PB84-189836

Guidelines for Contingency Planning NASA (National Aeronautics and Space Administration) ADP Security Risk Reduction Decision Studies

MITRE Corp., McLean, VA

Prepared for

National Aeronautics and Space Administration
Washington, DC

Jan 84

PB84-189836

Guidelines for Contingency Planning

David W. Mastbrook
Frederick G. Tompkins

November 1982

MTR-82W203

SPONSOR:
NASA
CONTRACT NO.:
NASW-3425
PROJECT NO.:
1915F
DEPT.:
W-27

Prepared for the
National Aeronautics and Space Administration

The MITRE Corporation
Metrek Division
1820 Dolley Madison Boulevard
McLean, Virginia 22102

50272-101

REPORT DOCUMENTATION PAGE	1. REPORT NO.	2.	3. Recipient's Accession No. PB84 189836

4. Title and Subtitle
Guidelines for Developing NASA ADP Security Risk Reduction Decision Studies

5. Report Date
January 1984

6.

7. Author(s)
Frederick G. Tompkins

8. Performing Organization Rept. No.
MTR-83W238

9. Performing Organization Name and Address
The MITRE Corporation
Metrek Division
1820 Dolley Madison Boulevard
McLean, VA 22102

10. Project/Task/Work Unit No.
1915L

11. Contract(C) or Grant(G) No.
(C) NASW-3425
(G)

12. Sponsoring Organization Name and Address
National Aeronautics and Space Administration
400 Maryland Avenue, S.W.
Washington, DC 20546

13. Type of Report & Period Covered
Final

14.

15. Supplementary Notes

16. Abstract (Limit: 200 words)

This report presents guidance to NASA Computer Security Officials for determining the acceptability or unacceptability of ADP security risks based on the technical, operational and economic feasibility of potential safeguards. The report also views the risk management process as a specialized application of the systems approach to problem solving and information systems analysis and design. Guidance is presented on reporting the results of the risk reduction analysis to management. Report formats for the risk reduction study are provided.

17. Document Analysis a. Descriptors
Computer Security, ADP Security, Risk Analysis, Risk Assessment, Risk Reduction Analysis, Systems Analysis and Design

b. Identifiers/Open-Ended Terms

c. COSATI Field/Group

18. Availability Statement:	19. Security Class (This Report)	21. No. of Pages
Release Unlimited	Unclassified	64
	20. Security Class (This Page)	22. Price

ABSTRACT

This report provides guidance for the preparation of contingency plans for NASA Data Processing Installations (DPIs). Contingency plans are necessary for every DPI providing essential ADP support and are required by OMB Circular A-71, Technical Memorandum No. #1. A simple, but thorough, methodology for contingency planning at NASA Centers is presented. The methodology is flexible enough to allow managers of large and small DPIs to design plans adequate for their specific needs. The contingency plans are composed of three separate plans: the Emergency Response, Emergency Backup, and Emergency Recovery Plans. A team concept is presented for meeting the requirements of each plan. A suggested format is presented for all three plans, including a description of a common appendix for the three plans.

TABLE OF CONTENTS

TABLE OF CONTENTS

(continued)

TABLE OF CONTENTS

(concluded)

LIST OF ILLUSTRATIONS

1. INTRODUCTION

The Office of Management and Budget (OMB) Circular A-71, Transmittal Memorandum No. 1, dated July 27, 1978, requires all Executive Branch Departments and Agencies to develop and implement computer security programs. This document provides guidelines for developing contingency plans for Data Processing Installations (DPIs) which is one aspect of NASA's overall computer security program. It is intended to offer an approach for providing the DPI manager with a predefined course of action in the event of a disaster. A contingency plan, to be comprehensive, must address three elements: (1) emergency response, (2) backup operations, and (3) recovery actions. Contingency plan documentation should be brief, tested on a recurring basis, and modified as changes in the data processing workload dictate.

NASA is well into the computer security program development phase in compliance with OBM Circular A-71, TM1. NASA Management Instruction (NMI) 2410.7, "Assuring Security and Integrity of NASA Data Processing" has been issued; Computer Security Officials (CSOs) at the Center, DPI, and applications level have been appointed; Center level management instructions have been developed; and computer security guidelines have been published to address performance of risk analysis, definition of security requirements for application software, and certification of existing sensitive application software.

In March 1981, the U.S. Department of Commerce, National Bureau of Standards published, FIPS PUB 87, "Guidelines for ADP Contingency Planning". FIPS PUB 87 was prepared to provide management personnel with information on which workable, usable contingency plans for ADP facilities can be developed and implemented. This report, based on FIPS 87, presents a methodology for developing contingency plans which utilizes a definitive team concept and a documented set of predefined actions. DPIs, by following the approaches presented herein, should be able to develop contingency plans which will:

(1) Minimize the impact and extent of damage to DPI operations.

(2) Provide an alternative operations strategy in the event of a disaster.

(3) Provide a systematic process for recovery and restoration of normal operations.

It is recommended that the reader obtain and have available a copy of FIPS 87. Furthermore, a copy of the Guidelines for Selection of Backup Strategies (MITRE MTR-82W00204, November 1982) should be used as a companion document throughout the development of a contingency plan. Additional background information which may be helpful to the reader is also available (References 8, 9, and 10).

The guidance provided herein may be modified by the NASA Centers, individual NASA DPIs or, with NASA approval, by the contractors who develop contingency plans for NASA DPIs. The guidance and contingency plan development cycle may also be modified to suit the specific needs of a DPI, commensurate with its size, computer configuration, and operations environment.

1.1 Purpose

The purpose of this document is to provide NASA DPIs with guidance on preparation of contingency plans which are adequate to (1) meet Federal and Agency requirements and (2) provide a realistic, yet cost effective, course of action to meet disasterous situations. This guidance addresses the contingency planning needs of all NASA DPIs. The formats specified, although designed for the larger DPIs, can be modified to suit the needs of small ones by combining elements of the plans.

1.2 Scope

The guidelines presented in this document are designed to plan for situations which may result in a major outage caused by catastrophic fires, earthquakes, bomb explosions, etc. Minor outages that normally occur on a routine basis, such as a CPU outage due to "normal" hardware failure, are not addressed by these guidelines. However, many remedies suggested in the guidance are applicable to those minor outages. Day-to-day management practices should be sufficient to handle most recurring minor problems. This guidance is sufficiently flexible to allow individual DPIs to adjust the process to meet their own needs and specific requirements. For example, managers of smaller DPIs may reduce the level of detail. A small DPI may be thought of as one that uses computers no larger than an HP-3000 or DEC VAX system.

1.3 Key Action Items in Contingency Planning

Contingency plan developers must accomplish a series of actions to assure that plans are both comprehensive and usable. Lack of a good plan may ultimately result in minor damage causing major problems. A good plan, on the other hand, may result in reducing the losses attendant to a major disaster. The action items which should be accomplished by contingency plan developers, maintainers, and managers are:

(1) Document the Existing Environment. Review and document the current equipment configuration, identify critical applications, and understand the risk environment.

(2) Select a Backup Strategy. A thorough understanding of a previously selected backup strategy is vital to the contingency plan.

(3) Establish Emergency Response Teams. Specific team members should be identified. Team assignments must be documented to ensure that a predefined set of actions will be accomplished during an actual emergency situation.

(4) Develop the Emergency Response Plan. The Emergency Response Plan details specific actions to be accomplished upon discovery of an emergency or potential emergency.

(5) Develop the Backup Plan. The Backup Plan details the actions to be accomplished when alternate operations must be initiated following the management decision to utilize other than normal data processing facilities.

(6) Develop the Recovery Plan. This plan identifies the activities to be performed to resume normal operations at a primary site.

(7) Develop Test Plan. The test plan should provide for various types of tests of the contingency plan elements to ensure that personnel can function effectively in the event that the plan, or any portion, must be activated.

1.4 Overview of the Report

First, an overview of the document and concepts is discussed in Section 2. Next, team utilization is discussed in Section 3. Documentation requirements for the plans are presented in Section 4. Sections 5, 6 and 7 discuss the three component plans which comprise the contingency plans document. Finally, Section 8 deals with plan execution and testing.

2. OVERVIEW OF CONTINGENCY PLANNING

Contingency planning, frequently referred to as disaster recovery planning, is an accepted and recommended management practice. It provides well thought-out responses to preclude and/or mitigate potentially disruptive events. Contingency planning is a management control process for anticipating emergency situations and developing strategies to cope with those emergencies. Contingency planning should be based on a risk analysis which identifies critical applications and weighs the threats and vulnerabilities related to DPI operations.

While the actual content, in terms of level of detail, will vary between small and large DPIs, the basic planning process and overall methodology is identical. The concepts and guidelines presented herein are based on the total destruction of a large DPI.

