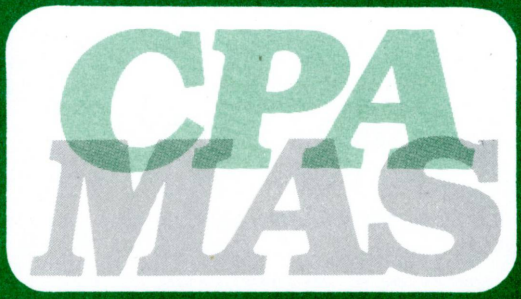
1991

Disaster recovery planning

American Institute of Certified Public Accountants. MAS Computer Applications Subcommittee



MANAGEMENT
ADVISORY SERVICES
PRACTICE AIDS

TECHNICAL CONSULTING PRACTICE AID **15**

Disaster Recovery Planning

AICPA
American Institute of Certified Public Accountants

NOTICE TO READERS

MAS practice aids are designed as educational and reference material for members of the Institute and others interested in the subject the aid addresses. They do not establish standards or preferred practices. The standards for MAS practice are set forth in the Statements on Standards for Management Advisory Services (SSMASs) issued by the AICPA. However, since the services described in this series of practice aids are management advisory services, the standards in the SSMASs should be applied to them as appropriate.

Members of the 1989–90 AICPA MAS Computer Applications Subcommittee were involved in the preparation of this practice aid. The members of the subcommittee are listed below.

Bruce F. Malott, *Chairman*
Nancy G. Britt
Bruce K. Bryant
Gilbert W. Charney
William C. Fleenor
Joel R. Kamil
Michael LaGioia
Joseph C. Maida
Darvin C. Melton
Evelyn R. Michaud
William J. Niles
David M. Smith
Irwin Winsten

The subcommittee gratefully acknowledges the efforts of Bruce K. Bryant in developing this practice aid, as well as the contribution of former subcommittee members.

Monroe S. Kuttner, *Director*
Management Advisory Services

Monte N. Kaplan, *Technical Manager*
Management Advisory Services

Steven E. Sacks, *Technical Manager*
Management Advisory Services

William J. Moran, *Editor/Coordinator*
Management Advisory Services

TECHNICAL CONSULTING PRACTICE AID **15**

Disaster Recovery Planning

AICPA
American Institute of Certified Public Accountants

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

Preface

This MAS practice aid is one in a series intended to assist practitioners in applying their knowledge of organizational functions and technical disciplines in the course of providing management advisory services. Although these practice aids often deal with aspects of MAS knowledge in the context of an MAS engagement, they are also intended to be useful to practitioners who provide advice on the same subjects in the form of an MAS consultation. MAS engagements and consultations are defined in Statement on Standards for Management Advisory Services (SSMAS) No. 1, issued by the AICPA.

This series of MAS practice aids should be particularly helpful to practitioners who use the technical expertise of others while remaining responsible for the work performed. It may also prove useful to members in industry and government in providing advice and assistance to management.

MAS technical consulting practice aids do not purport to include everything a practitioner needs to know or do to undertake a specific type of service. Furthermore, engagement circumstances differ, and, therefore, the practitioner's professional judgment may cause him or her to conclude that an approach described in a particular practice aid is not appropriate.

Contents

Introduction

Disaster struck the U.S. Postal Service one October evening in 1984 when a fire broke out in the ninth floor data center of its Washington, D.C. headquarters. The fire damaged more than 1,500 microcomputers, terminals, and peripherals and caused over $20 million in damages. In addition to the loss of equipment and facilities, which *could* be replaced, the U.S. Postal Service law department lost six years of files and active case records, which could *not* be replaced. There was no disaster recovery plan.

Almost two years later to the day, fire completely destroyed the Montreal headquarters of Steinberg, Inc., a $4.5 billion retailer generating millions of transactions every day. Less than forty-eight hours after the fire, Steinberg's computer operations were transferred to a leased facility in New Jersey and became operational, with full communications restored to all the organization's branches. The following day, the payroll for Steinberg's 28,000 employees was processed without any significant problems.

The difference in the outcome of these two disasters can be attributed to a detailed disaster recovery plan, which Steinberg, Inc. had prepared.

Scope of This Practice Aid

In the Information Age, an increasingly large number of organizations have replaced manual systems with computer-based automated systems. Many such organizations operate as if a disaster will never happen to them or as if they can deal with it without a plan. Others mistakenly believe that they are protected because they periodically back up their systems. Unfortunately, companies have discovered that unplanned interruptions of their data processing facilities can have catastrophic effects on their ability to continue in operation. When disasters occur, it is difficult, if not impossible, to recover these systems in a timely fashion.

Disaster recovery planning is becoming increasingly important today as companies become more dependent on their computer systems. This practice aid provides practitioners with a guide to preparing and evaluating a disaster recovery plan for both microcomputer and minicomputer systems. It discusses two specific application areas: (1) developing and implementing procedures to prevent a disaster or lessen its impact and (2) developing detailed procedures to follow if a disaster occurs. The details of the plan's procedures will vary according to the type and size of the organization.

This practice aid helps practitioners identify computer operations necessary to the organization's functioning and the steps to take to prevent disasters from crippling the business. This practice aid does not purport to cover all

contingencies, but focuses on some of the more important aspects of maintaining the integrity of files.

