1-1-1994

Computer disaster recovery planning guide

American Institute of Certified Public Accountants. Information Technology Division

INFORMATION TECHNOLOGY DIVISION

Computer Disaster Recovery Planning Guide

PRACTICE AID

AICPA

American Institute of Certified Public Accountants

Notice to Readers

This practice aid is one of a series of aids that provide accounting professionals with information about the implementation of a particular technology. These aids are issued by the AICPA Information Technology Division for the benefit of Information Technology Section members. This aid does not establish standards or preferred practice; it represents the opinion of the author and does not necessarily reflect the policies of the AICPA or the Information Technology Division.

The Information Technology Division expresses its appreciation to the author of this practice aid, Christopher J. Leach, CPA, a member of the AICPA Information Technology Executive Committee.

Various members of the 1992–1993 AICPA Information Technology Executive Committee were involved in the preparation of this technology bulletin. The members of the committee are listed below:

Michael W. Harnish, *Chairman*
Steven W. Bare
L. Gary Boomer
Terry L. Campbell
David J. Duray
Philip H. Friedlander
Donald W. Hunt
James C. Kinard
Christopher J. Leach
Robert R. Moeller
Amy Chen Pierce
William L. Reeb
Philip J. Scissors
Larry J. Wolfe
Robert C. Wynne

Richard D. Walker, *Director*
Information Technology Division

Nancy A. Cohen, *Technical Manager*
Information Technology Membership Section

INFORMATION TECHNOLOGY DIVISION

Computer Disaster Recovery Planning Guide

PRACTICE AID

AICPA

American Institute of Certified Public Accountants

1 2 3 4 5 6 7 8 9 0 IT 9 9 8 7 6 5 4

Library of Congress Cataloging-in-Publication Data
Computer disaster recovery planning guide / Information Technology
Division.
p. cm.
ISBN 0–87051–147–5
1. Data recovery (Computer science) I. American Institute of
Certified Public Accountants. Information Technology Division.
QA76.9.D348C66 1994
658.4'78—dc20 93-50783
CIP

Table of Contents

1. **Disaster Recovery Planning** 1

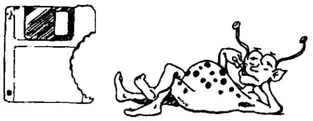
Introduction 1
General Office/Personnel Procedures 1
General Disaster Recovery Committee Guidelines 2
Vital Information Loss 2
Tape Backup Procedures 3
Tape Rotation 4
Virus Protection Software 5
Common Virus Infections 7
Telephone Protection 8

2. **Disaster Recovery Checklists** 9

General Checklist 9
Disaster Recovery Committee 10
Emergency Telephone Listing 11
First Aid/CPR Training 12
Equipment Listing 13
Software Listing 14
Insurance Evaluation 15
Backup Control Log 16
Key Vendor Contact List 17
Off-Site Location Worksheet 18
Off-Site Supply Listing 19
Annual Disaster Recovery Meeting Plan 20

Chapter 1. Disaster Recovery Planning

Introduction



You know the feeling from movies like *Jaws*. The music starts its slow, mounting rhythm, growing faster and louder until disaster strikes! Ask anyone who was in the San Francisco earthquake, the hurricanes in Florida and Hawaii, or the more recent floods in the Midwest. He or she will most likely tell you that "failure to plan is planning to fail." It is not until after the disaster that you find out how prepared you really are.

Disasters come in all shapes and sizes and can strike at any time with little or no warning. Typically, when we think of a disaster in a business sense, we think of earthquakes, tornadoes, fires, and other acts of nature. But what about the disaster caused by the death of a key employee, or theft of vital data-processing equipment, or even a revolution in a country where a major subsidiary is in operation? The purpose of this document is to direct the professional in a systematic and thoughtful way to anticipate areas where controls can be put in place or strengthened to quickly recover from an unforeseen disaster.

The primary focus of any disaster recovery plan should be to ensure (1) the safety of all employees, (2) the protection of client/customer documents as well as those of the firm, and (3) the safety of office equipment and furniture on the premises. After the status of these items can be verified, the next area of emphasis is to resume normal business operations as soon as possible. In addition, the suggestions in this document are intended to be "proactive" (anticipatory in nature) rather than "reactive."