2.1 Concepts

NBS FIPS PUB 87, "Guidelines for ADP Contingency Planning," indicates that:

> "A reasonable and systematic approach to contingency planning and documentation demands adherence to a carefully conceived structure. This structure is needed to:
>
> - Assure that all important areas are addressed.
> - Permit ease of reference to sections of immediate interest or concern.
> - Facilitate revision by minimizing the effect on the whole document in limited areas of concern.
>
> Therefore, unless there is a solid justification for doing otherwise, the documented plan should be in a loose-leaf form, highly sectionalized, with each page numbered and dated and with means provided to identify changes from the previous version of each page."

The guidance in this document embodies the intent of the structure discussed in FIPS PUB 87, and is based on four fundamental concepts which are similar to those presented in FIPS PUB 87. These four fundamental concepts are:

1. Preliminary planning is the basic driver of actions to be taken in the succeeding steps and requires:
   a. Obtaining management commitment
   b. Selection of a backup strategy.

2. Establishment of a team structure which serves as a predefined alternate organization. Each team and its members must be familiar with their respective activities, if the contingency plan is to succeed.

3. A set of three plans which specifically support

   a. Emergency response operations
   b. Backup operations
   c. Recovery operations.

4. Devising of test plans which adequately and reliably exercise the contingency plans. Test plans should be developed which provide experience to team members. Testing also should be used to evaluate the procedures in terms of operational feasibility.

Each of the concepts is essential to the overall workability and effectiveness of the contingency plan. No one concept is more important than the others. The concepts work together and follow the flow discussed in the key action items identified in Section 1.3.

2.2 Preliminary Planning

As indicated above, preliminary planning consists of three activities; obtaining management commitment, performance of a risk analysis, and selection of a back-up strategy. Risk analysis and selection of a backup strategy are the primary data collection and analysis activities which support the development and ultimate execution (test or live) of the contingency plan.

2.2.1 Management Commitment

ADP facilities provide a vital service to most, if not all, organizational elements. The senior management of these facilities must keep the consequences of any loss or damage to such vital services within tolerable limits. It is incumbent on management to recognize that their commitment is a key element in maintaining continuity of ADP operations in an effective and usable contingency plan. Furthermore, as stated in FIPS PUB 87:

> "Economic feasibility in contingency plans requires carefully derived decisions as to what organizational functions are deferrable and for how long."

The responsibility of this commitment is demonstrated in the following manner:

- Directing the establishment of contingency plans
- Directing the support of the planning process by organizational units
- Directing the initial and periodic tests of the plan
- Directing the periodic revision and update of the plan upon the occurrence of changes in facility operations and at a time commensurate with the risk and magnitude of loss and harm which could result from disruption of data processing support

2.2.2 Risk Analysis

Contingency planning should be developed with the full awareness of those system functions that are supported by ADP resources. Knowledge of the susceptibility of these ADP

resources to harm and the consequences therein drive the contingency plan. Risk analysis is a process which identifies the areas of potential loss and quantifies the consequences of loss. Risk analysis provides a basis for the identification, selection, and cost-justification of potential security measures to reduce the postulated losses. For further discussion of risk analysis refer to References 1, 5, 7, and 11.

Risk analysis documentation should provide contingency plan developers with some basic data needed for the various documents. Data collection activities generally include the following:

- Identification of critical applications
- Determination of "vaulting" requirements
- Determination of backup computer equipment
- Identification of supplies and unique resources
- Identification of input/output requirements
- Identification of data or telecommunication requirements

In the NASA environment, risk analyses are performed on computer facilities. The risk analysis products most useful to contingency planning are computer hardware configuration listings, current off-site storage inventories, listings of special forms and supplies, and data communication schematics. The security controls which are recommended for implementation can also serve to meet security requirements for alternate (backup) facilities/operatons.

2.2.3 Selection of Backup Strategy

Utilization of a backup site provides a means of accomplishing essential data processing tasks, subsequent to disruption of the ADP operations. Data processing activities performed under the backup plan continue until the facility is sufficiently restored or replaced. Backup may involve one or more strategies (actions). Selection of appropriate backup strategies is the core of the contingency plan. However, selecting and documenting the strategy is not sufficient to assure continuity of ADP operations during emergency or disaster situations. Once the backup strategy has been selected, the next step is to establish a team structure. Detailed guidance on backup strategies can be found in the "Guidelines For Selection of Backup Strategies" (MTR82W00204).

2.3 Contingency Plan Teams

A contingency plan, regardless of how well it is structured and documented, cannot guarantee an effective and efficient response to an emergency situation. The plan must be executed by knowledgeable, skilled, and experienced personnel. Without the necessary people, there can be no recovery. The organization of personnel into a structure which parallels the functional activities of the DPI is strongly recommended. An organization such as depicted in Figure 2-1 is suggested as a minimum team concept.

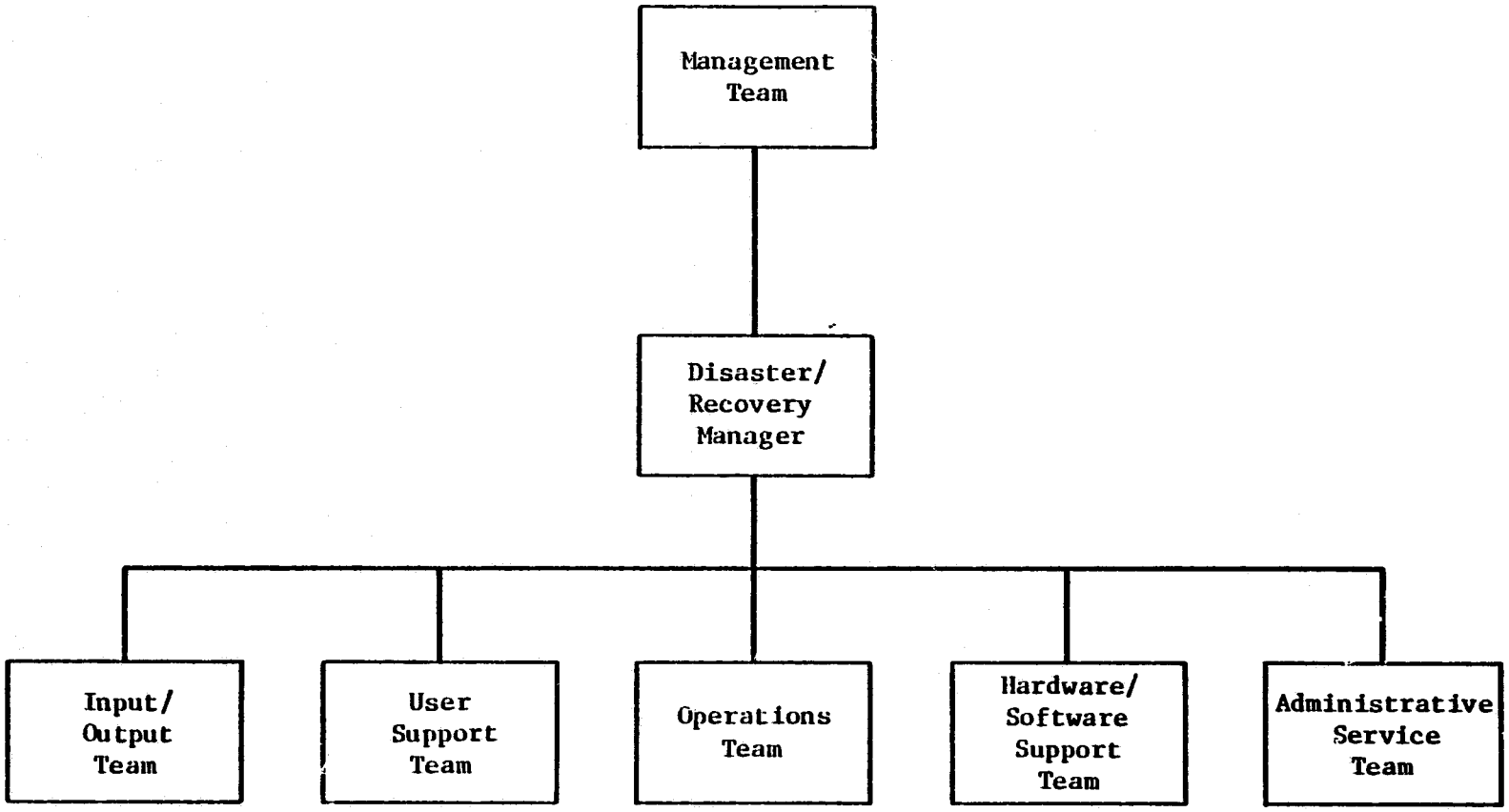


FIGURE 2-1
ORGANIZATION OF DISASTER/RECOVERY TEAMS

The Management Team - consists of management personnel with the authority to enact provisions of the emergency response plan that have financial, personnel, or operations related impacts. Section 3.1 provides additional guidance on the management team.

The Disaster/Recovery Manager - responsible for coordinating all activities of the Emergency Response Teams during and immediately following the enactment of the contingency plan. Section 3.2 provides additional guidance on the duties of the Disaster/Recovery Manager.