The Importance of Disaster Recovery Planning

The significance of a problem depends on its consequences. A short-term power loss may be immaterial to a company's operations. However, the company needs to learn how to prevent such occurrences from turning into disasters and to cope with severe disasters in the future.

Very few organizations can function with a prolonged interruption of data- and computer-processing capabilities. The financial costs associated with such a disruption could threaten the very existence of the organization. A disaster recovery plan may save thousands of dollars in losses from destruction of information or delay in its flow. It may not always prevent a disaster, but it can help keep an organization intact and operating. The goal of a disaster plan is to ensure business continuation.

In some regulated industries, disaster recovery planning is important enough to be required. For example, the Office of the Comptroller of the Currency requires all national banks to have disaster recovery plans and to test them periodically.

Disasters vary in magnitude and may involve more than just a loss of data or computer operations. Although the list of events that create disasters is endless, disasters all have one or more of the following elements of loss:

1. *Loss of information*, such as corrupted or deleted files resulting from unauthorized access and lost or destroyed tapes or disks
2. *Loss of hardware*, including stolen machines, failed hard disks, and worn-out hardware
3. *Loss of key employees*
4. *Long- and short-term losses of computer processing capabilities* due to power outages, acts of God, and so on

Preparing a Disaster Recovery Plan

A disaster recovery plan documents the procedures to follow when unexpected and undesirable events interrupt an organization's data processing capability.

The procedures make up a system to minimize damage from events such as fires, bomb threats, armed robberies, power failures, and hardware and telecommunications failures. A disaster recovery plan describes the steps necessary to recover data, applications programs, and processing capability.

A disaster recovery plan also identifies—

1. The steps to take immediately after a disaster strikes.
2. The systems and applications to restore first.
3. The location of the recovery site.
4. The back-up procedures and other actions that may help prevent a disaster or lessen its impact.
5. Key employees and their responsibilities.

The sections that follow discuss the major steps of a disaster recovery plan. Each step is crucial to the successful completion of the plan. If unable to complete each step properly, the practitioner needs to reevaluate whether the plan meets the client's objectives. Exhibit 1 in the Appendix is a sample engagement letter describing the typical approach in a disaster recovery planning engagement.

Although disaster recovery plans vary based on the organizations for which they are designed, all plans need to be easy to read and use. Some are best presented with charts, decision matrices, and tables. The Appendix contains a sample disaster recovery plan applicable to some, but not all, disasters.

For those companies with a single location that have a single-user PC or a small network, the disaster plan could be as simple as documentation of equipment, suppliers, and back-up procedures. As long as proper backups are occurring, the result of a disaster may be easily repaired through the simple replacement of a PC or network server.

Secure Top Management Support

Because preparing a disaster recovery plan requires a commitment of time, personnel, and financial resources, executive management support is critical. To gain this support, the practitioner can educate management about the effects of an unplanned interruption of data processing services, such as an inability to process payrolls and customer billing and maintain inventory control. Associated financial controls also need to be considered. A cost-benefit analysis would further strengthen management's support for the development of a disaster recovery plan.

The practitioner can recommend disaster recovery planning as a kind of insurance. Disasters often occur without warning, and therefore planning is important. The cost of disaster planning, like the cost of commercial insurance coverage, is usually minimal compared to the consequences of being unprepared. The ultimate consequence could be the end of the business.

Establish Objectives

Once executive management has made a commitment to disaster recovery planning, the practitioner establishes plan objectives that are realistic, achievable, and economically feasible.

Examples of such objectives include the following:

- Develop daily, weekly, or monthly procedures for data backup and security over computer operations.
- Establish procedures and priorities for restoration. Restore critical data processing operations as quickly as possible.
- Minimize losses and costs associated with the disaster and subsequent recovery.
- Maintain an acceptable level of customer service.
- Maintain the organization's competitive position.
- Establish controls to maintain security over system procedure manuals and related technical publications.

Although such objectives provide direction in preparing the disaster recovery plan, during the engagement the practitioner continually reevaluates whether they are realistic and achievable.

Conduct an Operational Impact Analysis

One phase of disaster recovery planning that is very important to the engagement's success is analyzing a disaster's impact on operations. During this phase, the practitioner identifies the systems and applications that are critical to continuing business. The key to analyzing these is understanding the organization, its operational priorities, and the personnel and locations involved.

The practitioner needs to define which of the primary business functions of the organization are supported by computer operations. This defining includes the use of flow charts and descriptions of the departmental operations, as well as identification of the key employees involved and referral to timetables for due dates, secondary suppliers, and so forth. The practitioner ranks the employee functions according to their impact on the organization's day-to-day operations. Using an analysis of the operations, the practitioner (1) determines what procedures need to be performed daily, weekly, or monthly and in what order and (2) identifies those areas requiring immediate attention.

In defining the primary business functions, the practitioner develops the flowcharts and descriptions of the departmental operations in a way that enables management to visualize the economic impact (costs and benefits) on the business processes of changes in the volume and frequency of computer transaction processing. To persuade management to take the appropriate actions, the practitioner compares the costs involved in preparing and maintaining a disaster recovery plan with the potential operating losses if no contingency planning is done.

