures documented?				
32. Are all problems in the computer room documented?				
33. Are metered hours correlated to lapsed time if practical?				
34. Is there a formal Problem Management system, where computer room problems are reviewed by members from operations and programming and remedies assigned?				

Questions-------------COMPUTER ROOM

	YES	NO	WIP	-------- ASSIGN/ACTION
35. Is all down time reviewed by operations management?				
36. Is all production job control reviewed by the operations department after testing is completed and before programs are turned over for production?				
37. Are there Run Manuals for all production applications!				
38. Do the operators have easy access to the Run Manuals?				

39. Are duplicate copies of the Run Manuals stored off site?				
40. Is all special processing for quarterly or annual runs properly documented?				
41. Are batch jobs scheduled for each shift?				
42. Is there a computerized job-accounting system!				
43. Is the job-accounting report reviewed to determine any unusual run patterns?				
44. Are all new systems reviewed for proper file rotation to off-site storage!				
45. Is there a list of all computer hardware including serial numbers, communication equipment and lines, power requirements, cooling requirements, floor space requirements, and acceptable substitute equipment for all the above; and is a copy of this list stored off-site?				
46. Is there a cable layout diagram and plug connector description For the current equipment, and is a copy stored off site?				
47. Is a Vendor Information sheet maintained for all vendors supplying computer equipment and supplies?				
48. Have you asked a used hardware vendor for a list of available equipment, in preparation for an emergency!				
49. Are the following backed up daily and rotated off site: Procedure library! Tape librarian? Job scheduling?				
50. Is there a formal procedure For obsoleting a program?				
51. Are the microfiche procedures documented and a copy stored off-site?				
52. Are there any water pipes near or above the computer room?				
53. Is there a threat of water leakage from nearby areas: kitchen, rest rooms, janitor closet, drinking fountain?				

Questions------------- TAPE LIBRARY

	YES	NO	WIP	-------- ASSIGN/ACTION
1. Is the tape library protected by Halon, CO,, or sprinklers!				
2. Are smoke detectors located in the tape library?				
3. Does the entrance to the tape library have a fire door?				
4. Does the tape library have emergency lights!				
5. Is access to the tape library restricted by card access or other security?				
6. Is a fire extinguisher mounted outside the door to the tape library?				
7. Has the tape library become a storage area for items other than tapes?				
8. Does the off-site storage for tapes have security, fire protection, 24-hour access, bonded pickup and delivery?				

Questions-------------SYSTEMS AND PROGRAMMING

	YES	NO	WIP	-------- ASSIGN/ACTION
1. Is all application software backed up and stored off site!				
2. Do all changes to programs need authorization?				
3. Are there audit trails that identify any program that has been copied for modification, or new program in development?				
4. Is all application software responsible for distributing funds, such as payroll and accounts payable, password protected?				
5. Do the systems above have adequate controls, such as batch totals, hash totals				

5. Do the systems above have adequate controls, such as batch totals, hash totals, run totals, and dollar amounts?				
6. Are checks outside the normal range flagged on an audit trail report?				
7. Does an accounts payable audit trail report list the payee for all checks?				
8. Do all financial applications hale complete audit trail reports?				
9. Is all of the on-site system documentation stored in fireproof cabinets?				
10. Are users asked to assist in the preparation of test data?				
11. Is there a formal methodology for design and programming?				
12. Is the design phase completed before the programming phase begins!				
13. Are there written design standards and programming standards?				
14. Are 311 permanent files categorized as critical, important, useful, and non-essential?				
15. Do the standards require the backing up of all critical files?				
16. Are the 3 most current generations of all important and critical files maintained (current, father, grandfather)?				
17. Do the standards require all programs to include proper controls and totals for complete auditing, and for the detection and correction of errors?				

Questions-------------SYSTEMS AND PROGRAMMING

	YES	NO	WIP	-------- ASSIGN/ACTION
18. Is test data with Predetermined results saved and used for heavily maintained systems such as payroll?				
19. Are program changes always made to the source code?				
20. Is the source code maintained on a library that is backed up and rotated off site?				
21. Are the program link-edit reports reviewed for errors and filed with the source code listing!				
22. Are programs always tested even when they have minor modifications?				
23. Does management randomly review program changes and test results?				
24. Do user departments sign off on program modifications and review test results?				
25. Is there a formal procedure for making a program in development a production program?				
26. Are operation Run Manuals required as part of the program turnover to operations?				
27. Are all modifications to purchased software fully documented and coded in a way that will not disturb the pure supplied code?				
28. Is a list available of all systems with the person responsible noted?				
29. Is there a list that identifies all programs in a system!				
30. Does each system have a back-up person!				
31. Is documentation kept current?				
32. Is documentation maintained on the computer, backed up, and rotated off site?				
33. Is there a listing of all technical manuals so they can be replaced if necessary?				
34. Does your company policy state the tile retention period for corporation assets information, stockholder information, tax records, employee information, and other vital records?				
35. Are record layouts maintained For the retention period along with the file media!				
36. Has the source information been identified that created the retained data?				

Questions-------------TECHNICAL SUPPORT

	YES	NO	WIP	-------- ASSIGN/ACTION
1. Is the operating system backed up and rotated off site!				
2. Is a list maintained of all operating system software?				
3. Are the people in the department cross- trained so that everyone has backup?				
4. Are all responsibilities, duties, and procedures documented and a copy stored off site!				
5. Is a Vendor Information sheet maintained for all vendors supplying software?				
6. Have provisions been made for purchased software to execute on another system during an emergency?				
7. Is a copy of the SYSGEN parameters stored off site?				
8. Is there complete documentation explaining how to bring up the operating system at the backup facility?				
9. Is the utilization of all disk devices documented?				
10. Has a plan been formulated on how alternate disk devices would be utilized?				
11. Is there documentation explaining how to modify the JCL to execute at the backup facility?				

Questions-------------DATABASE ADMINISTRATION

	YES	NO	WIP	-------- ASSIGN/ACTION
1. Are all databases identified?				
2. Are all programs that update each database identified?				
3. Is the activity that updates the database continually logged?				
4. Are all programs that access each database identified!				
5. Are databases backed up and rotated off site?				
6. Are audit trails available that identify databases that are filing up, and are these reports available on a daily basis?				
7. Are there documented procedures on how to test the validity of each database after it is restored?				
8. Is there documentation that identifies multiple databases that must be kept synchronized with each other?				

Questions------------- INTERNAL AUDIT

	YES	NO	WIP	-------- ASSIGN/ACTION
1. Have you reviewed the ,MIS Contingency Plan?				
2. Have you observed a recovery test that only used material stored offsite?				
3. Do you periodically review the data center operation and make written recommendations on improvements to procedures, security, and controls?				
4. Are user departments required to balance computer output to manual control totals for audit and security?				
5. Do you save test data to process through cash disbursement systems producing predetermined results!				

Questions-------------INSURANCE

	YES	NO	WIP	-------- ASSIGN/ACTION
1. Has the data center management been informed as to the do's and don'ts concerning insurance following a disastrous event?				
2. Does the insurance policy include business interruption coverage?				
3. Is another department in the organization responsible for insurance protection?				
4. Do you have a copy of the insurance policy?				
5. Have you reviewed the coverage in the past year!				
6. Do you have an annual formal review of your insurance coverage with the insurance carrier?				
7. Does the insurance coverage include data processing hardware and software!				
8. Did you perform a risk/impact analysis for the data center?				

Questions------------ BACKUP FACILITY

	YES	NO	WIP	-------- ASSIGN/ACTION
1. Do you currently subscribe to a fully-equipped backup facility!				
2. Is the backup facility located at a distance that will ensure that an area-wide disaster will not affect the facility!				
3. Is the security at the backup facility at least as good as the security at your current facility?				
4. Have you ever used the backup facility as part of a mock disaster?				
5. Does the backup facility have adequate hours available for testing?				

Questions-------------RECIPROCAL AGREEMENTS

	YES	NO	WIP	-------- ASSIGN/ACTION
1. Do you have a formal reciprocal agreement currently in effect?				
2. Does the other organization's computer have time available to share with you?				
3. Does your computer have time available to share with another organization?				
4. Are both computer systems compatible?				
5. Do both computer systems have the capacity to process critical applications for both organizations at the same time?				
6. Is the operating system software compatible?				
7. Is there sufficient tape and disk capacity and compatibility?				
8. Will your communication network quickly connect with the other organization's computer!				
9. Does either data center have specialized hardware such as laser printers or cartridge tape drives!				
10. Have both organizations agreed to notify the other about changes in hardware or software?				
11. Will your purchased software execute at the other data center!				
12. Have you tested a critical application at the other data center?				
13. Is there temporary storage available at the other data center For printer forms?				

14. Is there temporary storage available at the other data center for your tape library?				
15. Is there temporary office space available at the other data center for operations support personnel?				

Webmaster--Robert Arnold

Last Updated--Monday, January 27, 1997

1862 Old Lemay Ferry
Arnold, MO 63010
Call: (636) 282-5800
Fax: (636) 282-5802
Email: drj@drj.com

FOLLOW DRJ

- DRJ on LinkedIn
- DRJ on Twitter
- DRJ on Facebook
- DRJ RSS Feeds