The Input/Output Team - responsible for assisting/retrieving the vital records from the off-site storage area and establishing and maintaining input/output operations at the alternate site. Section 3.3 provides additional guidance on the Input/Output Team.

The User Support Team - responsible for interface between the user and the alternate DPI operations. Its primary function is to make users aware that the DPI is operating under emergency conditions and assure user satisfaction under existing constraints. Section 3.4 provides additional guidance on the duties of the User Support Team.

The Operations Team - responsible for establishing operational capability of the computer equipment in conjunction with the Hardware/Software Team and to notify the Input/Output Team when the DPI is ready to begin or resume processing. Section 3.5 provides additional guidance on the duties of the Operations Team.

The Hardware/Software Team - responsible for bringing up the computer hardware and system software in conjunction with the Operations Team. Section 3.6 provides a more detailed discussion of this team's duties.

The Administrative Services Team - responsible for administrative support tasks such as purchasing, travel, clerical, and legal/public relations during emergency operations. Section 3.7 provides more details concerning the responsibilities of this team.

The team structure described above is appropriate for large DPIs. The number of personnel assigned to each team will vary depending on the size of the DPI. Small (e.g. mini-computer) DPIs may combine some team functions. In an actual disaster, some of the primary team members may be incapacitated or unable to reach the DPI, therefore, alternate personnel should be assigned to each team.

2.4 Contingency Plan Components

A comprehensive plan of well thought-out procedures for handling contingency situations should be broken down into three distinct components: the emergency response plan, the backup operations plan, and the recovery plan. Figure 2-2 illustrates the relationship of these components.

2.4.1 Emergency Response Plan

The computer center, its equipment, and the operating personnel are essential to the organization's mission. Emergency response procedures include the immediate actions to be taken to protect life and property and to minimize the impact of the emergency. Section 5 presents a detailed discussion on the contents of the emergency response plan.

2.4.2 Backup Plan

This plan should describe what must be done to initiate and effect backup operations. The plan should be based on the selected backup strategy. Section 6 provides detailed guidance on developing the backup plan.

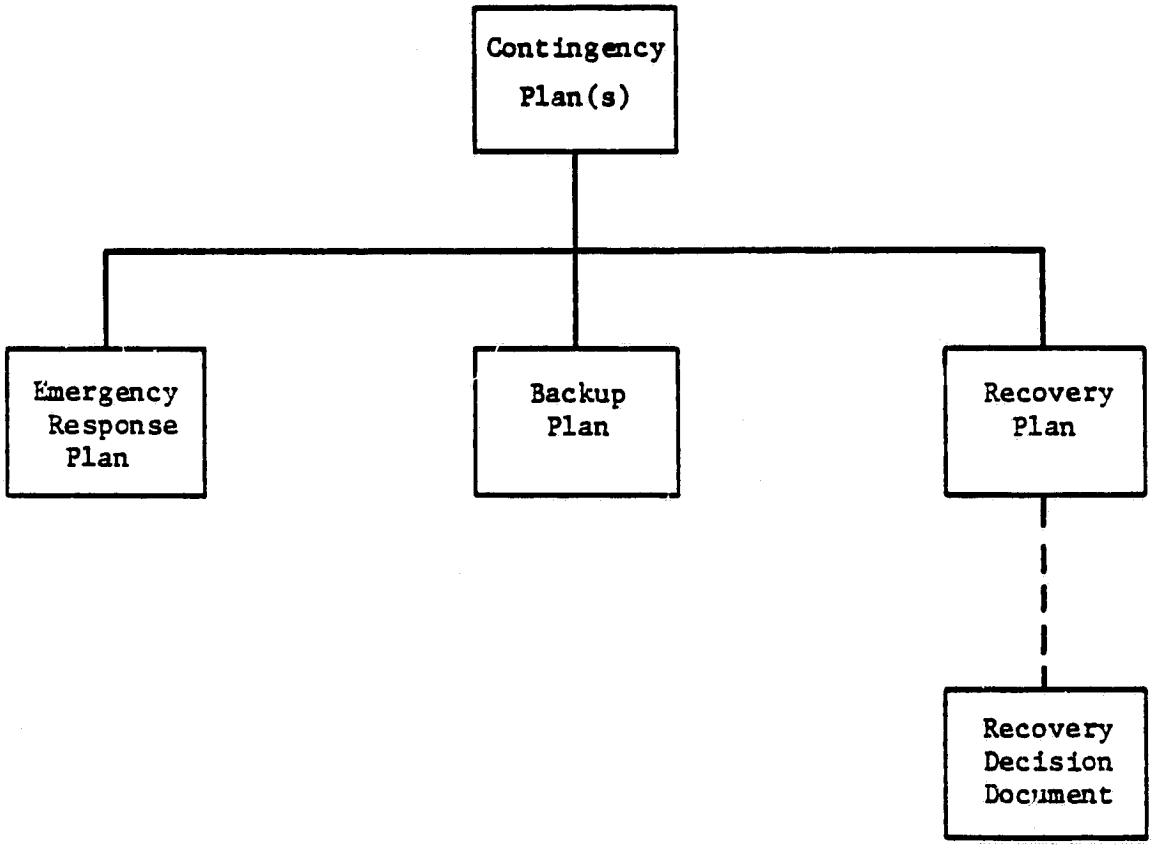


FIGURE 2-2
RELATIONSHIP OF COMPONENT PLANS

2.4.3 Recovery Plan

The restoration, reconstruction, or new construction of a computer center is a large, complex project. A recovery plan should be developed to permit the resumption of normal operations in the most efficient and cost-effective manner. An analysis of alternatives should be documented in a recovery decision document. Section 7 provides additional guidance on the recovery plan and the attendant recovery decision document.

2.5 Contingency Plan Execution and Testing

One of the most important aspects of successful contingency planning is the continued testing and evaluation of the plan. Test plans should be developed to exercise the plan thoroughly. Actual tests should be conducted to build experience in the areas of time response of team members, to determine weak or inappropriate procedures, and to train newly assigned personnel. Figure 2-3 illustrates the actual decision process and how each of the plans described in Section 2.4 relate to the contingency process.

Section 8 provides more detailed guidance on testing and execution.