Some of the costs of contingency planning are associated with the following tasks:

1. Organizing and managing the project
2. Documenting the major computer services provided
3. Documenting interruptions and general procedures
4. Developing procedures for major disasters
5. Developing procedures for testing and updating
6. Testing the disaster recovery plan

Exhibit 2 provides further detail about these tasks.

The practitioner identifies all data processing systems and subsystems, including hardware systems (with any on-site back-up systems), software programs and files, and the vendors capable of quickly supplying new hardware and software. The practitioner determines each system and subsystem's impact on business operations and learns how the systems and subsystems interrelate, as well as the consequences of their being out of operation. For example, can the order processing department function without receiving and inventory operations? Can the company fill and ship customer orders if inventory data are not updated for new receipts? Exhibit 3 is a list that will guide the practitioner in obtaining the information needed to assess the effect a disaster would have on operations.

When reviewing the information system's vulnerability to disaster, the practitioner considers how essential each element is to continuing the client's primary business functions. The elements to consider include the following:

- All business functions
- Telephone and mail communications
- Vital records
- Personal computers
- Data processing computers
- Data processing applications
- Distributed computers
- Central computers

Analyze Risk

Risk analysis involves determining the potential risks and evaluating existing security controls. The risks to data operations are like any other risks to an organization and include external as well as internal threats. Security controls include logistical, physical, personnel, communications, and operational considerations.

Security controls consist of both the physical security of the operations, such as building access and security systems, and computer access security, such as password protection. The practitioner evaluates the need for security

controls by considering the client's security history, the physical location of operations, and employee screening methods.

Strong security, which minimizes access to the building and to computer operations, is a key consideration in minimizing risk. If operations are not secure, disasters are more likely to occur.

External threats are the events and people over which the organization has little control. Natural disasters, such as acts of God, and accidents due to human error can destroy facilities, equipment, and data, thereby interrupting operations. The destruction may be intentional, resulting from arson and the acts of political revolutionaries or terrorists. Computer viruses pose an especially serious threat.

Internal threats include accidental and deliberate acts by individuals within the organization. These threats include employee sabotage, unauthorized access, computer viruses, and errors and omissions.

One of the best methods for analyzing risk is brainstorming with management to identify the threats and their potential effects on operations. The practitioner documents the risks to cover in the disaster recovery plan. Brainstorming is best conducted in a closed but informal meeting with management. Participants discuss past experiences and raise questions about what they see as potential risks. The practitioner poses open-ended what-if questions. The discussions need to center around the potential impact of loss of processing capability, regardless of the cause. At the conclusion of the meeting, the practitioner reviews the risks identified and documents those to cover in the disaster plan.

Develop the Plan

The practitioner bases the disaster recovery plan on the objectives and on the potential risks to and impact on operations. The plan includes definitions of the levels of the disaster. A level I disaster, for example, may mean full destruction of company headquarters. A level II disaster may mean complete loss of primary computer operations.

The plan documents the procedures to perform and includes the following information:

- Level of response to different types of disasters
- Facility, equipment, software, and communication needs and their sources
- Responsible personnel
- Data and storage requirements
- Internal and external support requirements
- The process of moving personnel and data to a recovery site
- The order of systems restoration, including time estimates to restore

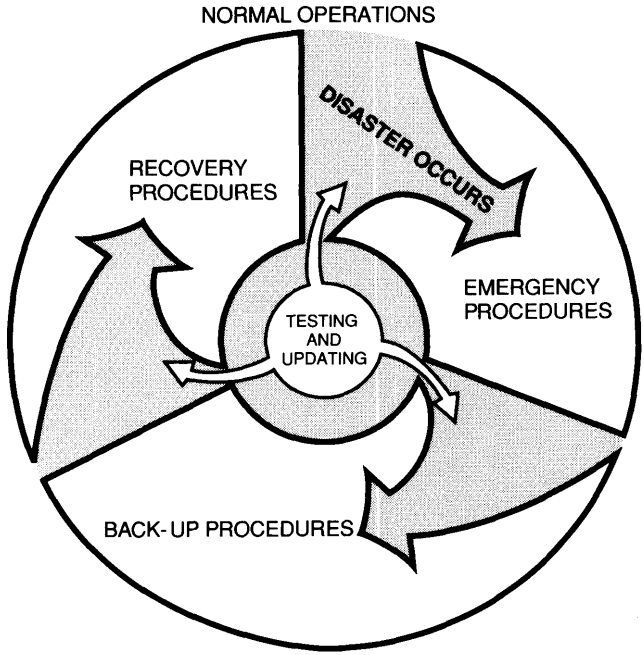
Exhibit 4 in the Appendix lists sample procedures.

In developing and documenting the procedures, the practitioner may find it helpful to consider the flow of activity during the implementation of the plan once a disaster interrupts normal operations. In general, the procedures fall into three categories:

1. *Emergency procedures.* These procedures are the first to be followed. Their purpose is to minimize further loss of personnel, data, and equipment. Usually these procedures detail how to determine the disaster level and whom to notify, such as key personnel, fire and police departments, and vendors. Exhibit 4.1 is a sample of a form that is used in determining a disaster level.
2. *Back-up procedures.* These procedures are designed to enable the organization to regain critical business functions, if only temporarily. For example, personnel and data may move to a "hot site" or the critical business functions may be performed manually on a temporary basis.
3. *Recovery procedures.* The process of returning to normal operations requires procedures designed to restore automation of the critical business functions.