General Office/ Personnel Procedures

The following are steps to be taken in the recovery process.

1. Appoint a disaster recovery chairperson. Be sure to secure the assistance and participation of senior management in this step. The chairperson will need to be given the proper authority to act in the event of any major disaster.
2. Appoint a disaster recovery committee. This committee should represent the various disciplines within the office. The committee, acting under the direction of the chairperson, should meet and determine the strengths and weaknesses in each area of the office.
3. Prepare a list of the appropriate emergency telephone numbers and distribute it to each employee. Be sure to include police, fire, medical emergency and utility company telephone numbers.
4. Arrange a cardiopulmonary resuscitation (CPR) demonstration and first aid course. Contact your local Red Cross for assistance. If an in-office demonstration is not possible, send two or three employees, from different departments and shifts, to receive this training.
5. Have an annual company disaster plan meeting. During this meeting, company employees should be briefed on the procedures they are to take in the event of a disaster. If possible, a fire or earthquake drill should be a part of this meeting.

6. Maintain adequate insurance on office equipment, software, and key employees. Many companies have added insurance to cover the loss of data and business interruption in the event of a natural disaster, but overlook that some of the most important assets, key employees, are not insured at all.
7. Maintain a current list of data processing hardware and software. This list is important for insurance purposes, and will assist the company in preparing for the contingency of off-site processing.
8. Perform routine backups of data files, and periodically test the backup media.
9. Develop a relationship with a local hardware vendor. Many vendors are willing to provide quick "loaner" hardware in the event of a disaster at little or no cost. Such a relationship can speed recovery from hardware failure or loss.
10. Locate two or three possible areas off the premises where temporary operations could resume for a limited time in the event of a disaster. This location could be in a mobile trailer, hotel room, or other suitable location.

General Disaster Recovery Committee Guidelines

- The committee should have a current copy of the employee list, complete with names, home addresses, and telephone numbers. This list should be updated each time there is a change in any employee record.
- Employees should be acquainted with each member of the disaster recovery committee, and how to contact them in case of emergency. This could be accomplished by telephone or in the event of phone or power failure, by reporting to a designated location.
- Disaster recovery committee members should maintain a current "contact" list. This list is a list of outside sources whose services would be utilized in the disaster recovery process (for example, computer vendors and the telephone company).
- The committee should communicate bimonthly, or more often if necessary. When new computer equipment or additional facilities are acquired, the disaster recovery chairperson should evaluate the need to meet and update the current recovery plan.
- Company employees should be encouraged to note any change in company policy, operation, or facility that would affect the disaster recovery plan and communicate such changes to the disaster recovery committee.

Vital Information Loss

Because many businesses today rely so heavily on information systems and office technology, equipment failure can be crippling. If the facilities are down for even a short time, the continued existence of the company can be jeopardized. Vital information can be lost through equipment theft, malfunction, or destruction. Adequate preparation for data loss must, therefore, be a part of any disaster recovery plan.

Consider the following testimonial to the importance of preparation from the January 1993 *Reader's Digest:* As vice president at Skalny Basket Co., in Springfield, Ohio, a wicker furniture and basket wholesaler, Cheryl Hart keeps tabs on who owes the company money. When Skalny computerized its bookkeeping, it made Hart's work easier, but it also gave her a new chore. Every night before closing she copied the company files onto a tape and *took it home.* She also drilled it into her assistants to back up files when she wasn't there. Still, it was a bother. The copying took a half-hour nightly.

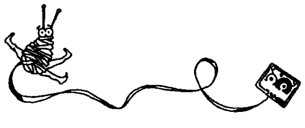
On December 23, 1987, Skalny was finishing its busiest season ever. Hart was out of the building Christmas shopping, but just before the office closed for the long holiday weekend, she stopped to pick up her briefcase. At 3 A.M. the following Monday, a call came from the fire department — Skalny was on fire. Not only was the company inventory destroyed, but all of the computer records of accounts receivable — some $600,000 owed to Skalny — had gone up in smoke. "We thought we were out of business," says Hart.

