System i

Systems management
Planning a backup and recovery strategy

Version 5 Release 4

System i

Systems management
Planning a backup and recovery strategy

Version 5 Release 4

Note

Before using this information and the product it supports, read the information in "Notices," on page 19.

Seventh Edition (February 2006)

This edition applies to version 5, release 4, modification 0 of IBM i5/OS (product number 5722-SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

Contents

Planning a backup and recovery strategy

If you lose information on your system, you need to use your backup copies of the information. This topic collection contains information about how to plan your strategy and make the choices you need to set up your system for backup, recovery, and availability.

The IBM® System i™ products are very reliable. You might 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 the computer problems decreases, the potential impact of the problems increases. Businesses are becoming more dependent on computers and the information that is stored in them. The information that is in your computer might 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 on planning and evaluating it?

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

After you study the backup and recovery timeline, you can start to plan your strategy by following these steps:

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

Related concepts

Backing up your system

Availability roadmap

Related information

Backup and recovery frequently asked questions

Backup and recovery

Printable PDF

Use this to view and print a PDF of this information.

To view or download the PDF version of this document, select Planning a backup and recovery strategy (about 317 KB).

Saving PDF files

To save a PDF on your workstation for viewing or printing:

1. Right-click the PDF in your browser (right-click the link above).
2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe Reader

You need Adobe Reader installed on your system to view or print these PDFs. You can download a free copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html) .

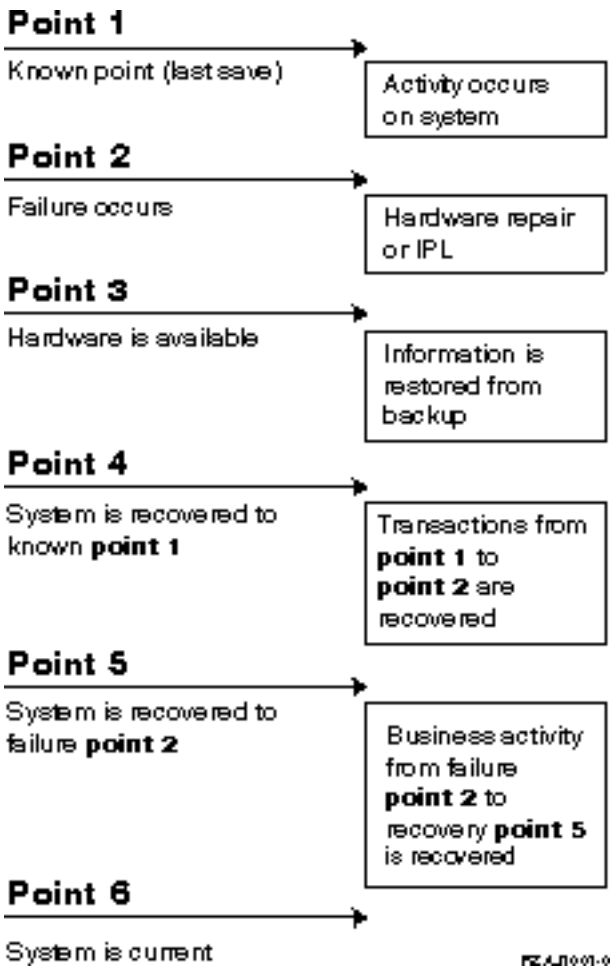
Backup and recovery timeline

The timeline for backup and recovery begins when you save the information and ends when your system is fully recovered after a failure.

Refer to this timeline as you read this information and make the decisions. Your strategies for saving and availability determine these things:

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

Use the following timeline to develop specific examples. What if the known point (1) is Sunday evening and the failure point (2) is Thursday afternoon? How long does it take to get back to the known point? How long does it take you to get to the current point (6)? Is it even possible with the save strategy that you have planned?



Here is the descriptions for the timeline image:

- Point 1: Known point (last save). Activity occurs on system.
- Point 2: Failure occurs. Hardware repair or initial program load (IPL) occurs.
- Point 3: Hardware is available. Information is restored from backup.