The following figure is a diagram showing the flow of these procedures. Included in the cycle are procedures for testing and updating the activities.

Disaster Recovery Plan Flow



The written plan, including personnel assignments, is distributed to key staff members along with home phone numbers for all personnel. Other critical phone numbers to include are those for off-site storage and back-up site management. The plan also gives information and phone numbers for contacts at insurance companies, police and fire departments, state regulators and other agencies (such as the Federal Savings and Loan Insurance Corporation [FSLIC] and the Federal Deposit Insurance Corporation [FDIC]), and business form, hardware, and software vendors. Exhibit 4.2 is an example of this key plan information.

The plan contains an inventory of current hardware and software (including the version in use) and other necessary equipment. It also lists the reporting requirements and data files and their format. The practitioner advises the client to update the plan as new hardware and software are acquired and operations are modified or relocated. A copy of the plan is stored securely at an off-site location.

Assign Responsibilities

All key employees need to be familiar with the plan, its operation, and the goals of implementation. They need instruction in what to do in an emergency and are assigned as many specific tasks as possible with procedures for follow-up to ensure timely completion. Each supervisor gives employees a copy of the emergency procedures and reviews them semiannually with employees. The supervisor also reviews any changes in responsibilities resulting from promotions and hardware and software acquisitions. New employees receive a copy of the emergency procedures, and during their probation the supervisor reviews them in detail with the employees.

Test the Plan

The plan requires regular or periodic testing. At a minimum, the tests include assessing the ability to recover key operations and files from backup. The disaster plan will be ineffective if management and employees feel that it may not work.

Testing will most likely be performed during off hours. The tests simulate the various disasters, just as fire drills do, and then implement the disaster plan to determine the effectiveness of the prescribed procedures. Testing includes a review of off-site back-up facilities to determine that all equipment is compatible and that transactions can be processed to maintain operations.

Testing also establishes estimates of recovery times, including the time spent restoring operations from the back-up systems and the time it takes to achieve full recovery. The plan should be revised immediately when there is any turnover of personnel or suppliers included in the plan. Regular testing of the plan will disclose turnover in client personnel and outside vendors.

Evaluate the Plan

While developing and testing the plan, the practitioner thoroughly evaluates it to determine that it meets its objectives in an orderly and cost-effective fashion. If the client cannot effectively carry out the plan at a reasonable cost, the practitioner needs to consider alternatives before making the plan final. During development of the plan, the practitioner needs to address this issue continually.

Other Considerations

During an engagement to develop a disaster recovery plan, the practitioner may also find opportunities to strengthen an organization's security plan, risk management, and insurance coverage, as well as to identify areas where efficiency could be improved. The practitioner may also consider discussing the engagement objectives with the organization's hardware and software vendors because some now offer disaster recovery capabilities.

Conclusion

An organization needs to plan for and recover quickly from various disasters. Implementing an effective plan in the event of a disaster may minimize cash flow problems, for instance, by maintaining necessary operating data.

Disasters strike anywhere, at any time. An adequate disaster recovery plan prevents a temporary setback from becoming an irreversible disaster.

APPENDIX

Illustrative Materials

Exhibit 1

Engagement Letter

[*CPA Firm's Letterhead*]

July 7, 19XX

Client's Name
Firm Name
Address
City, State 10111

Dear _____:

I appreciated the opportunity to meet with you about developing a disaster recovery plan. This letter outlines our understanding of how we will assist you in establishing the plan.

Engagement Scope

The scope of the engagement will include an analysis of your firm's data processing operating procedures crucial to the continuance of your operations and an evaluation of your back-up sites, vendor support, and deployment of key employees in the event of a disruption of services. The engagement will last approximately thirty working days and will begin on August 3, 19XX.

Engagement Approach

Our overall approach is to provide a step-by-step disaster recovery plan that will meet the engagement objectives. To accomplish this, we will review your current operations and accounting system and procedures and interview appropriate members of your staff. We will conduct the required work as follows:

1. Document current operations, locations of facilities, hardware and software in use, and key employees in each operation of the company.
2. Evaluate past and potential disasters and assign levels to each type of disaster.
3. Evaluate the costs and benefits of implementing various actions depending on the defined level of disaster.
4. Establish the disaster recovery plan and document the procedures to follow.
5. Test and evaluate the disaster recovery plan and alternatives.

To complete this work, we expect your company to provide access to all facilities, have professional and administrative staff available for interviews, meetings, and questionnaires, and cooperate with our staff in developing solutions.

Client Benefit

The disaster recovery plan will provide detailed operating procedures to follow when a disaster occurs. The documentation will include the names of responsible employees, back-up site locations, and key contacts and plan administration procedures for continued updating. This plan will enable your company to effectively evaluate and recover from disasters.