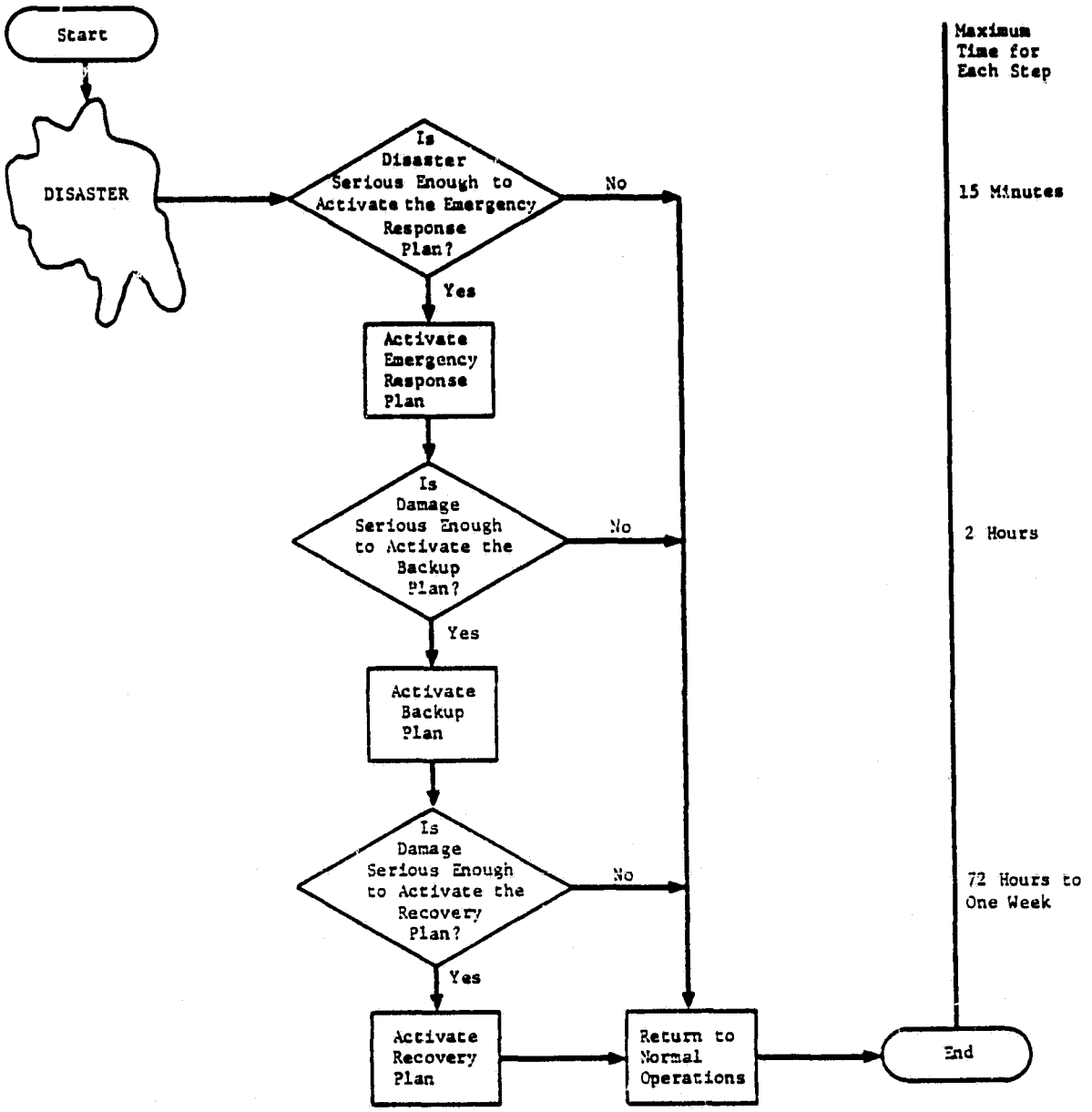


FIGURE 2-3
PROCESS INVOLVED IN IMPLEMENTATION OF CONTINGENCY PLANS

3. TEAM UTILIZATION

A team concept has been recommended for implementing the three component plans. Smaller DPI's may utilize individuals in lieu of teams to accomplish the same functions performed at larger DPIs. Team leaders of the various functional areas should be involved in the definition of functions and responsibilities for each area. Therefore, team leaders should be chosen early to assist in the development of contingency plans. Team leaders and members should be chosen on the basis of expertise and knowledge of the team's functional area. The team responsibilities vary across all three component plans and team size (Figure 3-1 illustrates the relationship of teams to plans). Items of importance in defining team responsibilities are as follows: the size of the DPI, the number of applications run, the backup strategy selected, skill and availability of personnel, and user service needs. Large DPIs which function as service bureaus may wish to augment the teams with user representatives.

TEAM	EMERGENCY RESPONSE PLAN	BACKUP PLAN	RECOVERY PLAN
MANAGEMENT	X	X	X
DISASTER/RECOVERY	X	X	X
I/O TEAM	N	X	X
USER SUPPORT	N	X	X
OPERATIONS	N	X	X
HARDWARE/SOFTWARE SUPPORT	X	X	X
ADMINISTRATIVE	N	X	X

N = NOTIFY, X = INVOLVEMENT

FIGURE 3-1
RELATION OF TEAMS TO THREE PLANS

3.1 Management Team

The management team should be staffed with high level managers who have either (1) oversight responsibilities for the DPI, (2) direct management responsibilities for the DPI, or (3) who manage user organizations which would be primarily affected by a DPI outage. Responsibilities for the management team should include:

- Damage Assessment
- Decision to Activate Emergency Response, Backup or Recovery Plans
- Activation of the Disaster Recovery Control Center
- Management Direction
- Monitoring of Recovery Activities
- Documentation of Progress and Decisions

The management team works in concert with the disaster/recovery manager. The disaster/recovery manager should act as an extension of the management team and operate under the team's oversight and direction. The size of the management team should be limited to three to five members. Primary candidates should include the data processing manager, the computer operations manager, and the manager of applications software.

3.2 Disaster/Recovery Manager

The disaster/recovery manager is the person with authority and responsibility to manage disaster/recovery operations. The five disaster/recovery teams should report directly to this

person. The position falls under the policy and management guidance of the management team. The disaster/recovery manager is the focal point of the entire disaster/recovery operation. Both the disaster/recovery manager and individual members of the management team should have independent authority to activate the emergency response plan. However, activation of the backup and recovery plans should be a joint decision.

3.3 Input/Output Team

The responsibility of the input/output team is to assure effective input/output operations. All steps necessary for input/output are the responsibility of this team including pickup and delivery. Responsibilities of this team should include the following:

- Retrieving Off Site Data
- Entering Data
- Pickup-Delivery of Input/Output
- Scheduling Data Entry
- Coordinating Input/Output
- Assuring Adequate Input/Output Supplies
- Setting Up Computer Runs
- Handling Forms
- Establishing New Distribution Points
- Maintaining Logs and Schedules
- Distributing Supplies

The input/output team should work closely with the user support team.

3.4 User Support Team

The user support team serves as the direct interface between the users and the DPI. Functions for this team should include the following:

- Notification of Users About the Disaster
- Maintainance of Priorities for the Applications Runs
- Resolution of User Problems
- Notification to Management about Special User Problems
- Reprioritization of Applications, When Necessary
- Development of Alternative Operation Strategies
- Implementation and Design of New Facilities
- Notification of Vendors

Once the backup plan has been operational for a period of time, the focus of this team's work will change from user assistance to new facility design and implementation (see Figure 8-1). Planning for a new facility is a large task, so this team will work closely with the hardware/software team which has primary responsibility for recovery planning and implementation.

3.5 Operations Team

The operations team is responsible for direct operation of the backup CPU and peripheral equipment. This team works closely with the hardware/software support team to restore the main CPU. Specific recommended functions are as follows:

- Activate Backup Facility
- Restore System Software
- Restore Data and Files
- Restore Application Software
- Assure System Integrity
- Restore Data Security Procedures and Systems
- Notify User Support and Input/Output Teams When Operating
- Order Required Supplies
- Operate in Backup Mode Indefinitely

The operations team should be staffed with personnel having systems programming, computer operations, and software programming experience.

3.6 Hardware/Software Support Team

This team consists of hardware and software specialists. They work closely with the operations team by providing basic assistance necessary for operations. Recommended functions for this team are:

- Assessing Damage to the CPU, Peripheral Equipment, and System Software
- Establishing Communications Between the Backup Site and the Users
- Assuring Adequate Job Control Language to Run Applications
- Assuring Availability of Systems and Application Software
- Assuring Adequate Documentation is Available
- Conducting Salvage Operations
- Coordinating Recovery Operations
- Planning for New Hardware
- Assisting in Procurement of Hardware

After the backup plan is implemented, this team begins work on the overall recovery operations effort. This team has primary responsibility for coordination of recovery activities. It works closely with the user support team and the administrative service team.

3.7 Administrative Service Team

The administrative service team provides the major administrative support services for the overall disaster/recovery operations. Functions may be assigned to individuals with direct authority in these areas, or may be coordinated through individuals with other organizational components having authority. The basic functions are:

- Security, Safety, Medical, Damage Containment
- Purchasing, Supplies, Contracts
- Travel, Transportation
- Legal/Public Relations
- Clerical Support
- Personnel
- Facilities, Communications (Phones)
- Services for Recovery Planning

This team works closely with the disaster/recovery manager to provide the support services needed for effective emergency, backup, and recovery operations.

4. DOCUMENTING THE CONTINGENCY PLAN

The format of the contingency plan documentation should be structured to ensure ease of use and to permit all persons to become familiar with their respective roles. The first step is to develop a basic outline. NBS FIPS PUB 87, APPENDIX ONE, presents an outline with three parts which address preliminary planning, preparatory actions, and the action plan, respectively. This format corresponds to the discussion presented in Section 3 of FIPS PUB 87. As an alternative, the outline presented in Appendix A of this document can be used in developing contingency plans for NASA DPIs. The major difference between the outlines is that in the FIPS PUB 87 version the outline is contained within the basic plan documentation. The outline presented in Appendix A includes the procedural information in the basic document and places the data most subject to change in a number of appendices.

A loose-leaf binder, subdivided with tabs, is recommended for the entire document. Each plan should be designed so that it can be removed as an entity. All pages should be dated. Tabular subsections for the teams should include the following items:

- List(s) of team members and alternates.
- Description of team responsibilities.
- Description of specific procedures to be followed.
- Flow chart(s) of procedures the team must conduct.
- Team modification procedures.
- Check list(s) of tasks to be performed.
- Check list(s) of supplies and resources needed.
- Special descriptions of each team.

This design will allow team members to be presented with all necessary information for their function. Instructions should be simple and to-the-point. The teams should not be burdened with too much information.

4.1 Contingency Plan Appendix

One common appendix for all three plans is recommended. The appendix should contain the following types of information:

- Emergency notification list--names and telephone numbers for the disaster/recovery manager, fire, police, etc.
- Master calling lists for team members and alternate members
- Critical applications lists (See Reference 4)
- Storage retrieval check lists
- Maps and directions to backup site and operations center
- Hardware/software inventories
- Example forms for procurement, travel, etc.
- Backup supplies check list
- Vendor contacts
- Backup test reports
- Initial meeting places for team members

- Facilities, communications, and utilities contracts
- Data entry forms
- Strategy documentation from backup plan (See Reference 4).
- Communications requirements
- Summary of personnel requirements to run backup operations organization charts

4.2 Distribution

Team members should have portions of each plan applicable to their specific function so that the team gets an overview of its own functions across all three plans. Personnel with oversight responsibility should receive all three complete plans. Distribution should be limited because security is a concern and system vulnerabilities can be exploited, if information in the plans is disclosed.