Then she remembered the computer backup. Had her assistant done it? She rushed to her briefcase and found the tape with all figures up to date.

Established backup procedures, carefully followed, saved the day in this scenario. The following are steps for forming your company's backup procedures.

- Secure computer equipment. This can be accomplished by controlling access to the building after hours. A recent study revealed that most office equipment theft occurs between the hours of 6 A.M. and 8 A.M. Thieves find that, during these hours, office buildings are unlocked for employees who arrive early — but unguarded.
- Back data up daily. This includes programs and operating system software (such as Novell, Unix, and DOS).
- Monitor the tape backup procedures daily to ensure adherence to this policy.
- Maintain a current list of hardware serial numbers and software version numbers. This will assist you in case of loss and insurance claims.
- If equipment is available for checkout by employees, set up and follow a system that tracks the usage and return of this equipment.
- Acquire a fire-rated file cabinet to store and maintain valuable equipment and software. Although the software should be backed up, such a file cabinet provides a good place to store original diskettes and other magnetic media.
- Periodically, run antivirus software and test your data. Test all outside media before placing them on a network or other company computer. Your antivirus software should be the kind that is periodically updated by the software manufacturer. This is of extreme importance as new, more innovative viruses are constantly being created and discovered.

Tape Backup Procedures



Make Full Backups

If at all possible, do a full backup. Most tape backup systems allow you to save only the files that have changed since the last backup. Although this can save time creating the backup, it can make the restoration process a nightmare. For example, if you need to restore information, you will need to restore files from *every* tape since the last full backup.

Also make sure that your programs are backed up. Many people do not back up their programs (for example, your word processing software) because they don't change and because the original diskettes are still available. Even if the original diskettes are handy, reinstalling and reconfiguring the programs can take a lot of time.

Back Up Every Day

Get into the habit of backing up your data every day. If you have a network, the file server is most likely left on all the time. You might as well make it do some work at night. Virtually all tape backup systems allow you to perform backups at a preset time. Depending on the size of your system, the process can take from a few minutes to several hours. A midnight backup will protect data while leaving the system free during business hours.

Test the Backups

A backup procedure may appear to be working properly, but the tape may be found to be blank or to contain unusable data. The only way to be certain that your backups work is to test them on a regular basis. It is also important to understand that magnetic media such as diskettes and tapes do have a "shelf life." Over time, the integrity of a tape will diminish as it is used again and again. Check with the manufacturer to find out the life of your backup media.

Use a Single Tape

Buy a tape system that can hold your entire hard drive(s) on one tape. You will be more likely to back up your system if you can do it all at once. The additional cost of a large tape backup system is justified in the data protection it affords.

Store Backup Tapes Off-Site

Although this seems obvious, and is probably stated in your procedure manual, it is often not done in practice.

Logout Workstations

Network administrators should make sure that all users have logged off the network before the backup process begins. Most tape backup systems are incapable of backing up files that are in use by a workstation.

Back Up Local Drives

If you keep important information on local hard drives (c: or d:), make sure that this data is backed up regularly. It is easy to overlook hard drives on the network. You may be surprised to find what irreplaceable information is there. Some network software such as MAP Assist from Fresh Technology Group in Gilbert, Arizona, allows you to back up local hard drives from the server.

Tape Rotation

There are as many methods used to rotate tape backups as there are tapes. What is important is that (1) backups are performed and (2) a rotation schedule is in place to allow the media to be stored off-site.

Grandfather – father – son

This is one kind of rotation wherein three tapes are used and rotated daily. The first tape (the grandfather) holds Monday's backup, the second tape (the father) holds Tuesday's work, and the third tape (the son) contains Wednesday's files. On Thursday, the oldest tape (the grandfather) becomes the son and Thursday's files are backed up on it. The father tape becomes the grandfather and the son becomes the father. On Friday, the oldest tape once again becomes the son and the cycle repeats itself. By following this rotation scheme, the grandfather and father tapes can be stored off-site. In the event of a disaster and total data loss, a company would only lose one day's information.