Engagement Staffing and Scheduling

During the engagement, your staff, especially you and your administrator, will be involved as much as possible. The greater your staff's participation, the easier it will be for them to adapt and implement the disaster recovery plan.

I will supervise the consulting engagement. Harold Baines, who has performed similar evaluations over the last ten years, will be in charge of the field work.

Project Completion

We will conclude the engagement by presenting you with the results of our procedures and a proposed disaster recovery plan.

If, during the engagement, either of us learns of circumstances that may prevent a successful conclusion, one of us may terminate the engagement by notifying the other in writing.

At the conclusion of the engagement, we may suggest a second engagement to provide implementation guidelines. We can discuss our respective roles in this phase when we deliver our final report. If desired, we will submit our proposal to provide additional services at that time.

Fees, Billing Arrangements, Payment

We will base our fees for this engagement on the time spent at our standard hourly rates. The estimated cost of the project is $XX,XXX. A retainer of $X,XXX is due on your acceptance. We will bill the remainder of the fee at the conclusion of the engagement. We will also bill you for any out-of-pocket costs, such as transportation or materials, in addition to our fees.

Engagement Acceptance

Please acknowledge your acceptance of these terms by signing this letter and returning one copy to us with a check for $X,XXX. Thank you for retaining us. We hope this will be the beginning of a long and mutually beneficial relationship.

Sincerely,

_____

John Doe, CPA

Approved by_____
President

Date_____

Disaster Recovery Planning Project
Summary Workplans

	Description	*Estimated Man-Days**
1.	Organize and manage the project.	
	Organize the project team.	0.2
	Define objectives and general approach.	0.5
	Finalize deliverables of the project.	0.1
	Finalize outline for the disaster recovery plan document.	0.2
	Finalize the project plan and schedule.	0.5
	Manage and administer the project.	2.5
	Total	4.0
2.	Document major computer services provided.	
	Identify major applications and key users.	0.2
	Interview key users and data processing staff.	2.5
	Document services, users, and considerations.	2.0
	Review write-ups with key users and data processing staff.	2.0
	Finalize major services documentation.	1.3
	Total	8.0
3.	Document interruptions and general procedures.	
	Identify potential service interruptions.	0.4
	Interview key data processing or other department staff.	2.5
	Prepare procedures for each interruption.	2.0
	Review procedures with key staff and management.	2.0
	Finalize interruption procedures.	1.1
	Total	8.0
4.	Develop procedures for major disasters.	
	Define emergency teams and responsibilities.	3.0
	Identify procedures to be developed.	1.0
	Develop the disaster recovery procedures.	12.0
	Review the procedures with key management.	3.0
	Finalize the recovery procedures.	1.0
	Total	20.0

*Estimated man-days are for illustrative purposes only and do not refer to a specific company size.

Description	*Estimated Man-Days*
5. Develop procedures for testing and updating.	
Develop procedures for testing the plan.	2.0
Develop procedures for maintaining the plan.	2.0
Total	4.0
6. Test the disaster recovery plan.	
Arrange for the test with contingency site.	0.1
Design any specific application test.	0.9
Conduct the test of local procedures and computer tests at contingency site.	6.0
Evaluate the test and determine any needed changes in the plan.	1.0
Update the plan as necessary.	2.0
Total	10.0

Disaster Recovery Planning Operational Impact Analysis

[*The practitioner uses this impact analysis to review and document the client's operations. This form is filed with permanent workpapers and updated at least annually.*]

General Company Operations

Client_____ Client No._____
Prepared by_____ Date_____
Reviewed by_____ Date_____

Form of entity:

Regular corporation_____ S corporation_____
Partnership_____ Sole proprietorship_____
Other (describe)_____

Nature of business:

Retail_____ Wholesale_____ Manufacturing_____ Service_____
Other (describe)_____

Types of products or services_____

Operating environment:

Who sets company objectives and makes major operating decisions?

_____

Client's philosophy: conservative_____ or risk-taking_____
Operations: centralized_____ or decentralized_____

Has the client

Acquired new businesses? Yes_____ No_____
Divested itself of subsidiaries? Yes_____ No_____
Made other changes (describe)?_____

_____

_____

What are the important assets, liabilities, revenue, and expenses (if any)?

_____

_____

_____

_____

Where are plants, stores, warehouses, showrooms, etc.?

_____

_____

_____

_____

Production method (describe):_____

_____

_____

_____

_____

Produce upon receipt of order?_____

Produce for stock?_____

Principal raw materials?_____

Is process

Labor-intensive?_____

Union or non-union?_____

Capital-intensive?_____

Where does the client buy raw materials?

Manufacturer_____ Distributor_____ Importer or exporter_____
Other (describe)_____

How is product or service distributed or sold?

Employee salespeople_____ Independent agents_____ Mail order_____
Store_____ Catalog_____ Other (describe)_____

Unusual payment arrangements for purchases:

Special invoice dating_____ Consignment_____
Other (describe)_____

Unusual customer arrangements (describe):

Consignments_____ Special return privileges_____

_____

Special payment arrangements_____
Other_____

How does the client keep accounting records?

Handwritten_____ Bookkeeping machine_____ Service bureau_____
In-house mainframe_____ Microcomputer_____
Other (describe)_____

In what areas does the client use computer programs?

_____

_____

_____

_____

_____

_____

What software programs are in use?

Program	*Employees Using*	*Locations of Use*

Basis of accounting used for accounting records:

Accrual_____ Cash_____ Income tax_____
Other (describe)_____

Basis of accounting used for tax purposes:

Accrual_____ Cash_____
Other (describe)_____

Computer hardware in use by location and suppliers

Equipment	*Location*	*Supplier*

Ledgers and journals used (indicate **C** if prepared by computer; **M** if prepared manually):

General ledger_____ Sales journal_____ Purchase journal_____
Cash receipts journal_____ Check register_____
Perpetual inventory records_____ Accounts receivable subsidiary_____
Accounts payable subsidiary_____ Other (describe)_____

Accounting records prepared by client's personnel

Through trial balance_____ Through financial statements_____

What are the stated qualifications of bookkeeping and accounting personnel?

Name	*Position*	*Above Average*	*Average*	*Below Average*

Compensation method (indicate whether salaried, hourly, or commission; whether bonus, profit sharing, or similar arrangements):

Management_____
Office and administrative_____
Salespeople_____
Plant_____
Other (describe)_____

Payroll prepared:

In-house_____ By outside service bureau_____

Names and relationships of related parties:

Types of material transactions with related parties:

Other important information about client:

Computer Operations

Program	*Number of Users*	*Key Employees*

Daily computer operations (include back-up procedures):

Weekly computer operations:

Key computer processing and information systems and priority of operation:

System	*Priority (Rank 1–10)*	*Impact if Operations Ceased*

Sketch a flow chart of computer operations and interdependent functions in each department (use additional sheets if necessary).

XYZ Corporation Disaster Recovery Plan*

Company Description, Physical Facilities, and Locations

XYZ Corporation is a wholesale distributor of commercial and industrial insulation. Its primary customers are independent contractors and large utilities. It has approximately one hundred employees.

The company maintains corporate headquarters in Lenexa, Kansas, where twenty-five employees work. The company also leases warehouses in Lenexa; Omaha, Nebraska; and Phoenix, Arizona. Approximately twenty-five employees work at each warehouse location.

Computer operations, in the form of a microcomputer network, are at company headquarters. Each warehouse facility is linked directly to headquarters via modems using dedicated telephone lines.

Responsible Employees

William Johnson, vice president, data processing, will maintain and implement this disaster recovery plan. In his absence, Michael Barnett, supervisor, will be responsible. When a disaster occurs, the disaster recovery plan administrator assigns it to one of the levels defined in this plan.

Disaster Avoidance Procedures (Internal)

1. Daily procedures: Frank Brett will perform backups of the dedicated file server twice daily at 11:30 A.M. and 5:30 P.M. Mr. Brett will take the 5:30 back-up tape off-site and will store the 11:30 tape in the company's fireproof safe on-site.
2. Weekly procedures: Each Friday, Frank Brett will send the 5:30 back-up tapes to the ABC off-site storage facility. Mr. Brett will also review all operating programs and files to determine if there are any unauthorized applications that may contain a program virus. Any unauthorized applications will be deleted.
3. Monthly procedures: Mr. Brett will test the monthly back-up tapes to ensure their reliability and the ability to restore data from the tapes. He will compare system files to the active dedicated file server and investigate any differences immediately.
4. Other: Employees are responsible for performing daily backups of their hard disks (if applicable). These may be stored in the company's fireproof safe.

Disaster Level Defined

Once the disaster level is assigned, refer to the specific procedures to complete for each level. Please contact the individuals below immediately when a disaster has occurred or may occur.

*This is an abbreviated plan and its procedures are not intended to cover all possible types of disasters.

Disaster Plan Administrator:	William Johnson Work: (913) 278-1000 Home: (913) 642-8873 Beeper: (913) 591-6401
Backup 1:	Michael Barnett Work: (913) 278-1002 Home: (913) 642-8874
Backup 2:	Robert Smith Work: (913) 278-1003 Home: (913) 642-8875

Disaster Level Definitions

The following disaster levels are listed in order of priority from highest to lowest:

I. All computer operations are lost through destruction of the computers or facility, long-term power outage (more than five days), or evacuation of the building because of an external threat.

II. The network server fails at one or more locations or departments, or the hard disk fails or programs and files on the disk cannot be accessed.

III. Telephone connections to remote locations are interrupted or modem operations are in disarray because of faulty or broken equipment.

IV. Files within any application are corrupted.

Disaster Recovery Procedures

I. Level I Disaster

A. Key employees: Plan administrator—William Johnson
Computer operations—Frank Brett
Facility management—Thomas Wilson
Warehouse operations—Fred Carlton

B. Procedures

1. Plan administrator
   - Contact president and above employees to inform them of the disaster.
   - Complete the disaster level assignment matrix (see exhibit 4.1); assign priorities to each department, and determine if site evacuation is required.
   - Follow up and check off completion of assignments.

2. Computer operations
   - Contact suppliers to arrange new hardware if needed or back-up computer facilities if disaster has impaired any operations at headquarters (see key plan information in exhibit 4.2) and arrange for resumption of operations.
   - Contact the back-up-tape storage facility and arrange for pickup of tapes.
   - Install computer systems on back-up hardware in the order prescribed by the administrator (refer to the priority ranking in the disaster-level assignment matrix).

- Determine if modem connections to all outside locations are complete.
- Notify the department as its applications become available on the back-up computer.

3. Facility management
   - Determine the extent of damage to the facility.
   - Contact contractors for repair or the back-up location if operations cannot continue at the facility.
4. Warehouse operations
   - Implement manual operations for tracking shipments and receipts until computer operations resume.
   - Contact outside warehouse to implement manual operations.
   - Monitor manual paper flow to data processing.

C. Hardware and software in use [*brand names are fictitious*]
   1. Equipment inventory
      a. Primary site

Dedicated file server:	PC—BKB 1000 2-MB RAM 170-MB hard disk
Printers:	2 laser printers 3 IKZA dot-matrix high-speed
Workstations:	8 PCs—BKB 500 1-MB RAM 40-MB hard disks each
Modem:	4800 baud

      b. Remote locations (same inventory at each)

Workstations:	5 PCs—BKB 500 1-MB RAM 40-MB hard disks
Printers:	3 IKZA dot-matrix high-speed
Modems:	5 4800 baud

      c. Recovery site

File server:	PC—BKB 2000 4-MB RAM 340-MB hard disk
Printer:	1 IKZA dot-matrix high-speed
Workstations:	4 PCs—BKB 500 1-MB RAM 40-MB hard disks
Modems:	3 4800 baud

   2. Software—primary and remote sites
      a. ABC Accounting Package
         General ledger, version 1.12
         Accounts receivable, version 1.12
         Accounts payable, version 1.10
         Purchase order, version 1.10
         Sales order, version 1.10
         Inventory, version 1.11
      b. Spreadsheets
         Network version CDF Calc, release 3.04

c. Data bases
Network version BigBase, release 2.07

d. Key personnel

1. Recovery team
   a) William Johnson—supervisor 278-1000
   b) Michael Barnett—backup 278-1002
   c) Steve Morris—operator 229-3675
2. Recovery site (ABC Computer Corporation)
   a) Roger Peters—system support 491-6363
   b) Dennis Wilson—data systems 491-6324
   c) Joseph Bennett—account rep 491-6368
3. Company officer team
   a) Jim Smith—assistant VP 228-5980
   b) Jessica Graves—controller 228-6070

II. Level II Disaster

A. Key employees: Plan administrator—William Johnson
Computer operations—Frank Brett

B. Procedures

1. Plan administrator
   - Contact president and above employees to inform them of the disaster.
   - Complete the disaster-level assignment matrix by assigning priorities to each department.
   - Follow up and check off for timely completion of assignments.
2. Computer operations
   - Notify all users to log off the dedicated file server until further notice and document procedures in process that were interrupted.
   - Notify hardware vendor of the existing disaster and arrange for immediate hard disk testing or replacement of hard disk.
   - Attempt backup of hard disk onto new back-up media. If this fails, notify users that all systems will be restored to the date and time of last backup and therefore activity after that date will have to be reprocessed.
   - Test repaired or new hard disk for diagnostics and proper operation. Once satisfactory, notify users to resume operations.

III. Level III Disaster

A. Key employees: Plan administrator—William Johnson
Computer operations—Frank Brett
Employees affected by terminal failure

B. Procedures

1. Plan administrator
   - Contact computer operations manager and affected employees at remote locations.
   - Complete disaster-level assignment matrix by assigning priorities.
   - Follow up and check off completion of assignments.

2. Computer operations
   - Run diagnostic tests on modems to determine cause of failure and contact phone company to notify them of the interruption.
   - Assign affected employees to any open terminals and notify their supervisor of action.
   - Notify hardware vendors and contact maintenance personnel of failure and arrange for repair or replacement.

IV. Level IV Disaster
   A. Key employees: Plan administrator—William Johnson
      Computer operations—Frank Brett
   B. Procedures
      1. Plan administrator
         - Contact computer operations manager.
         - Complete disaster-level assignment matrix by assigning priorities.
      2. Computer operations
         - Notify all users to terminate any activity on the dedicated file server.
         - Back up all files of the dedicated file server.
         - Run diagnostics on the file server to determine extent of damage (that is, bad sectors on the hard disk or potential of a spreading virus).
         - Review computer activity log for potential causes.
         - Block out bad sectors on the disk and restore corrupted files or send in the virus killer program and test for success. Replace and restore hard disk, if necessary.
         - Notify all users when operations are at full capacity.

Exhibit 4.1

Disaster Level Assignment

Disaster Level_____

Department or Area	*Percentage Affected*	*Locations*	*Personnel*	*Systems*		*Priority*
				Network	*PCs*	
Corporate facilities						
Order entry						
Billing						
Cash receipts						
Payroll						
Purchase order						
Receiving						
Accounts payable						
General ledger						
Other_____						

Key Plan Information

Off-Site Storage Facilities

Daily backups are maintained at XYZ storage facility.

Phone:	(913) 111-2222
Key contact:	John Smith or Bill Jones
Location:	8717 W. 110th Street Overland Park, KS 66210
Description:	Warehouse facility back-up tapes are filed by day in fireproof safes. XYZ maintains security over safes. Access is available twenty-four hours a day.

Back-up Site

Computer operations are backed up at BU.

Phone:	(913) 222-1111
Key contact:	Sally Jones or Bertha Smith
Location:	15620 W. 99th St. Lenexa, KS 66215
Description:	BU requires two hours' notice to set up available computers. Estimated time to load programs and data files is twelve hours. Access is available twenty-four hours a day.

Key Contacts

Fire department:	(913) 237-1212
Police:	(913) 245-1188
Insurance:	Jones Insurance Company (913) 888-1273 Phil Smith or Doug Peete
Security:	Maggie Lester or Mark Aldridge (212) 123-4567
Business forms:	ABC Form Company (816) 711-1271 Mike Hill or Mike Myers All company forms are purchased here, and ABC maintains originals for duplication. ABC needs two hours' notice to begin printing.

Personnel Assignments

Computer operations are set up at the back-up facility.

Data loading:	Ernest Billings
Home phone:	(913) 222-1717
Car phone:	(913) 311-6401
Beeper:	(913) 311-7777
Back-up person:	Steve DeBerg
Home phone:	(913) 111-7218

Vendors for Replacement Material

1. Hardware: All hardware can be purchased at BKB Computers, 1111 Grand Avenue, Lenexa, KS (913-494-8000). BKB maintains an inventory of all hardware and will deliver it within two hours of contact.
2. Software: Joseph Account, CPA, 1274 Main Street, Lenexa, KS (913-492-8787), maintains working copies of the software programs if the back-up copies fail.

Bibliography

Baker, Richard H. *The Computer Security Handbook.* Blue Ridge Summit, Pa.: TAB Professional and Reference Books, 1985.

Burger, Ralph. *Computer Viruses: A High-tech Disease.* London: Abacus, 1988.

Cooper, James A. *Computer Security Technology.* Lexington, Mass.: Lexington Books, 1984.

The Disaster Contingency Book. Long Beach, Calif.: Chantico Publishing, 1985.

Highland, Harold J. *Protecting Your Microcomputer System.* New York: John Wiley & Sons, 1983.

Lord, Kenniston W. *The Data Center Disaster Consultant.* Wellesley, Mass.: Q.E.D. Information Sciences, 1977.

Lundell, Alan. *Virus!: The Secret World of Computer Invaders That Breed and Destroy.* Chicago: Contemporary Books, Inc., 1989.

Muttic, Snead. *Security Mechanisms for Computer Networks.* Peoria, Ill.: Ellis Horton, 1989.

Richard, Arnold. *The Disaster Recovery Plan.* Wellesley, Mass.: Q.E.D. Information Sciences, 1989.

Roberts, Ralph and Pamela Kane. *Computer Security.* Greensboro, N.C.: Compute! Publications, Inc., 1989.

MAS PRACTICE AIDS

MAS Small Business Consulting Practice Aids Series

No. 1 *Assisting Small Business Clients in Obtaining Funds*
No. 2 *Identifying Client Problems: A Diagnostic Review Technique*
No. 3 *Assisting Clients in Maximizing Profits: A Diagnostic Approach*
No. 4 *Effective Inventory Management for Small Manufacturing Clients*
No. 5 *Assisting Clients in Determining Pricing for Manufactured Products*
No. 6 *Business Planning*
No. 7 *Personal Financial Planning: The Team Approach*
No. 8 *Valuation of a Closely Held Business*
No. 9 *Diagnosing Management Information Problems*
No. 10 *Developing a Budget*
No. 11 *Cash Management*
No. 12 *Evaluating and Starting a New Business*
No. 13 *Assessing Franchise Opportunities*
No. 14 *Assisting Professional Clients in Pricing Services Using Budgeting Techniques*
No. 15 *Developing Management Incentive Programs*
No. 16 *Improving Organizational Structure*

MAS Technical Consulting Practice Aids Series

No. 1 *EDP Engagement: Systems Planning and General Design*
No. 2 *Financial Model Preparation*
No. 3 *Financial Ratio Analysis*
No. 4 *EDP Engagement: Software Package Evaluation and Selection*
No. 5 *EDP Engagement: Assisting Clients in Software Contract Negotiations*
No. 6 *Assisting Clients in the Selection and Implementation of Dedicated Word Processing Systems*
No. 7 *Litigation Services*
No. 8 *Mergers, Acquisitions, and Sales*
No. 9 *Improving Productivity Through Work Measurement: A Cooperative Approach*
No. 10 *EDP Engagement: Implementation of Data Processing Systems Using Mainframes or Minicomputers*
No. 11 *Conversion to a Microcomputer-Based Accounting System*
No. 12 *Assisting Clients in Developing an Employee Handbook*
No. 13 *Microcomputer Security*
No. 14 *Microcomputer Training*
No. 15 *Disaster Recovery Planning*

MAS Practice Administration Aids Series

No. 1 *Developing an MAS Engagement Control Program*
No. 2 *Cooperative Engagements and Referrals*
No. 3 *Written Communication of Results in MAS Engagements*
No. 4 *Starting and Developing an MAS Practice*
No. 5 *Communicating With Clients About MAS Engagement Understandings*