5. EMERGENCY RESPONSE PLAN

The purpose of the Emergency Response Plan is to provide specific, easy to understand instructions for responding to emergencies which may cause serious harm or damage. The plan should not be voluminous, but it should reference sources necessary for detailed information, where required. As mentioned previously, this plan is a separate section of the contingency plans document. Specific subjects which will be discussed below in regard to this plan are:

- Purpose
- Development
- Types of Disasters
- Scenarios
  - Decision to Evacuate
  - Evacuation Procedures
- Notification Process
- Computer Power-Down Procedures
- Damage Containment
- Decision to Implement the Backup Plan
- Securing the DPI

5.1 Development

This plan should be developed in concert with center level security personnel. Many of the emergency procedures pertaining to each DPI will be strongly influenced by policy and procedures developed by safety/security personnel with

oversite for each center. External agencies such as GSA and the Federal Protective Service may have responsibilities affecting this plan. Therefore, a first step in the development is to get input from the center security/safety officers.

5.2 Emergency Detection

An emergency situation must first be detected before a response can be initiated. Other than a sudden, unpredictable natural disaster like an earthquake, many disasters are reported or forecast on the news media. In cases where advance notice is given, responsibility for monitoring the news is usually delegated to full-time security personnel. As part of the installation notification process for the center, provision should be made for these personnel to notify the DPI Computer Security Official, disaster/recovery manager member of the management team, or other appropriate official directly.

Other disasters may occur without warning. This type of disaster, such as a fire or water damage, may be detected by personnel or by detection systems. Such systems may have local and remote reporting capabilities. The type of detection systems may include the following:

- Intrusion
- Closed Circuit TV
- Heat
- Smoke
- Water

Once a system is activated, procedures for notification of appropriate security/management personnel and evacuation, etc., should be clearly specified and posted in the DPI.

5.3 Emergency Response Scenarios

Emergency response procedures will depend on the type of emergency at hand, e.g., a minor fire will certainly require a different response than a bomb threat. The DPI emergency plan may include specific responses for the following types of situations:

- Minor Fire
- Major Fire
- Bomb Threat
- Major Storm or Earthquake
- Flood

The specific scenarios included or added to the above list will depend on the DPI itself. Each scenario should include the specific steps involved in responding to each type of emergency. The steps involved may vary from notification of the disaster/recovery manager to immediate evacuation of the DPI.

The decision to evacuate should be assigned to management team members, the disaster/recovery manager, or appropriate safety personnel. The responsibility for making such a decision should be clearly shown in the plan. Personnel who are likely to be acting for officials in their absence should also be

listed. During after hours operation, the responsibility should be delegated to the managers, safety officials, or supervisors on duty at the time of the emergency situation. Both on-duty and off-duty phone numbers for these officials should be included. The decision to evacuate may also be made by "other" authorities having jurisdiction over the center such as the GSA, Federal Protective Service, or local police and fire officials.

5.4 Notification Process

Once the evacuation decision is made, the plan should clearly outline the process for notifying employees, team members, and users. A suggested notification sequence is as follows: responsible management officials should be notified first; supervisors should be notified next who should, in turn, notify employees and team members; team members will notify users. In situations where the evacuation decision is made by DPI or center personnel, procedures for notification of non-NASA authorities should be specified clearly.

As mentioned earlier, phone numbers for management and DPI security officials both for after-hours and office hours should be included in the plan appendix along with alternates who may be in charge. The management official responsible for activation of the emergency response plan should notify the disaster/recovery teams. In order to expedite notification, a calling tree may be used.

5.5 Computer Power-Down Procedures

In certain emergencies, the computer systems should be powered-down and shut off, and the operations personnel should evacuate the building. If the emergency occurs in or directly effects the computer room, emergency shut down procedures should be employed. If there is a threat to life, all personnel should be evacuated immediately. The protection of the equipment is secondary to the protection of life. Computer system manuals needed as references to power-up and power-down the computer should be stored in the computer center and at the off-site backup records storage facility (in case the on-site copy is destroyed).

5.6 Damage Containment

Steps and equipment necessary to contain and limit damage in an emergency situation may be specified in the DPI Risk Analysis. If not, these procedures should be defined and equipment necessary to reduce security vulnerabilities should be provided.

Containment process activities for each situation will depend on the nature of the emergency. Step-by-step procedures for the various types of emergencies should be specified. For example, in the case of a small fire in a piece of hardware the following scenario may apply:

1. Turn off the hardware
2. Use a Halon or can fire extinguisher on the fire
3. If the fire is out, notify management and safety personnel

4. If the fire is not out,

   - activate room halon system, if not already activated
   - pull fire alarm
   - leave area
   - evacuate the building

5. Notify the management team.

In other cases, such as a slowly leaking roof, covering hardware with plastic sheeting and powering down may be an adequate procedure.

5.7 Decision to Implement the Backup Plan

Once the DPI has been evacuated, a preliminary assessment of damage should be conducted by the management team and/or disaster/recovery manager. Based on the damage surfaced by this assessment, a decision on whether or not to activate the backup plan will be made. If the decision is made to do so, the security of the installation should be considered.

5.8 Securing the DPI

Damage to a particular DPI may be such that extra security should be taken immediately to protect hardware, software, and data. It may be necessary to provide guards around the clock until security measures can be adjusted to compensate for the emergency situation. The DPI computer security official should be part of the damage assessment team. Based on damage assessment decisions made, he should decide whether or not to increase security measures at the installation to compensate for the outage.

6. BACKUP PLAN

The backup plan is the main portion of the contingency plan document. Specific concerns which will be discussed for backup plans in the following sections are:

- Role of Backup Strategy Documentation
- Notification, Assembly Points, and Directions
- Team Functions
- Emergency Operations Center
- Plan Operation
- Closing the Backup Center

DPIs should design their plans based on their unique needs. The backup plan should evolve from the previously documented backup strategy. Data used to document the backup strategies should be obtained.

6.1 Role of Backup Strategies Documentation

The documentation developed for backup strategy selection is the core around which the backup plan is constructed. For the purpose of developing the backup plan, it should be assumed that a large DPI is totally destroyed. Documentation should specify a backup strategy with an operational, alternate backup facility available to run applications immediately. Backup plans developed for strategies different from this example would also be different in structure. Backup strategy documentation should be included as an appendix to the contingency plans document.

6.2 Notification, Assembly Points, and Directions

In the case of a disaster, the disaster/recovery manager and the management team decide on implementation of the backup plan. The decision is based on the initial damage assessment conducted as part of the emergency response plan. Once the backup plan is initiated, team leaders must be notified that the plan is in effect. To accomplish this, call lists for team leaders and team members should be included as an appendix.

Each team section of the backup plan should indicate assembly points for team members. Exact directions, with maps, should be provided to allow team members to respond quickly.

6.3 Additional Functions of the Backup Teams

The recommended functions for the various teams have been discussed previously. However, there are several additional specific items which are recommended to assist teams in performance of backup operations. These items should be included under the team sections of the backup plan:

- Team Member Lists
- Notification Process when Feasible
- Check List Procedures for Functions Assigned to the Team

Check lists and procedures to assist team functions should be developed in advance. Functions which can be easily reduced to a check list format include transportation, notification, damage assessment, backup site activation procedures, and material

resources check lists. However, complex functions may not be reducable to a checklist format. In this case, the DPI must rely on the expertise of personnel assigned to those functions.

6.4 Decision Points and Backup Plan Operation

The sequence of events in the model plan shown in Figure 8-1 is designed to obtain operational capability within 24 hours of a disaster. At this point, a decision should be made by the management team as to whether or not to continue the backup plan. Assuming operations do continue, a second decision will be made on implementation of the recovery plan. (This should occur sometime between 3 days and 7 days after implementation of the backup plan.) The backup plan should be designed to operate on an indefinite basis, i.e., 3 to 6 months.

6.5 Emergency Operations Center

An emergency operations center should be selected. The emergency operations center is the management and administration command center for backup operations. Two alternatives are as follows: (1) it could be at or near the backup site, or (2) it may be located elsewhere. In the second case, if the backup site is remotely located, it may be desirable to have the operations center in the vicinity of the original DPI.

Also, close proximity of the emergency operations center to the original DPI will permit users to coordinate I/O for backup operations. Furthermore, a nearby location will be very useful in the reconstruction process in which direct control of backup operations will be more feasible. After opening the emergency center, communication should be established through phones and data links as soon as possible. In addition, office furniture and supplies will be needed for the teams.