- Point 4: System is recovered to known point 1. Transactions from point 1 to point 2 are recovered.
- Point 5: System is recovered to failure point 2. Business activity from failure point 2 to recovery point 5 is recovered.
- Point 6: System is current.

Related concepts

"Testing your strategy" on page 8
If your situation requires a medium save strategy or a complex save strategy, it requires regular review.

Related reference

"Knowing what to save and how often to save it"
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.

Knowing what to save and how often to save it

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.

You cannot 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 system, you can recover to point 4 (the last save) that is shown in the backup and recovery timeline.

Parts of your system that change often

This table shows the parts of the system that change often and need to be saved daily.

Table 1. What to save daily

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[1]
Configuration objects in QSYS	No	Regularly, when device descriptions are added or changed, or when you use the Hardware Service Manager function to update the configuration information[1]
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

[1] These objects might also be changed when you update the 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

Item description	IBM-supplied?	When changes occur
Licensed Internal Code (LIC)	Yes	Program temporary fixes (PTFs) or new release of the operating system

Table 2. What to save weekly (continued)

Item description	IBM-supplied?	When changes occur
Operating system objects in QSYS library	Yes	PTFs or new release of the operating system
IBM i5/OS® optional libraries (QHLPSYS, QUSRTOOL)	Yes	PTFs or new release of the operating system
Licensed program libraries (QRPG, QCBL, Qxxxx)	Yes	Updates to the licensed programs
Licensed program folders (Qxxxxxxx)	Yes	Updates to the licensed programs
Licensed program directories (/QIBM/ProdData, /QOpenSys/QIBM/ProdData)	Yes	Updates to the licensed programs

Related concepts

"Backup and recovery timeline" on page 2
The timeline for backup and recovery begins when you save the information and ends when your system is fully recovered after a failure.

Related reference

"Simple save strategy"
You have a long save window, which means that you have an 8-hour to a 12-hour block of time available daily with no system activity (including batch work). The simplest save strategy is to save everything every night or during off-shift hours.

Finding your save window

When you run save procedures, how you run save procedures and what you save depend on the size of your save window.

A *save window* is the amount of time that your system cannot be available to users while you perform the 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 that you might lose and the amount of time that it might 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 system, including clusters.

Based on the size of your save window, choose one of the following save strategies: simple, medium, or complex save strategy. Then reevaluate your decision based on how your save strategy positions you for a recovery.

Related concepts

Availability roadmap

Simple save strategy

You have a long save window, which means that you have an 8-hour to a 12-hour block of time available daily with no system activity (including batch work). The simplest save strategy is to save everything every night or during 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 might 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 capacities.

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

Related reference

"Knowing what to save and how often to save it" on page 3
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.

Medium save strategy

You have a medium save window, which means that you have a 4-hour to 6-hour block of time available daily with no system activity. Use this strategy if you find that you do not have a long-enough save window to use a simple save strategy.

If you run large batch jobs on your system at nights or you have very large files that take a long time to save. You might 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.

The following techniques are available to use in a medium save strategy. You can use one of them or a combination:

- Saving changed objects.
- Journaling objects and saving the journal receivers.

Saving 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 a group of libraries is 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 the documents and the folders that have changed. Likewise, you can use the Save (SAV) command to save the objects in directories that have changed since a particular point.

You can also choose to save the changed objects if your batch workload is heavier some nights. For example:

Day	Batch workload	Save operation
Friday night	Light	Save menu option 21
Monday night	Heavy	Save changes only[1]
Tuesday night	Light	Save menu option 23
Wednesday night	Heavy	Save changes only[1]
Thursday night	Heavy	Save changes only[1]
Friday night	Light	Save menu option 21

[1] Use a combination of the SAVCHGOBJ, SAVDLO, and SAV commands.

Journaling objects and saving journal receivers

If your save operations for integrated file system objects and data areas are taking too long, you can choose to journal the objects to make your save operations more efficient.

If you have a file member with 100 000 records and 1 record changes, the Save Changed Objects (SAVCHGOBJ) command saves the entire file member. In this situation, journaling your database files and saving journal receivers regularly might be a better solution, even though recovery is more complex.