Daily Tapes

Under this scenario, a tape is acquired for each daily backup. If an organization is in operation seven days, then seven tapes would be purchased. On Monday, the tape from the previous Monday would be overwritten with the current data. On Tuesday, the previous Tuesday's tape would be used and so on. Once again, the other tapes should be stored off-site.

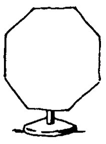
Historical

This system whereby a monthly and/or yearly backup tape is retained for one year is similar to the methodology in the *Daily Tape* schedule described above. This system has the advantage of being able to retrieve information on a schedule that coincides with typical business cycles and accounting periods.

Some companies will keep a permanent monthly or annual backup tape that is not overwritten with new data. These tapes are archived off-site and should be checked for data integrity from time to time. The drawback of this system is no more than the cost of the extra tapes.

Virus Protection Software

The following is a partial list of software vendors who provide virus protection software. It should be noted that this is a very dynamic area. Therefore, the software chosen should be updated on a regular basis by the manufacturer.



Manufacturer	Product Name
Abacus 5370 52 St. Grand Rapids, MI 49512 (616) 698–0330 (800) 451–4319	Virus Secure
Central Point Software 15220 NW Greenbrier Pkwy. #200 Beaverton, OR 97006 (503) 690–8088 (800) 445–4208	Central Point Anti-Virus
The Davidsohn Group 20 Exchange Pl., 27th Fl. New York, NY 10005 (212) 422–4100 (800) 999–6031	Vaccine
Diversified Computer Products PO Box 579 Swampscott, MA 01907 (617) 592–9001	PC Doctor

(Continued)

Manufacturer	Product Name
Fifth Generation Systems 10049 N. Reiger Rd. Baton Rouge, LA 70809–4862 (504) 291–7221 (800) 873–4384	Untouchable
IMSI 1938 Fourth St. San Rafael, CA 94901 (415) 454–7101 (800) 833–4674	VirusCure Plus
McAfee Associates 3550 Scott Blvd., Bldg. 14 Santa Clara, CA 95054 (408) 988–3832	Viruscan
Ontrack Computer 6321 Bury Dr., Ste.15–19 Eden Prairie, MN 55346 (612) 937–1107 (800) 752–1333	Dr. Solomon's Antivirus
Parsons Technology PO Box 100 Hiawatha, IA 52233–0100 (319) 395–9626 (800) 223–6925	ViruCide Plus
PC Guardian 1133 E. Francisco Blvd., #D San Rafael, CA 94901 (415) 459–0190 (800) 288–8126	Virus Prevention Plus
Symantec 10201 Torre Ave. Cupertino, CA 95014–2132 (408) 253–9600 (800) 441–7234	Norton AntiVirus
TCP Techmar Computer Products 98-11 Queens Blvd., Ste. 2-C Rego Park, NY 11374 (718) 997–6666 (800) 922–0015	AntiVirusPlus
Xtree 4115 Broad St., Bldg. 1 San Luis Obispo, CA 93401–7993 (805) 541–0604 (800) 876–6368	ViruSafe

Common Virus Infections

1575

This virus displays a caterpillar, which gobbles up characters. It attaches itself to COM and EXE files when performing DOS operations. Does not damage files.

Azusa

This virus installs itself as a terminate-and-stay-resident (TSR) program and starts to infect floppies. Once it has infected 32 diskettes it scrambles the parallel and serial ports on the computer, rendering them inoperative. Azusa has also caused diskettes to be unusable and may damage overwrite files on high-density diskettes.

Cascade 170X

This virus attaches itself to COM files. Then, when an infected COM file is executed, the virus installs itself as a TSR. It may lock up, reboot, or even format the hard disk at random times after becoming an active virus.

Dark Avenger

This virus installs itself in memory and then infects COM, EXE, and overlay files. After every sixteenth infection, the virus will overwrite a random disk sector. In addition, it will cross-link files, damage the FAT and degrade network performance.

Form

This virus will sound simulated key clicks when you use your keyboard on the eighteenth or twenty-fourth day of the month. The virus has also reportedly corrupted disk files.