6.6 Closing the Backup Center

Procedures for closing the backup site and switching over to the new or reconstructed center should be clearly defined for each team. Possible alternatives include: (1) gradual cut-over, and (2) dead stop--hot start. For larger systems, a gradual cutover is recommended because of the complexities of getting a new DPI on-line. Smaller systems may be able to utilize the second alternative for off-the-shelf systems. Each team's function in this plan will vary and may not be subject to exact prior definition. The disaster/recovery manager should manage this transition in coordination with the DPI staff to assure efficiency and effectiveness in the transfer of operations.

7. RECOVERY PLAN

The recovery plan addresses major functions which must be conducted in order to resume normal operations at a primary site. It is documented in the same way as the other plans with tabs for team tasks, etc.

Considerations for recovery from a total outage will be discussed in this section. The options available vary according to the extent of the disaster because of the nature of recovery operations. Thus, a lesser outage will require less work to recover, even though the disaster/recovery manager may have a comprehensive plan available.

The recovery plan centers around the development of a recovery decision document. This is a separate document which will be developed by teams during implementation of the recovery plan. Once a decision is made to implement the recovery plan, the actual recovery decision document should be developed under the direction of the disaster/recovery manager in concert with the hardware/software, the user support, and administrative teams.

Elements which should be addressed in the recovery decision document are as follows:

- Recovery Options
- Management Constraints
- Recovery Decision
- Environmental Requirements
- Hardware Requirements
- Software Requirements

Each of these elements will be discussed in the subsections below.

7.1 Recovery Options

Several alternatives should be considered in developing the recovery decision document: damaged hardware may be (1) repaired, (2) replaced one-for-one, or (3) upgraded. An influencing factor on which of these to implement is the position taken by vendors. Many vendors that lease to the government have insurance on the equipment. Therefore, the vendor may choose to replace the equipment directly or to offer incentives to upgrade to newer equipment.

7.2 Management Constraints

Management constraints may affect the selection of a recovery option. These constraints include the following:

- Cost Benefit
  - lease
  - purchase
- Timeframes
  - application requirements
  - hardware delivery
- System Software and Applications Software Interface Problems
- Resources
  - budget
  - manpower

In the above list, the budget constraints may be the most difficult obstacle. Large dollar amounts may be difficult to obtain in a short timeframe because of the budget cycle. Budgeting reallocation, however, may be a viable alternative to consider.

Furthermore, operating system upgrades may be difficult, especially if there is a large investment in system dependent software.

7.3 Recovery Decision

The recovery decision should be made as early as possible. A separate decision document should be prepared for management which discusses the positive and negative aspects of the options and constraints above. This document, developed during implementation of the recovery plan, should be prepared by the disaster/recovery manager for the signature of the management team or an appropriate management official. Alternatives should be listed and recommendations should be made.

Once management approval is obtained, the disaster/recovery manager should coordinate implementation action with the management teams involved in this plan (see Figure 8-1). Items discussed in the following three subsections are important for implementation of a major DPI repair and/or construction program.

7.4 Environmental Requirements

Some of the major environmental requirements which must be considered for recovery of a large DPI are as follows:

- Hardware Spacing
- Cooling
  - Air conditioning
  - Chilled water
- Raised Floors
- Electrical Power and Lighting

- Office Space and Equipment
- Physical Security
- Schedule to Complete Construction

A more comprehensive list of requirements can be developed from FIPS PUBS 31, 65, 73, and 87 or vendor information. For example, one vendor offers a course in laying out a design for a computer center. Other types of outside assistance may also be available.

7.5 Hardware Requirements

Some of the elements that the hardware/software team should consider for the recovery process are:

- Hardware Specifications
- Service Contracts
- Delivery and Installation Schedules
- Application Software Conversion Problems Due to System Differences
- Schedules to Complete Installation
- Schedules to Complete Testing

If a system upgrade is involved, special consideration should be given to application interface problems. Hardware performance will have to be performed following NASA and Federal regulations.

7.6 Software Requirements

A new full-performance system should run applications software as efficiently and effectively as the original system. Special concerns for software are:

- Full operating system testing before going on-line
- Interface parameter difficulties for applications and sub-systems when changes are made
- Change-over procedures for running applications when activating the new DPI
- Software security specifications

The software life-cycle processes described in FIPS PUB 38 and 73 are directly applicable to these requirements. A more comprehensive list is included in this document, and it is suggested that the FIPS 73 be available for use during the recovery.

7.7 Recovery Guidance Summary

The recovery plan is less structured than the emergency response or backup plans. This is because it is effected by the extent of the disaster and the recovery options selected from the recovery decision document. Therefore, the recovery plan is a "plan for a plan." It should be designed to put a mechanism in place to develop an adequate recovery decision document for management, (see section 7.3) and implement management's recovery decision. Background information should be available to assist the teams in implementating their emergency response tasks. The disaster/ recovery manager should work closely with the management team to assure effective implementation of the decision document.

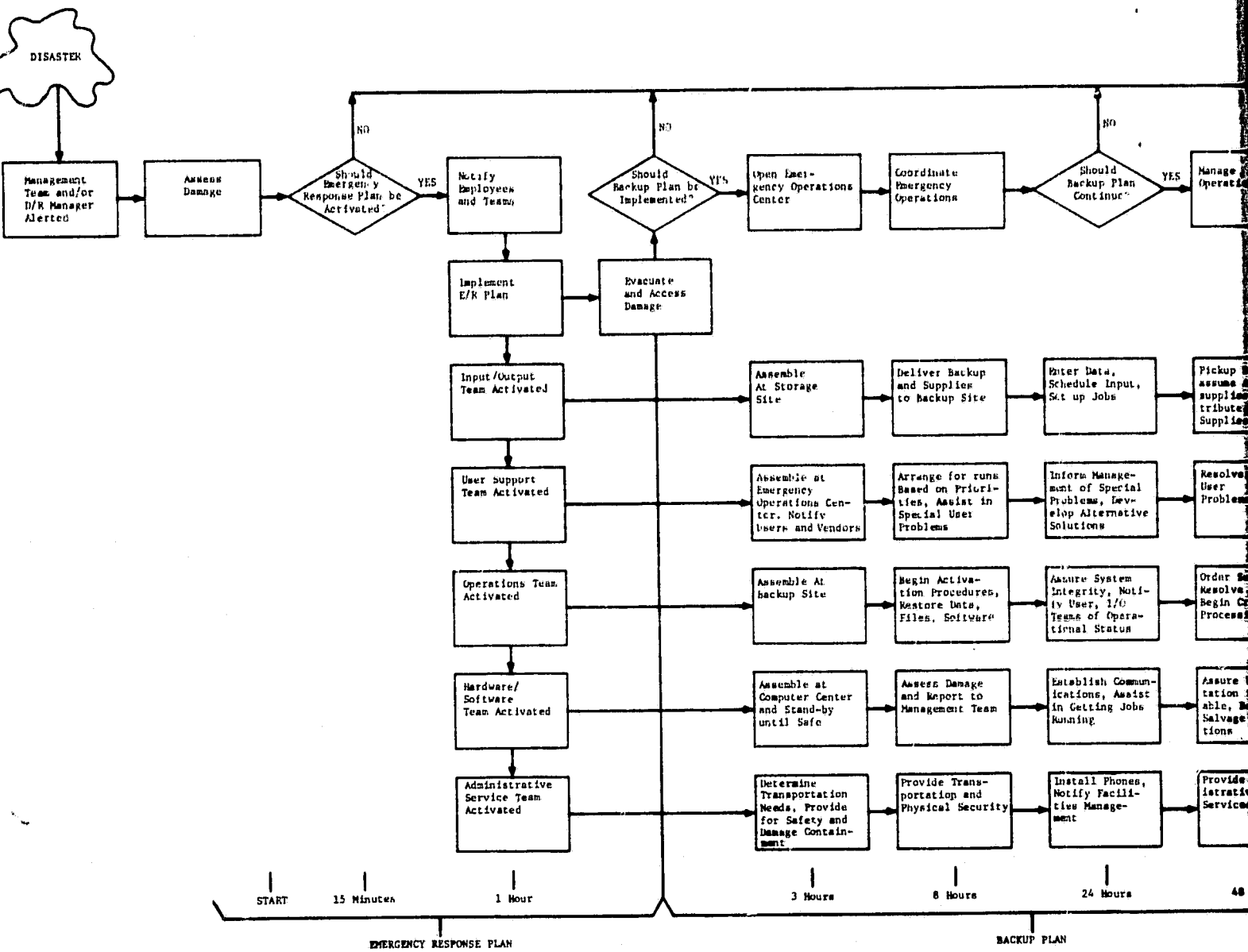
8. CONTINGENCY PLAN EXECUTION AND TESTING

The final test of the viability of the Contingency Plan is the execution of the plan (or portions) as the result of an actual emergency. Figure 8-1, provides, as a sample situation, an estimate of the elapsed time that might be experienced under very ideal conditions. However, since each organization is unique in structure, personnel and geographic environment, each DPI should conduct a number of tests to establish their own time baseline. A general description of the execution process is discussed in Section 8.1. Section 8.2 describes a series of tests which range from low or no-cost to those which will require expenditure of some budgetary resources. It is recommended that all tests be documented and the results maintained by the disaster/recovery manager.

