



@server

iSeries

Plan a backup and recovery strategy







@server

iSeries

Plan a backup and recovery strategy



---

# Contents

---

<b>Part 1. Plan a backup and recovery strategy</b> . . . . .	<b>1</b>
<b>Chapter 1. Backup and recovery timeline</b> . . . . .	<b>3</b>
<b>Chapter 2. Know what to save and how often to save it</b> . . . . .	<b>5</b>
<b>Chapter 3. Find your save window</b> . . . . .	<b>7</b>
Simple save strategy . . . . .	7
Medium save strategy . . . . .	8
Save changed objects . . . . .	8
Journal objects and save journal receivers . . . . .	8
Complex save strategy . . . . .	9
<b>Chapter 4. Choose availability options</b> . . . . .	<b>11</b>
<b>Chapter 5. Test your strategy</b> . . . . .	<b>13</b>
<b>Chapter 6. Disaster recovery plan—template</b> . . . . .	<b>15</b>
Disaster Recovery Plan . . . . .	15
Image description . . . . .	24



---

## Part 1. Plan a backup and recovery strategy

Computers in general, and the iSeries™ server in particular, are very reliable. You may run your system for months or even years without experiencing any problems that cause you to lose information on your system. However, as the frequency of computer problems has decreased, the potential impact of problems has increased. Businesses are more and more dependent on computers and the information that is stored in them. The information that is in your computer may not be available anywhere else.

Saving the information on your system is time-consuming and requires discipline. Why should you do it? Why should you spend time planning and evaluating it?

Because you may have a problem. You **will** need to use your backup copies of information. Every system needs to restore some or all of its information at some point in time.


The Backup and recovery timeline provides a high level overview of the events that occur during the backup and recovery process.

Once you study the backup and recovery timeline, you are ready to start planning your strategy. Follow these steps:

1. Know what to save and how often to save it
2. Find your save window
3. Choose availability options
4. Test your strategy

You may also find the Disaster recovery plan template useful as a planning resource.

This topic contains information on how to plan your strategy and make the choices you need to make as you set your system up for backup, recovery, and availability. For information on how to actually perform

the tasks that are related to these topics, see Backup and Recovery  and the Back up your server topic. The Availability roadmap for your iSeries server topic provides information about the common types of failure that can occur.



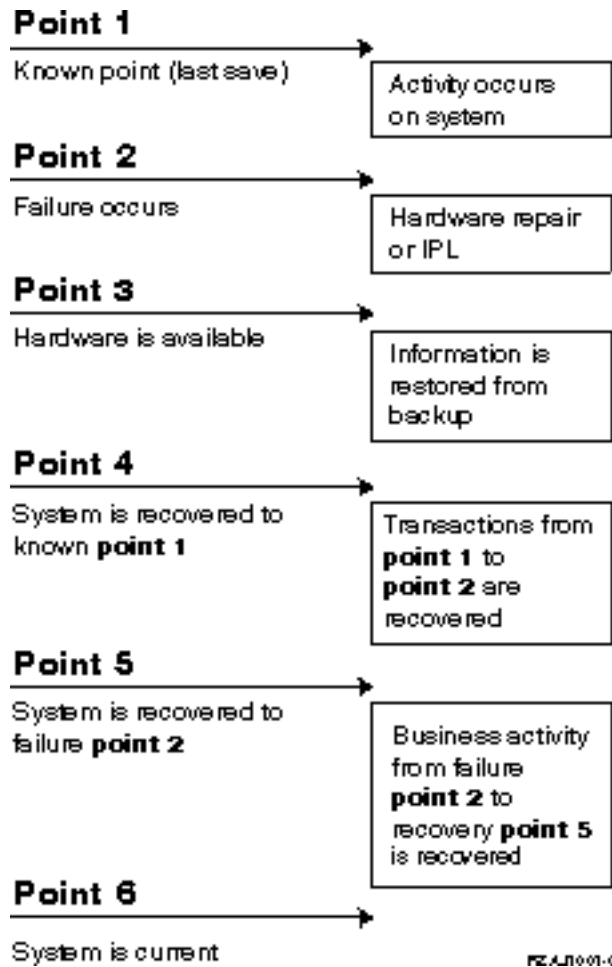


# Chapter 1. Backup and recovery timeline

The timeline for backup and recovery begins when you save information and ends when your system is fully recovered after a failure. Refer to this timeline as you read this information and make decisions. Your strategies for saving and availability determine these things:

- Whether you can successfully complete each step in the chart
- How long it will take you to complete each step

As you read, use the chart to develop specific examples. What if the known point (1) is Sunday evening and the failure point (2) is Thursday afternoon? How long will it take to get back to the known point? How long will it take you to get to the current point (6)? Is it even possible with the save strategy you have planned?





## Chapter 2. Know what to save and how often to save it

You should save everything in your system as often as possible. You may not be prepared to recover from a site loss or certain types of disk failures if you do not regularly save everything. If you save the right parts of your iSeries server, then you can recover to point 4 (the last save) shown in backup and recovery timeline. You should save the parts of your system that change often daily. Every week, you should save the parts of your system that do not change often.

### Parts of your system that change often

This table shows the parts of the system that change often, and so should be saved daily:

Table 1. What to save daily: Parts of the system that change often

Item Description	IBM®- Supplied?	When Changes Occur
Security information (user profiles, private authorities, authorization lists)	Some	Regularly as new users and objects are added or authorities are changed <sup>1</sup>
Configuration objects in QSYS	No	Regularly, when device descriptions are added or changed or when you use the Hardware Service Manager function to update configuration information <sup>1</sup>
IBM-supplied libraries that contain user data (QGPL, QUSRSYS)	Yes	Regularly
User libraries that contain user data and programs	No	Regularly
Folders and documents	Some	Regularly, if you use these objects
Distributions	No	Regularly, if you use the distribution function
User directories	No	Regularly

<sup>1</sup> These objects may also change when you update licensed programs.

### Parts of your system that do not change often

This table shows the parts of the system that do not change often; you can save these on a weekly basis.

Table 2. What to save weekly: Parts of the system that do not change often

Item Description	IBM- Supplied?	When Changes Occur
Licensed Internal Code	Yes	PTFs or new release of the operating system
Operating system objects in QSYS library	Yes	PTFs or new release of the operating system
Operating System/400 optional libraries (QHLPSYS, QUSRTOOL)	Yes	PTFs or new release of the operating system
Licensed program libraries (QRPGL, QCBL, Qxxxx)	Yes	Updates to licensed programs
Licensed program folders (Qxxxxxxx)	Yes	Updates to licensed programs
Licensed program directories (/QIBM/ProdData, /QOpenSys/QIBM/ProdData)	Yes	Updates to licensed programs



---

## Chapter 3. Find your save window

Realistically, when you run save procedures, how you run save procedures and what you save depend on the size of your save window. Your **save window** is the amount of time that your system can be unavailable to users while you perform your save operations. To simplify your recovery, you need to save when your system is at a known point and your data is not changing.

When you select a save strategy, you should balance what your users think is an acceptable save window with the value of the data you might lose and the amount of time it may take to recover.

If your system is so critical to your business that you do not have a manageable save window, you probably cannot afford an unscheduled outage either. You should seriously evaluate all the availability options of the iSeries server, including clusters. The Availability roadmap for your iSeries server topic has more information about availability options.

Choose one of the following save strategies, based on the size of your save window. Then reevaluate your decision based on how your save strategy positions you for a recovery.

- **Simple save strategy**  
You have a long save window, which means that you have an 8- to 12-hour block of time available daily with no system activity (including batch work).
- **Medium save strategy**  
You have a medium save window, which means that you have a shorter block of time (4 to 6 hours) available daily with no system activity.
- **Complex save strategy**  
You have a short save window, which means that there is little or no time when your system is not being used for interactive or batch work.

---

### Simple save strategy

The simplest save strategy is to save everything every night (or off-shift hours). You can use option 21 (Entire system) from the Save menu to do this. You can schedule option 21 to run without an operator (unattended) beginning at a certain time.

You can also use this method to save your entire system after you upgrade to a new release or apply program temporary fixes (PTFs).

You may find that you do not have enough time or enough tape unit capability to run option 21 without an operator. You can still employ a simple strategy:

Daily	Save everything that changes often.
Weekly	Save the things that do not change often.

Option 23 (All user data) on the Save menu saves the things that change regularly. Option 23 can be scheduled to run unattended. To run unattended, you must have enough online backup media capacity.

If your system has a long period of inactivity on the weekend, your save strategy might look like this:

Friday night	Save menu option 21
Monday night	Save menu option 23
Tuesday night	Save menu option 23
Wednesday night	Save menu option 23
Thursday night	Save menu option 23
Friday night	Save menu option 21

---

## Medium save strategy

You may find that you do not have a long enough save window to use a simple save strategy. Perhaps you run large batch jobs on your system at night. Or, you have very large files that take a long time to save. If this is the case, you may need to develop a medium save strategy, which means that the complexity for saving and for recovery is medium.

When developing a medium save strategy, apply this principle: the more often it changes, the more often you should save it. You just need to be more detailed in evaluating how often things change than when you use a simple strategy.

Several techniques are available to use in a medium save strategy. You may use one of them or a combination.

- Save changed objects
- Journal objects and save the journal receivers

### Save changed objects

You can use several commands to save only information that has changed since the last save operation or since a particular date and time.

You can use the Save Changed Objects (SAVCHGOBJ) command to save only those objects that have changed since a library or group of libraries was last saved. This can be particularly useful in a situation where programs and data files are in the same library. Typically, data files change frequently and programs change infrequently. You can use the SAVCHGOBJ command to save only the files that change.

You can use the Save Document Library Object (SAVDLO) command to save only documents and folders that have changed. Likewise, you can use the Save (SAV) command to save objects in directories that have changed since a particular point.

You might also choose to save changed objects if your batch work load is heavier some nights. For example:

Day	Batch Workload	Save Operation
Friday night	Light	Save menu option 21
Monday night	Heavy	Save changes only <sup>1</sup>
Tuesday night	Light	Save menu option 23
Wednesday night	Heavy	Save changes only <sup>1</sup>
Thursday night	Heavy	Save changes only <sup>1</sup>
Friday night	Light	Save menu option 21

<sup>1</sup> Use a combination of the SAVCHGOBJ, SAVDLO, and SAV commands.

### Journal objects and save journal receivers

If your save operations for database files take too long because your files are large, saving changed objects may not help you. If you have a file member with 100 000 records and 1 record changes, the SAVCHGOBJ command saves the entire file member. In this situation, journaling your database files and saving journal receivers regularly may be a better solution, even though recovery is more complex.

A similar principle applies to integrated file system objects and data areas. If your save operations for integrated file system objects and data areas are taking too long, you may choose to journal the objects to make your save operations more efficient. Saving journal receivers may be a better option.

When you journal objects, the system writes a copy of every change in the object to a journal receiver. When you save a journal receiver, you are saving only the changed portions of the object, not the entire object.

If you journal your objects and have a batch work load that varies, your save strategy might look like this:

Day	Batch Workload	Save Operation
Friday night	Light	Save menu option 21
Monday night	Heavy	Save journal receivers
Tuesday night	Light	Save menu option 23
Wednesday night	Heavy	Save journal receivers
Thursday night	Heavy	Save journal receivers
Friday night	Light	Save menu option 21

#### Notes:

1. To take advantage of the protection that journaling provides, you should detach and save journal receivers regularly. How often you save them depends on the number of journaled changes that occur. Saving journal receivers several times during the day may be appropriate for you. How you save journal receivers depends on whether they are in a separate library. You might use the Save Library (SAVLIB) command or the Save Object (SAVOBJ) command.
2. You must save new objects before you can apply journal entries to the object. If your applications regularly add new objects, you should consider using the SAVCHGOBJ strategy either by itself or in combination with journaling.

The Journal management topic has more information about journaling.

---

## Complex save strategy

A very short save window requires a complex strategy for saving and for recovery. You use the same tools and techniques that are described for a medium save strategy, but at a greater level of detail. For example, you may need to save specific critical files at specific times of the day or week. You may also want to consider using a tool such as Backup Recovery and Media Services for iSeries (BRMS).

Saving your system while it is active is often necessary in a complex save strategy. The save active (SAVACT) parameter is supported on these commands:

- Save Library (SAVLIB)
- Save Object (SAVOBJ)
- Save Changed Objects (SAVCHGOBJ)
- Save Document Library Object (SAVDLO)
- Save (SAV)

If you use save-while-active support, you can significantly reduce the amount of time that files are made unavailable. When the system has established a checkpoint for all objects being saved, the objects can be made available for use. Save-while-active support can be used in combination with journaling and commitment control to simplify the recovery procedure. If you use the \*LIB or \*SYNCLIB values with the SAVACT parameter, you should use journaling to simplify recovery. If you use the \*SYSDFN value with the SAVACT parameter, you must use commitment control if the library you are saving has related database objects. If you choose to use save-while-active support, make sure that you understand the process and monitor how well checkpoints are being established on your system.

You can also reduce the amount of time that files are unavailable by performing save operations on more than one device at a time, or performing **concurrent save operations**. For example, you can save libraries to one device, folders to another device, and directories to third device. Or, you can save different sets of libraries or objects to different devices.

If you are using V4R4 or a later release, you can also use multiple devices simultaneously by performing a **parallel save operation**. To perform a parallel save operation, you need Backup Recovery and Media Services or an application that allows you to create media definition objects.

For more information on save-while-active support, concurrent save operations, and parallel save operations, see the Back up your server information. The Commitment control topic has more detailed information about commitment control. The Journal management topic has more detailed information about journaling.



---

## Chapter 4. Choose availability options

Availability options are a complement to a good save strategy, not a replacement. Availability options can significantly reduce the time it takes you to recover after a failure. In some cases, availability options can prevent you from having to perform a recovery.

To justify the cost of using availability options, you need to understand the following:

- The value your system provides.
- The cost of a scheduled or unscheduled outage.
- What your availability requirements are.

The following are the availability options that you can use to complement your save strategy:

- Journal management lets you recover the changes to objects that have occurred since your last complete save.
- Access path protection lets you re-create the order in which records in a database file are processed.
- Disk pools limit the amount of data you have to recover to the data in the disk pool with the failed unit.
- Device parity protection enables you to reconstruct data that is lost; the system can continue to run while the data is being reconstructed.
- Mirrored protection helps you keep your data available because you have two copies of the data on two separate disk units.
- Clustering lets you maintain some or all data on two systems; the secondary system can take over critical application programs if the primary system fails.

The Availability roadmap for your iSeries server topic contains information that you can use to implement an availability solution on your iSeries server.



---

## Chapter 5. Test your strategy


If your situation requires a medium save strategy or a complex save strategy, it also requires regular review, as follows:

- Are you saving **everything** occasionally?
- What do you need to do to recover to the known point (4) on the backup and recovery timeline?
- Are you using options like journaling or saving changed objects to help you recover to the failure point (5)? Do you know how to recover using those options?
- Have you added new applications? Are the new libraries, folders, and directories being saved?
- Are you saving the IBM-supplied libraries that contain user data (for example QGPL and QUSRSYS)?

**Note:** The Special values for the SAVLIB command topic lists all of the IBM-supplied libraries that contain user data.

- Have you tested your recovery?

The best way to test your strategy for saving is to test a recovery. Although you can test a recovery on your own system, doing so can be risky. If you have not saved everything successfully, you may lose information when you attempt to restore.

A number of organizations offer recovery testing as a service. IBM Continuity and Recovery Services  is one organization that can assist you with recovery testing.



---

## Chapter 6. Disaster recovery plan—template

The objective of a disaster recovery plan is to ensure that you can respond to a disaster or other emergency that affects information systems and minimize the effect on the operation of the business. This topic provides you with guidelines for the kind of information and procedures that you need to recover from a disaster. When you have prepared the information described in this topic, store your document in a safe, accessible location off site.

Here is a template to use as you create your disaster recovery plan. You can browse this template here; to print it, download and print the PDF file for this topic.

---

### Disaster Recovery Plan

#### Section 1. Major goals of this plan

The major goals of this plan are the following:

- To minimize interruptions to the normal operations.
- To limit the extent of disruption and damage.
- To minimize the economic impact of the interruption.
- To establish alternative means of operation in advance.
- To train personnel with emergency procedures.
- To provide for smooth and rapid restoration of service.

#### Section 2. Personnel

Data processing personnel			
Name	Position	Address	Telephone

**Note:** Attach a copy of your organization chart to this section of the plan.

#### Section 3. Application profile

Use the Display Software Resources (DSPSFWRSC) command to complete this table.

Application profile				
Application Name	Critical? Yes/No	Fixed Asset? Yes/No	Manufacturer	Comments
<b>Comment legend:</b>				
1. Runs daily_____.				
2. Runs weekly on _____.				
3. Runs monthly on _____.				

#### Section 4. Inventory profile

Use the Work with Hardware Products (WRKHDWPRD) command to complete this table. This list should include the following:

- Processing units
- Disk units
- Models
- Workstation controllers
- Personal computers
- Spare workstations
- Telephones
- Air conditioner or heater
- System printer
- Tape and diskette units
- Controllers
- I/O processors
- General data communication
- Spare displays
- Racks
- Humidifier or dehumidifier

Inventory profile					
Manufacturer	Description	Model	Serial Number	Own or Leased	Cost

Inventory profile					
Manufacturer	Description	Model	Serial Number	Own or Leased	Cost
<b>Note:</b> This list should be audited every _____ months.					

Miscellaneous inventory		
Description	Quantity	Comments
<b>Note:</b> This list should include the following: <ul style="list-style-type: none"> <li>• Tapes</li> <li>• PC software (such as DOS)</li> <li>• File cabinet contents or documentation</li> <li>• Tape vault contents</li> <li>• Diskettes</li> <li>• Emulation packages</li> <li>• Language software (such as COBOL and RPG)</li> <li>• Printer supplies (such as paper and forms)</li> </ul>		

### Section 5. Information services backup procedures

- iSeries Server
  - Daily, journal receivers are changed at \_\_\_\_\_ and at \_\_\_\_\_.
  - Daily, a save of changed objects in the following libraries and directories is done at \_\_\_\_\_:
    - \_\_\_\_\_
    - \_\_\_\_\_
    - \_\_\_\_\_
    - \_\_\_\_\_
    - \_\_\_\_\_
    - \_\_\_\_\_
    - \_\_\_\_\_
    - \_\_\_\_\_

This procedure also saves the journals and journal receivers.

- On \_\_\_\_\_ (day) at \_\_\_\_\_ (time) a complete save of the system is done.
- All save media is stored off-site in a vault at \_\_\_\_\_ (location).
- Personal Computer
  - It is recommended that all personal computers be backed up. Copies of the personal computer files should be uploaded to the server on \_\_\_\_\_ (date) at \_\_\_\_\_ (time), just before a complete save of the system is done. It is then saved with the normal system save procedure. This provides for a more secure backup of personal computer-related systems where a local area disaster could wipe out important personal computer systems.

### Section 6. Disaster recovery procedures

For any disaster recovery plan, the following three elements should be addressed.

## **Emergency Response Procedures**

To document the appropriate emergency response to a fire, natural disaster, or any other activity in order to protect lives and limit damage.

## **Backup Operations Procedures**

To ensure that essential data processing operational tasks can be conducted after the disruption.

## **Recovery Actions Procedures**

To facilitate the rapid restoration of a data processing system following a disaster.

### ***Disaster action checklist***

1. Plan Initiation
  - a. Notify senior management
  - b. Contact and set up disaster recovery team
  - c. Determine degree of disaster
  - d. Implement proper application recovery plan dependent on extent of disaster (see Section 7. Recovery plan—mobile site)
  - e. Monitor progress
  - f. Contact backup site and establish schedules
  - g. Contact all other necessary personnel—both user and data processing
  - h. Contact vendors—both hardware and software
  - i. Notify users of the disruption of service
2. Follow-Up Checklist
  - a. List teams and tasks of each
  - b. Obtain emergency cash and set up transportation to and from backup site, if necessary
  - c. Set up living quarters, if necessary
  - d. Set up eating establishments, as required
  - e. List all personnel and their telephone numbers
  - f. Establish user participation plan
  - g. Set up the delivery and the receipt of mail
  - h. Establish emergency office supplies
  - i. Rent or purchase equipment, as needed
  - j. Determine applications to be run and in what sequence
  - k. Identify number of workstations needed
  - l. Check out any off-line equipment needs for each application
  - m. Check on forms needed for each application
  - n. Check all data being taken to backup site before leaving and leave inventory profile at home location
  - o. Set up primary vendors for assistance with problems incurred during emergency
  - p. Plan for transportation of any additional items needed at backup site
  - q. Take directions (map) to backup site
  - r. Check for additional magnetic tapes, if required
  - s. Take copies of system and operational documentation and procedural manuals.
  - t. Ensure that all personnel involved know their tasks
  - u. Notify insurance companies

### ***Recovery start-up procedures for use after a disaster***

1. Notify \_\_\_\_\_ Disaster Recovery Services of the need to utilize service and of recovery plan selection.



**Note:** Guaranteed delivery time countdown begins at the time \_\_\_\_\_ is notified of recovery plan selection.

- a. Disaster notification numbers

\_\_\_\_\_ or \_\_\_\_\_

These telephone numbers are in service from \_\_\_\_\_ am until \_\_\_\_\_ pm Monday through Friday.

2. Disaster notification number: \_\_\_\_\_

This telephone number is in service for disaster notification after business hours, on weekends, and during holidays. Please use this number only for the notification of the actual disaster.

3. Provide \_\_\_\_\_ with an equipment delivery site address (when applicable), a contact, and an alternate contact for coordinating service and telephone numbers at which contacts can be reached 24 hours a day.
4. Contact power and telephone service suppliers and schedule any necessary service connections.
5. Notify \_\_\_\_\_ immediately if any related plans should change.

### **Section 7. Recovery plan—mobile site**

1. Notify \_\_\_\_\_ of the nature of the disaster and the need to select the mobile site plan.
2. Confirm in writing the substance of the telephone notification to \_\_\_\_\_ within 48 hours of the telephone notification.
3. Confirm all needed backup media are available to load the backup machine.
4. Prepare a purchase order to cover the use of backup equipment.
5. Notify \_\_\_\_\_ of plans for a trailer and its placement (on \_\_\_\_\_ side of \_\_\_\_\_). (See the Mobile site setup plan in this section.)
6. Depending on communication needs, notify telephone company (\_\_\_\_\_) of possible emergency line changes.
7. Begin setting up power and communications at \_\_\_\_\_.
  - a. Power and communications are prearranged to hook into when trailer arrives.
  - b. At the point where telephone lines come into the building (\_\_\_\_\_), break the current linkage to the administration controllers (\_\_\_\_\_). These lines are rerouted to lines going to the mobile site. They are linked to modems at the mobile site.

The lines currently going from \_\_\_\_\_ to \_\_\_\_\_ would then be linked to the mobile unit via modems.
  - c. This could conceivably require \_\_\_\_\_ to redirect lines at \_\_\_\_\_ complex to a more secure area in case of disaster.
8. When the trailer arrives, plug into power and do necessary checks.
9. Plug into the communications lines and do necessary checks.
10. Begin loading system from backups (see Section 9. Restoring the Entire System).
11. Begin normal operations as soon as possible:
  - a. Daily jobs
  - b. Daily saves
  - c. Weekly saves
12. Plan a schedule to back up the system in order to restore on a home-base computer when a site is available. (Use regular system backup procedures).
13. Secure mobile site and distribute keys as required.
14. Keep a maintenance log on mobile equipment.

### **Mobile site setup plan**

Attach the mobile site setup plan here.

### ***Communication disaster plan***

Attach the communication disaster plan, including the wiring diagrams.

### ***Electrical service***

Attach the electrical service diagram here.

## **Section 8. Recovery plan—hot site**

The disaster recovery service provides an alternate hot site. The site has a backup system for temporary use while the home site is being reestablished.

1. Notify \_\_\_\_\_ of the nature of the disaster and of its desire for a hot site.
2. Request air shipment of modems to \_\_\_\_\_ for communications. (See \_\_\_\_\_ for communications for the hot site.)
3. Confirm in writing the telephone notification to \_\_\_\_\_ within 48 hours of the telephone notification.
4. Begin making necessary travel arrangements to the site for the operations team.
5. Confirm that all needed tapes are available and packed for shipment to restore on the backup system.
6. Prepare a purchase order to cover the use of the backup system.
7. Review the checklist for all necessary materials before departing to the hot site.
8. Make sure that the disaster recovery team at the disaster site has the necessary information to begin restoring the site. (See Section 12. Disaster site rebuilding).
9. Provide for travel expenses (cash advance).
10. After arriving at the hot site, contact home base to establish communications procedures.
11. Review materials brought to the hot site for completeness.
12. Begin loading the system from the save tapes.
13. Begin normal operations as soon as possible:
  - a. Daily jobs
  - b. Daily saves
  - c. Weekly saves
14. Plan the schedule to back up the hot-site system in order to restore on the home-base computer.

### ***Hot-site system configuration***

Attach the hot-site system configuration here.

## **Section 9. Restoring the entire system**

To get your system back to the way it was before the disaster, use the procedures on recovering after a complete system loss in the *Backup and Recovery*, SC41-5304-06.

*Before You Begin:* Find the following tapes, equipment, and information from the on-site tape vault or the off-site storage location:

- If you install from the alternate installation device, you need both your tape media and the CD-ROM media containing the Licensed Internal Code.
- All tapes from the most recent complete save operation
- The most recent tapes from saving security data (SAVSECDTA or SAVSYS)
- The most recent tapes from saving your configuration, if necessary
- All tapes containing journals and journal receivers saved since the most recent daily save operation
- All tapes from the most recent daily save operation
- PTF list (stored with the most recent complete save tapes, weekly save tapes, or both)
- Tape list from most recent complete save operation
- Tape list from most recent weekly save operation
- Tape list from daily saves
- History log from the most recent complete save operation
- History log from the most recent weekly save operation
- History log from the daily save operations
- The *Software Installation* book
- The *Backup and Recovery* book
- Telephone directory
- Modem manual
- Tool kit

### **Section 10. Rebuilding process**

The management team must assess the damage and begin the reconstruction of a new data center.

If the original site must be restored or replaced, the following are some of the factors to consider:

- What is the projected availability of all needed computer equipment?
- Will it be more effective and efficient to upgrade the computer systems with newer equipment?
- What is the estimated time needed for repairs or construction of the data site?
- Is there an alternative site that more readily could be upgraded for computer purposes?

Once the decision to rebuild the data center has been made, go to Section 12. Disaster site rebuilding.

### **Section 11. Testing the disaster recovery plan**

In successful contingency planning, it is important to test and evaluate the plan regularly. Data processing operations are volatile in nature, resulting in frequent changes to equipment, programs, and documentation. These actions make it critical to consider the plan as a changing document. Use these checklists as you conduct your test and decide what areas should be tested.

*Table 3. Conducting a recovery test*

Item	Yes	No	Applicable	Not Applicable	Comments
Select the purpose of the test. What aspects of the plan are being evaluated?					
Describe the objectives of the test. How will you measure successful achievement of the objectives?					

Table 3. Conducting a recovery test (continued)

Item	Yes	No	Applicable	Not Applicable	Comments
Meet with management and explain the test and objectives. Gain their agreement and support.					
Have management announce the test and the expected completion time.					
Collect test results at the end of the test period.					
Evaluate results. Was recovery successful? Why or why not?					
Determine the implications of the test results. Does successful recovery in a simple case imply successful recovery for all critical jobs in the tolerable outage period?					
Make recommendations for changes. Call for responses by a given date.					
Notify other areas of results. Include users and auditors.					
Change the disaster recovery plan manual as necessary.					

Table 4. Areas to be tested

Item	Yes	No	Applicable	Not Applicable	Comments
Recovery of individual application systems by using files and documentation stored off-site.					
Reloading of system tapes and performing an IPL by using files and documentation stored off-site.					
Ability to process on a different computer.					
Ability of management to determine priority of systems with limited processing.					
Ability to recover and process successfully without key people.					
Ability of the plan to clarify areas of responsibility and the chain of command.					
Effectiveness of security measures and security bypass procedures during the recovery period.					
Ability to accomplish emergency evacuation and basic first-aid responses.					
Ability of users of real-time systems to cope with a temporary loss of on-line information.					
Ability of users to continue day-to-day operations without applications or jobs that are considered noncritical.					
Ability to contact the key people or their designated alternates quickly.					
Ability of data entry personnel to provide the input to critical systems by using alternate sites and different input media.					

Table 4. Areas to be tested (continued)

Item	Yes	No	Applicable	Not Applicable	Comments
Availability of peripheral equipment and processing, such as printers and scanners.					
Availability of support equipment, such as air conditioners and dehumidifiers.					
Availability of support: supplies, transportation, communication.					
Distribution of output produced at the recovery site.					
Availability of important forms and paper stock.					
Ability to adapt plan to lesser disasters.					

### Section 12. Disaster site rebuilding

- Floor plan of data center.
- Determine current hardware needs and possible alternatives. (See Section 4. Inventory profile.)
- Data center square footage, power requirements and security requirements.
  - Square footage \_\_\_\_\_
  - Power requirements \_\_\_\_\_
  - Security requirements: locked area, preferably with combination lock on one door.
  - Floor-to-ceiling studding
  - Detectors for high temperature, water, smoke, fire and motion
  - Raised floor

### Vendors

### Floor plan

Include a copy of the proposed floor plan here.

### Section 13. Record of plan changes

Keep your plan current. Keep records of changes to your configuration, your applications, and your backup schedules and procedures. For example, you can get print a list of your current local hardware, by typing:

```
DSPLCLHDW OUTPUT(*PRINT)
```

---

## Image description

The description for the timeline image is as follows:

1. Point 1: Known point (last save). Activity occurs on system.
2. Point 2: Failure occurs. Hardware repair or IPL occurs.
3. Point 3: Hardware is available. Information is restored from backup.
4. Point 4: System is recovered to known point 1. Transactions from point 1 to point 2 are recovered.
5. Point 5: System is recovered to failure point 2. Business activity from failure point 2 to recovery point 5 is recovered.
6. Point 6: System is current.





Printed in U.S.A.