Jerusalem

Probably the most common virus, Jerusalem has many strains. Symptoms associated with this virus include the playing of "Frere Jacques" at five-minute intervals on Fridays; slowing the system; and displaying a black box half an hour after a file is infected. The virus attaches itself to EXE, overlays, and COM files.

Joshi

This virus will lock up an infected system on January 5, and display the message "Type Happy Birthday Joshi!" The system will not respond until you obey.

Michelangelo

This is the most widely known virus due to recent publicity. This virus will overwrite the first 9Mb of an infected hard disk. The destruction occurs on March 6, Michelangelo's birthday.

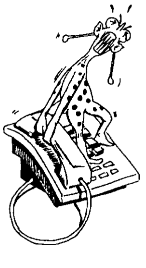
No-Int(Stoned)

This is a variation on Stoned that is basically undetectable while the virus is resident in memory. The virus can cause conflicts with disk utility programs and has been known to destroy the boot sector or partition table of a hard disk.

Stoned

This virus displays the message "Your PC Is Now Stoned!" every eighth system boot. Additional symptoms include the overwriting of the FAT and difficulty in retrieving files from infected diskettes.

Telephone Protection



Many companies today have complex private branch exchange (PBX) telephone systems with integrated call accounting and voice mail. Losing telephone service is like losing the ability to breathe for most organizations. Therefore, it is extremely important for an organization to have a contingency communications plan in the event of equipment failure.

With advances in digital technology, many phone systems are able to reroute their calls, with assistance from the telephone company, to another number or location. In addition, it is recommended that the following plan be put into effect in the event of a front console failure:

- Make sure that there are several bypass phones around the office that do not need to be routed through the PBX. These phones can then handle incoming calls with minimal interruption.
- Keep a listing of the location of the bypass telephones and train personnel in the operation of the system in the event of a console failure. These telephones should be tested periodically.
- Contact the telephone company and explore other options available to you in the event of equipment failure.
- Discuss your options with your telephone vendor. These options should include maintenance, response time in the event of equipment failure, and hardware/software updates.

Chapter 2. Disaster Recovery Checklists

The following checklists will provide a mechanism for gathering information and analyzing requirements of disaster recovery planning.

General Checklist

Task	Responsible Individual	Date Completed
1. Appoint Chairperson		
2. Appoint Committee		
3. Prepare Emergency Telephone Listing		
4. Identify two candidates for first aid/CPR training		
5. First Aid Training Completed		
6. CPR Training Completed		
7. Prepare Hardware Listing		
8. Prepare Software Listing		
9. Evaluate Insurance		
10. Identify Key Vendors		
11. Identify Off-Site Operations Locations		
12. Schedule Annual Disaster Recovery Plan Meeting		

Disaster Recovery Committee

Disaster Recovery Chairperson: ____________________

Address: ____________________

Telephone: ____________________

Management Information Systems: ____________________

Address: ____________________

Telephone: ____________________

Physical Facilities: ____________________

Address: ____________________

Telephone: ____________________

Personnel: ____________________

Address: ____________________

Telephone: ____________________

First Aid and Safety: ____________________

Address: ____________________

Telephone: ____________________

Company Management: ____________________

Address: ____________________

Telephone: ____________________

Alternate # 1: ____________________

Address: ____________________

Telephone: ____________________

Alternate # 2: ____________________

Address: ____________________

Telephone: ____________________

Emergency Telephone Listing

Fire: ______________________________

Police: ______________________________

Ambulance: ______________________________

Hospital: ______________________________

Alarm Company: ______________________________

Contact: ______________________________

Gas Company: ______________________________

Contact: ______________________________

Electric Company: ______________________________

Contact: ______________________________

Telephone Company: ______________________________

Contact: ______________________________

Leasing Agency (for sites and equipment): ______________________________

Contact: ______________________________

Computer Vendor (for software and hardware): ______________________________

Contact: ______________________________

Company President/Officer: ______________________________

First Aid/CPR Training

Candidate #1:

Name:____

Address: ____

Telephone: ____

Remarks ____

____

____

____

____

Interviewed by: ____________________ Date: ______________________

Scheduled Training: __________________

Candidate #2:

Name:____

Address: ____

Telephone: ____

Remarks ____

____

____

____

____

Interviewed by: ____________________ Date: ______________________

Scheduled Training: __________________

Equipment Listing

Description	Cost/Date Acquired	Features
Hardware:		
Work Station		
File Server		
Main CPU		
CD-ROM Drive		
Modem		
Printers:		
Dot Matrix		
Laser		
Color Laser		
Other Equipment:		
Copy Machines		
Fax Machine		
PBX/Telephone System		
Scanners		
Optical Storage System		
Audiovisual		

Software Listing

Description	Cost/Date Acquired	Version
Operating System (DOS, Novell, Unix)		
Word Processing		
Financial Reporting		
Payroll Processing		
Inventory		
Accounts Payable		
Accounts Receivable		
Spreadsheet		
Database		
Time and Billing		
Due Date Monitoring		
Purchase Order		
Depreciation		
Tax Preparation		
Desktop Publishing		
CD-ROM Library		

Insurance Evaluation

Insurance Carrier: ____________________

Address: ____________________

Telephone: ____________________

Contact: ____________________

Type of Current Coverage:

1. ____________________
2. ____________________
3. ____________________
4. ____________________
5. ____________________
6. ____________________

Limitations: ____________________

____

____

Last Review Date:

By: ____________________

Approved: ____________________

Backup Control Log

By Whom:	Date:	Time:	Data Verified:

Key Vendor Contact List

Name: ____________________

Contact: ____________________

Address: ____________________

Telephone: ____________________

Type of company: ____________________

Services to be provided: ____________________

Lead time required: ____________________

Estimated cost: ____________________

Last contact date: ____________________

Last contacted by: ____________________

Name: ____________________

Contact: ____________________

Address: ____________________

Telephone: ____________________

Type of company: ____________________

Services to be provided: ____________________

Lead time required: ____________________

Estimated cost: ____________________

Last contact date: ____________________

Last contacted by: ____________________

Off-Site Location Worksheet

1. Name: ______________________ Phone: ______________________

   Contact person: ______________ Last contact date: ______________

   Size of area: ____

   Approximate cost: ____

   Comments: ____

2. Name: ______________________ Phone: ______________________

   Contact person: ______________ Last contact date: ______________

   Size of area: ____

   Approximate cost: ____

   Comments: ____

3. Name: ______________________ Phone: ______________________

   Contact person: ______________ Last contact date: ______________

   Size of area: ____

   Approximate cost: ____

   Comments: ____

4. Name: ______________________ Phone: ______________________

   Contact person: ______________ Last contact date: ______________

   Size of area: ____

   Approximate cost: ____

   Comments: ____

Off-Site Supply Listing

Office Supplies
Calculators,
Tape, Staplers, Paper Clips,
Pencils, Pens, Markers,
and Paper

____

____

____

____

____

____

____

____

____

____

____

____

____

Office Equipment
Telephones,
Copier,
Fax Machine,
Computer(s) and Printer(s),
Desk and Chairs,
Work Table

____

____

____

____

____

____

____

____

____

____

____

____

Annual Disaster Recovery Meeting Plan

Introduction of Disaster Recovery Chairperson

Introduction of Disaster Recovery Committee

Presentation of Disaster Recovery Plan

Introduction of First Aid/CPR Specialists

First Aid and Safety Training

Fire/Earthquake Drill

The Information Technology Section

IT Section Membership

The AICPA IT Section provides products and services that will allow you to keep pace with changes in technology and increase your competence in information technology. It will also offer advice that will help you provide information technology services in a more professional — and profitable — manner. Annual membership dues are $100. Section benefits include—

- Subscription to the IT Section's quarterly newsletter, *InfoTech Update,* with essential information on new developments in the ever-changing world of technology.
- Practice aids, technology bulletins, and research reports.
- At least four issues of *Technology Alerts* — one-page releases on up-to-the-minute topics.
- Vendor discounts on selected products and publications.
- Discounted registration to the annual Microcomputer Conference.

For more information on IT Section membership, please call Nancy Cohen at (212) 596–6010.