An example can be postulated to illustrate the steps involved in plan execution and estimates of time-phasing. In the example shown in Figure 8-1, it is assumed that (1) a large DPI is totally destroyed, and (2) it will take approximately three months to reconstruct the damaged center, and (3) an operational backup site is available based on a documented strategy. The Figure shows how the plans interrelate once execution is initiated.

8.1 Time Phasing of Plan Execution

Approximately 15 minutes after a disaster, the emergency response plan can be activated as shown in the Figure. Within three hours of the disaster, team members have assembled and assessed the damages in conformance with tasks and instructions in the contingency plans. After the assessment, a decision can be made on


DISASTER
Management Team and/or D/R Manager Alerted
Assess Damage
Should Emergency Response Plan be Activated?
NO
YES
Notify Employees and Teams
Implement E/R Plan
Should Backup Plan be Implemented?
NO
YES
Evacuate and Access Damage
Open Emergency Operations Center
Coordinate Emergency Operations
Should Backup Plan Continue?
NO
YES
Manage Operati
Input/Output Team Activated
User Support Team Activated
Operations Team Activated
Hardware/ Software Team Activated
Administrative Service Team Activated
Assemble At Storage Site
Deliver Backup and Supplies to Backup Site
Enter Data, Schedule Input, Set up Jobs
Pickup assume supplie tribute Supplie
Assemble at Emergency Operations Center. Notify Users and Vendors
Arrange for runs Based on Priorities, Assist in Special User Problems
Inform Management of Special Problems, Develop Alternative Solutions
Resolve User Problem
Assemble At backup Site
Begin Activation Procedures, Restore Data, Files, Software
Assure System Integrity, Notify User, I/O Teams of Operational Status
Order Resolva Begin Process
Assemble at Computer Center and Stand-by until Safe
Assess Damage and Report to Management Team
Establish Communications, Assist in Getting Jobs Running
Assure tation able, Salvage tions
Determine Transportation Needs, Provide for Safety and Damage Containment
Provide Transportation and Physical Security
Install Phones, Notify Facilities Management
Provide istrative Services
START
15 Minutes
1 Hour
3 Hours
8 Hours
24 Hours
48
EMERGENCY RESPONSE PLAN
BACKUP PLAN

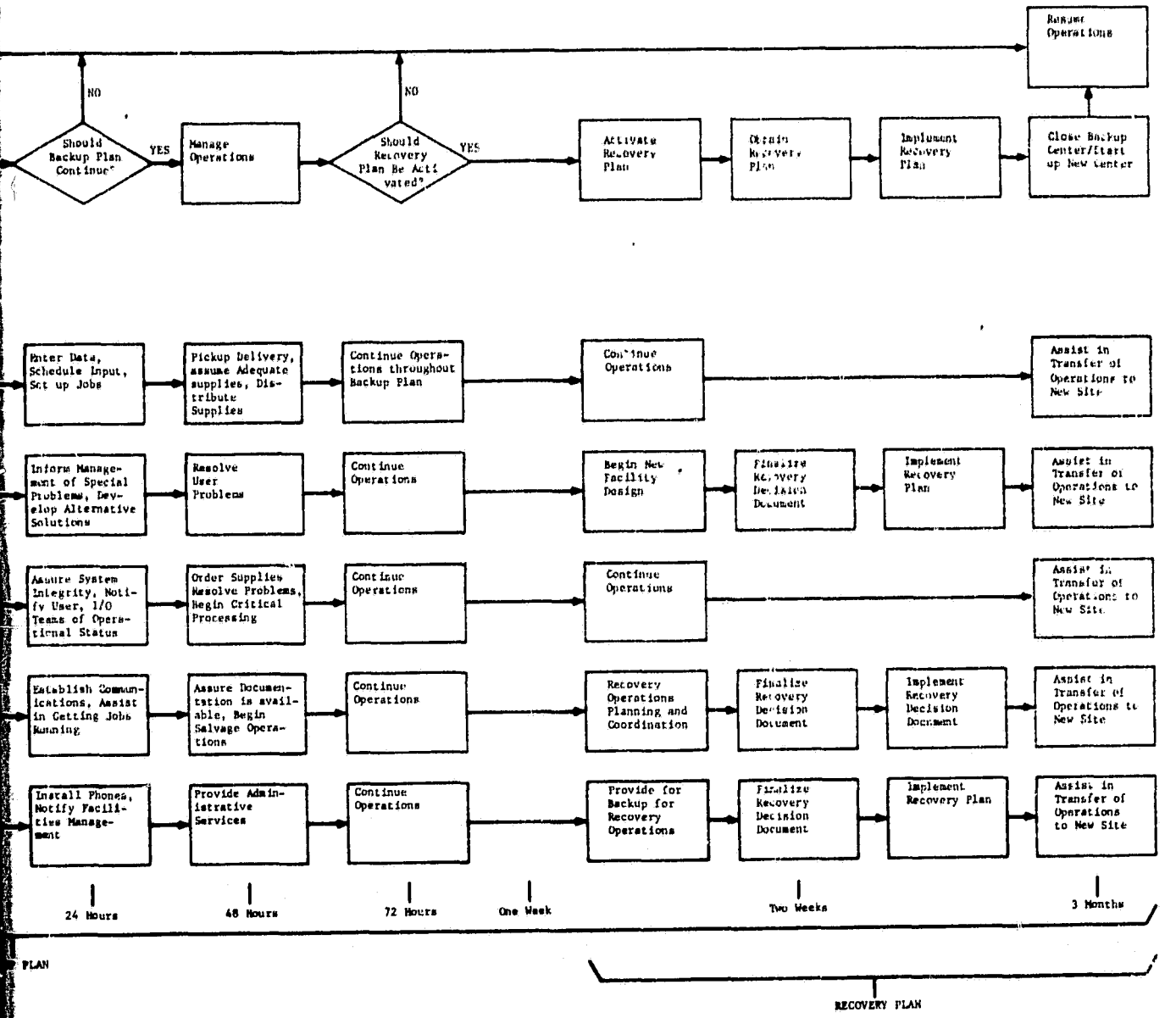


FIGURE 8-1
EXAMPLE: CONTINGENCY PLANS TIME-PHASING
(ASSUMES TOTAL DESTRUCTION OF A LARGE DI

8-3

implementation of the backup plan. When the backup plan is activated, the full alternate organization, i.e., the team structure, becomes fully operational. Teams that are not already functional assemble at predetermined points and begin performing functions outlined in the backup plan.

Seventy-two hours to one week later, a decision to implement the Recovery Plan can be made based on the situation at that time. If the decision to implement the Recovery plan is made, the user support, hardware/software and administrative service teams shift their functions. Although some backup function will continue to be performed by these teams, they will begin functions necessary to recovery. During this time frame the recovery decision document should be developed to provide management with a decision document and an implementation process to effect recovery. Figure 8-1 further illustrates that, after approximately three months, the damaged site has been reconstructed and operations are transferred back from the backup site. Each DPI should construct a similar time-phase chart to integrate team functions suitable for execution of the DPI's plans. This chart should be included in the introductory portion of the contingency plans documentation.

8.2 Testing the Backup Plan

To ensure that the contingency plans will be most useful in coping with a disaster, various parts of the plan should be exercised and refined on an annual basis. This section presents five basic levels of drills that should be performed to test the contingency plans. They are:

Level 1 Test - Verification of emergency response team member/alternate phone number.

Level 2 Test - Determine response time and emergency operations center readiness.

Level 3 Test - Determine readiness of off-site storage.

Level 4 Test - Run a selected critical system at the alternate/backup site.

Level 5 Test - Simulate a major disaster and activate the emergency response procedures.

The following sections describe the checklist items which must be observed during each type of test. Results from these tests should be evaluated and used to refine the emergency plans. Note that in this discussion, personnel are identified in terms of their "emergency only" job titles.

8.2.1 Level 1 Test - Verification of Team Member Phone Numbers

The emergency response team member/alternate phone number lists should be periodically verified. The following questions concerning these lists should be checked every 3 to 6 months to ensure that adequate key personnel are available to respond to an emergency situation.

1) Is the backup personnel list available for verification?

2) Are personnel currently assigned to each of the member/alternate slots in the team roster?

3) Are all those people currently employed at the DPI?

4) Is there a documented notification procedure?

5) Using these procedures, is it possible to contact all the team members/alternates by phone either at work or at home?

6) Was everyone contacted aware of his or her role on the team and the procedure for initial assembly of the group?