A similar principle applies to the integrated file system objects and data areas. Saving journal receivers might be a better option.

When you journal the 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:

Table 3. Example save strategy

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:

- 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 might be appropriate for you. How you save journal receivers depends on whether they are in a separate library. You can use the Save Library (SAVLIB) command or the Save Object (SAVOBJ) command.
- 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.

Related concepts

Journal management

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. 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 need to save specific critical files at specific times of the day or week. You also want to consider using Backup, Recovery, and Media Services (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 establishes a checkpoint for all the objects being saved, the objects can be made available for use. You can use save-while-active commands 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 by 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.

You can also use multiple devices simultaneously by performing a parallel save operation. To perform a parallel save operation, you need BRMS or an application that allows you to create the media definition objects.

Related concepts

Backup, Recovery, and Media Services (BRMS)

Save-while-active and your backup and recovery strategy

Saving to multiple devices to reduce your save window

Backing up your system

Commitment control

Journal management

Choosing availability options

Availability options are complements to a good save strategy, not replacements. Availability options can significantly reduce the time that it takes you to recover after a failure. In some cases, availability options can prevent you from performing a recovery.

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

- The value that your system provides.
- The cost of a scheduled or an unscheduled outage.
- The type of your availability requirements.

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

- Journal management enables you to recover the changes to objects that have occurred since your last complete save.
- Access path protection enables you to recreate the order in which records in a database file are processed.
- Disk pools limit the amount of data you need to recover to the data in the disk pool with the failed unit.
- Device parity protection enables you to reconstruct the 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 enables you to maintain some or all data on two systems. The secondary system can take over critical application programs if the primary system fails.

Related concepts

Availability roadmap

Related reference

Special values for the SAVLIB command

Testing your strategy

If your situation requires a medium save strategy or a complex save strategy, it requires regular review.

The regular review is 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, it is very risky. If you do not save everything successfully, you might lose information when you attempt to restore.

A number of organizations offer recovery testing as a service. Business continuity and resiliency is one organization that helps you with the recovery testing.

Related concepts

"Backup and recovery timeline" on page 2
The timeline for backup and recovery begins when you save the information and ends when your system is fully recovered after a failure.

Planning disaster recovery

These guidelines contain the information and procedures that you need to recover from a disaster.

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 can minimize the effect on the operation of the business. When you have prepared the information described in this topic, store your document in a safe and accessible location off site.

Disaster recovery plan

This topic contains a template to use when you create a disaster recovery plan.

Section 1. Major goals of this plan

The following list contains the major goals of this plan:

- To minimize the 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

Table 4. 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.

Table 5. Application profile

Application profile				
Application name	**Critical? Yes/No**	**Fixed asset? Yes/No**	**Manufacturer**	**Comments**

Comment legend:

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 items:

- 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

Table 6. Inventory profile

Inventory profile					
Manufacturer	**Description**	**Model**	**Serial number**	**Own or leased**	**Cost**

Table 6. Inventory profile (continued)

Inventory profile					
Manufacturer	**Description**	**Model**	**Serial number**	**Own or leased**	**Cost**
Note: This list should be audited every _____ months.					

Table 7. Miscellaneous inventory

Miscellaneous inventory		
Description	**Quantity**	**Comments**
Note: This list includes the following items: • Tapes • PC software • File cabinet contents or documentation • Tape vault contents • Diskettes • Emulation packages • Programming language software • Printer supplies (such as paper and forms)		

Section 5. Information services backup procedures

- i5/OS operating system
  - Daily: Journal receivers are changed at _____ and at _____.
  - Daily: Changed objects in the following libraries and directories are saved at _____:
    - _____
    - _____
    - _____
    - _____
    - _____
    - _____
    - _____
    - _____

    This procedure also saves the journals and journal receivers.
  - On _____ (day) at _____ (time) a complete save operation of the system is done.
  - All save media is stored off site in a vault at _____ (location).
- Personal computer
  - It is suggested that all personal computers be backed up. The copies of the personal computer files should be uploaded to the system on _____ (date) at _____ (time), just before a complete save

operation of the system is done. It is saved with the normal system save procedure. This provides for a more secure backup of personal computer-related systems where a local area disaster can wipe out important personal computer systems.

Section 6. Disaster recovery procedures

For any disaster recovery plans, the following three elements should be addressed:

Emergency response procedures
To document the appropriate emergency response to a fire, natural disaster, or any other activities in order to protect lives and limit damages.

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 the senior management.
   b. Contact and set up a disaster recovery team.
   c. Determine the degree of a disaster.
   d. Implement an appropriate application recovery plan dependent on the extent of the disaster (see "Section 7. Recovery plan–mobile site" on page 13).
   e. Monitor the progress.
   f. Contact the backup sites and establish the 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 the backup site.
   c. Set up the living quarters.
   d. Set up the eating establishments.
   e. List all personnel and their telephone numbers.
   f. Establish the user participation plans.
   g. Set up the delivery and the receipt of mail.
   h. Establish the emergency office supplies.
   i. Rent or purchase the equipment, as needed.
   j. Determine the applications to be run and in what sequence.
   k. Identify the number of workstations that are needed.
   l. Check out any offline equipment needed for each application.
   m. Check on the forms needed for each application.
   n. Check all data being taken to the backup site before leaving, and leave the inventory profile at the home location.
   o. Set up the primary vendors for assistance with problems incurred during emergency.
   p. Plan for transportation of any additional items needed at the backup site.
   q. Take the directions (maps) to backup site.
   r. Check for the additional magnetic tapes.

s. Take copies of the system and operational documentation and procedural manuals.
t. Ensure that all personnel involved know their tasks.
u. Notify the 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 _____ a.m. until _____ p.m. 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 need to be changed.

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 the 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 the 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 the lines going to the mobile site. They are linked to the modems at the mobile site.

      The lines currently going from _____ to _____ is linked to the mobile unit via modems.
   c. This might conceivably require _____ to redirect lines at _____ complex to a more secure area in case of disasters.
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” on page 14).
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-based computer when a site is available. (Use regular system backup procedures).
13. Secure the mobile site and distribute the 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" on page 17).
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-based 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 Systems management: Backup and recovery.

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.
- All tapes containing journals and journal receivers saved since the most recent daily save operation.
- All tapes from the most recent daily save operation.
- Program temporary fix (PTF) list (stored with the most recent complete save tapes, weekly save tapes, or both).
- Tape list from the most recent complete save operation.
- Tape list from the 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 Installing, upgrading, or deleting i5/OS and related software topic collection.
- The Systems management: Backup and recovery topic collection.
- 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, you need to consider the following factors:

- What is the projected availability of all needed computer equipment?
- Is 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 can be upgraded for computer purposes?

After the decision to rebuild the data center is made, go to “Section 12. Disaster site rebuilding” on page 17.

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 your conduct, your test, and decide what areas should be tested.

Table 8. 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 do you measure successful achievement of the objectives?					

Table 8. 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 the test results at the end of the test period.					
Evaluate the results. Is recovery successful? Why or why not?					
Determine the implications of the test results. Does the successful recovery in a simple case imply the 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 9. 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 initial program load (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 online 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 9. 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 supports: supplies, transportation, and 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 the data center.
- Determine the current hardware needs and possible alternatives. (See "Section 4. Inventory profile" on page 10.)
- 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 current plan. Keep records of changes to your configuration, your applications, and your backup schedules and procedures. For example, you can print a list of your current local hardware by typing:

```
DSPHDWRSC OUTPUT(*PRINT)
```

Related information

Display Hardware Resources (DSPHDWRSC)

Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information about the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Programming Interface Information

This Planning a backup and recovery strategy publication documents intended Programming Interfaces that allow the customer to write programs to obtain the services of IBM i5/OS.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

| IBM
| IBM (logo)
| System i
| i5/OS

Other company, product, and service names may be trademarks or service marks of others.

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED ″AS-IS″ AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Printed in USA