Any new information gathered during any segment of the tests should be incorporated into the plan and all copies of the plan revised accordingly. It should be verified that there are enough current copies of the plan at all times to support operations after an emergency. Copies of the plan should be distributed as follows:

a) A copy in the office and another in the home of the Disaster/Recovery Manager and his alternate

b) One at the off-site storage facility

c) One at the backup processing site

The address, phone number, and directions to both the off-site storage facility and the backup site should be in the emergency plans and should be checked annually. In addition, police, fire department, rescue squad, building security, gas company, water company, electric company, telephone company, etc. phone numbers should be included in the plan and should be checked periodically.

8.2.2 Level 2 Test - Check Response Time and Emergency Operations Center Readiness

The level 2 test is run to verify that the personnel shown on the notification lists test actually know where they are supposed to go and how long it takes to get there. Team members should be quizzed on individual responsibilities and what should be supplied to accomplish the next steps. Small informal meetings should be held with each of the individual task force teams. These meetings should consist of question and answer type drills between the team members and the emergency response coordinator. Level 2 testing should be accomplished at least once per year.

An office area with desks, chairs, telephones, and some basic supplies should be designated as the Emergency Operations Center from which all of the emergency operations are managed. A primary and secondary emergency operations center should be designated in advance. Street addresses, directions, and phone numbers of each should be documented in the plan.

After an emergency has occurred and the computer center has been secured, the emergency task force teams should meet at a prearranged point before traveling to the various facilities to do their jobs. Initial meeting points should be determined in advance. A third level backup meeting place may be needed in case of wide spread disaster. All meeting points should be documented.

The emergency response management team should be quizzed to verify that each team member knows how to locate a copy of the emergency plan. Then a copy of the plan should be provided and the team asked what they would do given a particular disaster scenario (say total destruction by tornado or fire), how long it would be expected to take, and what would be needed to do it. This approach should reveal any shortcomings in the following three major areas:

a) Does everyone know where the plans are kept?

b) Does everyone know what information is contained in the plans?

c) Is the information appropriate (too much, not enough, inaccurate, etc)?

In particular, this exercise with the management team should check the following items:

a) Have initial meeting places and emergency operations centers been formally designated?

b) Have the addresses, phone numbers, and directions to each of these been documented in the plan?

c) Are the telephones, desks, chairs, office space, and backup supplies at each of the emergency operations centers adequate for the given scenario?

d) Are these items currently in place and ready for emergency operations at the centers?

Next, the team responsible for damage assessment should be asked to submit a dummy damage assessment report to see if it contains adequate detail and is in understandable format. The other teams should be assembled and quizzed in a similar manner, given an assumed scenario and the damage assessment obtained above.

8.2.3 Level 3 Test - Determine Readiness of Off-Site Storage

A test should be conducted to test the response time for an emergency run to the off-site storage and to verify the completeness of those records and supplies.

Using the list of files developed by the Disaster/Recovery Manager under level 2 tests and a list of supplies, the input/output team should be transported to the storage facilities to pull the files and supplies which should be loaded and taken to the backup facility.

This test should be timed. The results should be used to refine the task timings for these and related tasks in the emergency plan.

The adequacy of the file and supplies backup listings and procedures can be verified and refined as necessary using this test. Also, the ease of making transportation arrangements can be judged. Any weaknesses found in the timing estimates, procedures, or information contained in the plan should be identified and corrected.

8.2.4 Level 4 Test - Run a Critical System at the Backup Site

Extending the prior test to the next step, the pulled files and supplies should actually be used to set up and process a selected critical application system at the backup site. The backup processing capability needed for a complete run should be thoroughly tested at the backup site. A level 4 test should be done twice per year after the Emergency Response Plan is in place.

At the end of this exercise, the following major questions need to be addressed:

1) Did all personnel know where to go and what to do?
2) Is there a contract for the backup site?
3) Were the hours/days required available?
4) Was the computer size and memory capability compatible?
5) Were all the proper files present?
6) Were there adequate scratch tapes?
7) Were the tape drives density, tracks compatible?
8) Were there sufficient tape racks available?
9) Was there a tape storage safe/vault?
10) Was there enough disk space?

11) Were the disk types sufficient, compatible?

12) Were the supplies adequate?

13) Were the proper authorizations obtained from software vendors to move proprietary packages to the backup site?

14) Was there a 24 hour telephone line operating?

15) Was there sufficient work area?

16) Were the phone numbers of the backup site manager and vendor available, correct?

17) Does the backup site provide computer support personnel - operators, computer engineers, analysts, etc.?

18) Did all other hardware and computer peripheral devices function properly?

19) Was the run successful or did it experience problems not usually encountered when the processing is done at the primary computer centers?

20) What were the problems and what procedures should be changed to correct the problem?

8.2.5 Level 5 Test - Simulate a Major Disaster and Activate the Emergency Response Plan

The only way to reasonably ensure that the plan is adequate and proper is to simulate a major disaster; activate the plan; shut down the computer center; evacuate; and move to the backup site. This is usually expensive, but it is a very effective tool for testing the plan. It is also a good technique for engraining security and safety consciousness in all employees. Testing is also a good mechanism to indicate to all employees that the computer security program is fully supported by management. It is recommended that this test be run once a year.

8.3 Summary

One of the most important aspects of successful contingency preplanning management is the continued testing, evaluation, and updating of the contingency plan. Each significant change in the operating environment, whether organization structure, hardware, or operating procedures, must be reviewed for its impact upon the contingency plan.

APPENDIX A

CONTINGENCY PLAN OUTLINE

VOLUME 1 - CONTINGENCY PLANNING AND PREPARATION

1. INTRODUCTION TO VOLUME I
2. DESCRIPTION OF CURRENT EMERGENCY PLANS
3. EMERGENCY RESPONSE PLAN TESTING

VOLUME 2 - EMERGENCY RESPONSE PLAN

1. INTRODUCTION TO VOLUME 2
2. EMERGENCY RESPONSE TASK FORCE
3. EMERGENCY RESPONSE PROCEDURES
4. BACKUP OPERATIONS PROCEDURES

VOLUME 3 - RECOVERY PLAN

1. INTRODUCTION TO VOLUME 3
2. RECOVERY TASK FORCE
3. RECOVERY PROCEDURES

APPENDICES

APPENDIX A - EMERGENCY CALL LIST

APPENDIX B - BACKUP SUPPLIES INVENTORY AND DIRECTIONS TO STORAGE

APPENDIX C - APPLICATION SYSTEMS INVENTORY, PROCESSING TIMELINE, AND DIRECTIONS TO STORAGE FACILITY

APPENDIX D - SYSTEMS SOFTWARE INVENTORY

APPENDIX A

(concluded)

APPENDIX E - MINIMUM HARDWARE CONFIGURATION

APPENDIX F - VENDOR CONTACTS

APPENDIX G - BACKUP SITE FACILITIES

APPENDIX H - BACKUP TEST REPORT CHECKLISTS

APPENDIX I - EMERGENCY OPERATIONS CENTER RESOURCE

APPENDIX J - PREDESIGNATED INITIAL MEETING PLACES

APPENDIX K - SUPPORT SERVICES CHECKLIST

APPENDIX L - UTILITIES CONTACTS

APPENDIX M - DATA ENTRY FORMS AND FORMAT KEYS

APPENDIX N - FACILITY PLANNING REQUIREMENTS FOR RECOVERY OF THE DPI COMPUTER CENTER

APPENDIX O - COMMUNICATIONS REQUIREMENTS FOR RECOVERY OF THE DPI COMPUTER CENTER

APPENDIX P - PERSONNEL REQUIREMENTS

APPENDIX Q - COMMUNICATIONS REQUIREMENTS

APPENDIX B

REFERENCES

1. NASA, "Computer Resources Handbook," NHB 2410.1, Appendix J.

2. OMB Circular A-71, Transmittal Memorandum No. 1, July 27, 1978.

3. National Bureau of Standards, FIPS PUB-87: Guidelines for ADP Contingency Planning, March 27, 1981.

4. Mastbrook, D. W., Guidelines for Selection of Backup Strategies, MTR-82W00204, The MITRE Corporation, November 1982.

5. Garrison, H. G., Jr., and Simpson, G.A., An Overview of ADP Risk Analysis, MTR-79W00445, The MITRE Corporation, November 1979.

6. National Bureau of Standards, FIPS PUB-73: Guidelines for Security of Computer Applications, June 30, 1980.

7. Giragosian, P. A., Mastbrook, D. W. and Tompkins, F. G., Guidelines for Certification of Existing Sensitive Systems, MTR-82W00018, The MITRE Corporation, July 1982.

8. IBM, Contingency Planning for Catastrophic Events in Data Processing Centers, G320-5649-1, March 1979.

9. Marguerite Zientia, "Disaster Recovery: Some Like It Hot, Others Cold," Computerworld, September 1982, p. 10.

10. Kull David, "Disaster Recovery Just in Case...," Computer Decisions, September 1982.

11. National Bureau of Standards, FIPS PUB 65: Guideline for Automatic Data Processing Risk Analysis.

12. NASA, "Assuring Security and Integrity of NASA Data Processing," NMI 2410.7.

MITRE Department
and Project Approval: