# COMPUTER CENTER PHYSICAL SECURITY AND DISASTER RECOVERY

# CONTINGENCY PLANNING AND DISASTER RECOVERY

CONTENTS PAGE



Figures



## 1. GENERAL

**1.01** The guidelines in this section were developed by a multicompany GUARDSMAN project team under the direction of the AT&T Information Systems Technical Support and Standards. This section is issued by AT&T Director—Information Systems Planning and Support to assist the Bell System Companies in implementing a Physical Security and Disaster Recovery Program.

**1.02** Whenever this section is reissued, the reason(s) for reissue will be given in this paragraph.

**1.03** The following terms are used throughout this section. Refer to Section 007-590-301 for definitions:

- Contingency Planning
- Contingency Program
- Disaster Recovery Plan
- Disaster Recovery Manual
- Disaster Recovery Operation
- Processing Environment.

**1.04** The three main objectives of this section are:

- Identify and discuss the items of contingency planning which are essential to an effective contingency program and disaster recovery plan
- Discuss a structured approach to the design of disaster recovery manuals which will lead to a modularized and flexible series of documents that can address the requirements of any size and type of computer facility in the Bell System
- Identify and describe the phases of a disaster recovery operation using the scenario method and discuss some of the physical, logistical, and decision problems which are likely to be encountered.

## 2. EFFECTIVE CONTINGENCY PLANNING

**2.01** This part identifies and discusses the items essential to an effective contingency planning program. Developing the procedures and work efforts which satisfy these requirements will be left up to the organization within each company that is responsible for developing the contingency program and disaster recovery plan. Refer to Section 007-590-300 for discussion of administration responsibilities.

**2.02** There are six items which are essential to an effective contingency planning program. In some cases, these items are work products and will be part of the disaster recovery plan. In other cases, the items are work generators and will be part of the contingency program. Some organizations/installations will identify additional items which they feel must be considered. The six items listed below and discussed in the subsequent paragraphs of this part are the minimum required for a contingency program that can be expected to work.

- Disaster Recovery Management Team
- Off-Site Storage of Critical Data and Supplies
- Predetermined Backup Processing Site(s)
- Information of Items and Checklists
- Documented and Maintained Plan(s) and Manual(s)
- Testing of the Plan(s).

### A. Disaster Recovery Management Team

**2.03** A management group should be organized at each computer site. The purpose of this group would be to provide the management infrastructure necessary to direct a disaster recovery operation. The group should have special training in managing recovery activities. In addition, the group should be given special emergency authority over a wide range of areas important to successful disaster recovery.

**2.04** The disaster recovery management team should consist of the following two internal responsibility levels:

- Primary Disaster Recovery Team
- Secondary Disaster Recovery Team.

**2.05** The primary disaster recovery management team, which is the decision-making body, should be made up primarily of operations personnel. The group should be supervised by the site operations manager, be chosen on the basis of experience and knowledge of the work flow, and consist of no more than ten members. Operational areas of a typical installation that must be represented in this group are:

- Management
- Technical Staff
- Teleprocessing
- User Interface
- Scheduling.

The Site Computer Security Administrator and the Corporate Computer Center Security Administrator, if one exists, must also be members of the primary recovery management team. Refer to Section 007-590-300 for definitions of these functions.

**2.06** The secondary disaster recovery management team consists of numerous individuals who may be needed by the primary team for consultation

or the handling of specific problems. These people would not attend disaster recovery team meetings unless specifically invited by the primary team. Included on the secondary team would be a representative from each of the following areas:

- Corporate Security
- Local Security
- Facilities Engineering
- Building Engineering
- Maintenance Department
- Representative of Each Application
- Public Relations Department
- Medical Department
- Vendors
- Contract Negotiations
- Finance Department
- Legal Department
- Transportation Department
- Personnel Department.

All members of the secondary disaster recovery management team must know what their responsibilities and authorities will be during a recovery operation.

**2.07** Details of the organizational structure and members of the disaster recovery management team must be documented in the disaster recovery manual(s).

**2.08** The disaster recovery management team must have a reliable and documented chain-of-command interface to higher management. This interface would have the following effects.

- The recovery team would have the authority to make and enforce critical decisions.
- The recovery team would have the ability to rally the resources of the company.

**B. Preselected Backup Processing Site(s)**

**2.09** An application system cannot be considered recoverable unless a backup processing facility, which is physically removed from the primary site, can be identified for that system. Essentially, there are four approaches to satisfying the need for backup processing capability.

- Configuring a replacement computer facility
- Off-loading to an existing facility
- Off-loading to a standby facility or "shell"
- Combination of the above.

**2.10** The first approach, configuring a replacement facility, is applicable only when the elements of the processing environment can be shown to be replaceable by vendors, building engineers, etc, within a time frame acceptable to the application/user group(s). The time frame may be days, weeks, or months depending on the complexity of the installation. An example of this approach would be a minicomputer facility with a backup housed in a mobile van.

**2.11** When more than one computer site, having similar processing environments, operates within the same or related management structure—a situation common throughout the Bell System—the option of off-loading to existing facilities is practical. Utilizing this choice requires the following considerations.

- Configurations and operating systems must match the applications.
- Discretionary processing at the backup site(s) must be identified.
- Reciprocal backup arrangements must be made and documented.
- EC (Engineering Change) level of backup facility must be adequate.
- Scheduling must be planned.
- Transportation must be planned.
- Numerous backup sites will probably be required to cover the loss of any one site.

- Required special features must be available, such as special printing configurations, emulators, etc.

**2.12** The flourishing of "on-line" systems with complex interfaces to the communication network introduces a new set of problems to the identification of backup processing capability.

- The network interfaces must be duplicated or quickly replaceable.
- Front end processors must be duplicated or quickly replaceable.
- A CPU must often be dedicated.

**2.13** When the workload of a facility is mostly teleprocessing, it is important to identify an alternate facility for backup processing. However, this approach should be considered whenever the following conditions exist or can be justified.

- Extra space is available in an existing computer facility
- A processor is installed for totally discretionary processing such as a "test machine"
- An unused structure exists which can be quickly equipped to serve as a computer facility, for example, an unused central office.

**2.14** The size and complexity of many of the Bell System computer facilities and their processing environments will often make the use of a single backup processing option insufficient. The final choice is to use a combination of the discussed options. This approach will offer the most recovery time flexibility and may be the most cost-effective.

**2.15** The option chosen to satisfy the need for backup processing capability must be covered by adequate physical security. This is especially important after a disaster when there is a possibility that the disruption was people-caused.

**2.16** Backup processing options must be discussed before a disaster occurs and agreed to by the user, applications staff support, and operations. Requirements and options must be documented. The final choice must be made by the disaster recovery management team during disaster recovery, as dictated by the level of disruption and the criticality of the application to be recovered.

### C. Off-Site Storage

**2.17** Disruption of a processing environment could include damage to data files that are critical to the ongoing operation of an application system. If a system is to be considered recoverable, backup copies of master files, data bases, transaction files, etc, must be rotated to and secured in an off-site storage facility.

**2.18** The commonly used term, "off-site storage," implies a location different from that of the primary storage. Although a distant site is desirable, it is not a necessity. To qualify as off-site storage, the facility must meet the following criteria.

- It must be survivable when the primary facility has been totally destroyed.
- It must be accessible when the primary facility has collapsed.
- It must have security which is independent from that of the primary facility.

**2.19** The following is a summary of the kinds of items which should be considered for storage at an off-site storage facility. Some items are data and others are physical items. All must be adequately secured.

- Backup copies of critical data files, as selected by the applications, which could be used to restart their systems
- Backup copies of the operating system(s)
- Backup copies of application software libraries
- Backup copies of system catalogs
- Copies of data set management system listings
- Run books
- Vendor documentation
- Disaster recovery manual(s)
- Preprinted forms and carriage control tapes

- Unique hardware such as check signers, etc
- Backup copies of critical documentation.

**2.20** Special consideration must be given to the need for physical security at the off-site storage location and in the method of transporation selected. This is critically important whenever there is any possibility that the disruption was caused by a disgruntled employee. An accountability trail must be established.

### D. Information

**2.21** During a disaster recovery operation, the recovery management team will have to make critical decisions about what must process, what can process, and where processing capability is available. These decisions must be made based on accurate, up-to-date information on at least the following topics.

- Application system processing requirements
- Computer system configurations
- Availability of vendor replacement and support
- Teleprocessing networks and interfaces
- Operating system versions and levels
- Resident program products
- Local modifications to operating systems.

**2.22** Much of this information already exists in some form. Some of it can be summarized, such as scheduling data for individual programs. To ensure the availability of information, it must be maintained in the disaster recovery manual.

### E. Documented Disaster Recovery Plan

**2.23** The disaster recovery plan is the preconceived sequence of activities which would result in minimization of the impact of a disastrous disruption to a computer processing environment. The plan is designed to use the recoverability which has been provided for by thoughtful contingency planning and prudent satisfaction of its requirements.

**2.24** The documentation for the disaster recovery plan is the disaster recovery manual. The recovery manual refers to actions to be performed and to documents which support those actions.

**2.25** At computer sites with a limited number of applications, disaster recovery manuals will be of a size manageable with standard word processing techniques. Sites with multiple computer facilities and many applications will find effective disaster recovery manuals to be a sizable collection of material. The use of a data processing subsystem with text-editing features is suggested. Consideration should also be given to the development of a recovery scheduling subsystem which could match jobs to processing capability and produce emergency processing schedules.

**2.26** A detailed discussion of a hierarchical approach to the problem of producing and maintaining a reliable disaster recovery plan and its documentation is contained in Part 3.

### F. Testing of the Disaster Recovery Plan

**2.27** Disaster recovery plans must be tested for the following reasons:

- Testing will ensure compliance with the impositions of the contingency program.
- The disaster recovery management team will learn to use portions of the recovery plan to contend with limited disruptions.
- The procedures and actions of a disaster recovery operation can be practiced.
- Errors and shortcomings of the contingency program and the recovery plans can be exposed.
- Successful testing will instill confidence in the viability of the plans.
- The EDP auditors will be satisfied.
- Testing will ensure that the processing environment needed to support critical applications can be restored in less time than the maximum allowed outage.

**2.28** It is undesirable and unnecessary to test all of a recovery plan at one time. Such an

action could itself be disastrous. Recovery plan testing can be accomplised in the following ways:

- Informational items can be periodically reviewed for accuracy and timeliness.
- A limited disaster can be "declared" and talked through.
- Unannounced drills can be conducted.

## 3. DISASTER RECOVERY MANUALS

### A. Structuring Disaster Recovery Plans

**3.01** The organizational structure of a reliable disaster recovery plan suggests that a hierarchically interlocking system of recovery manuals be developed. This produces two positive effects.

(a) Modularity is introduced into what can become a very complex document.

(b) Redundancy is avoided by isolating common areas of recovery documentation.

**3.02** The number of hierarchical level recovery plans can vary depending on the complexity of the installation(s) involved.

**3.03** The simplest recovery plan is for the installation having one computer with one application. A single manual containing the recovery plans for the application and the site is sufficient.

**3.04** The disaster recovery plan is complicated when multiple applications are processed within the same site. Each application must have its own recovery manual. These manuals all connect organizationally to the site manual, which is one level above in the plan structure. The site recovery manual supports the recovery plans for the computer facility or site.

**3.05** Complexity increases again when multiple sites are involved in the overall recovery plan. This is desirable because mutual backup processing arrangements can be made and documented. An executive recovery manual which supports the areas of the recovery plan common to all sites is necessary.

**3.06** Figure 1 illustrates the relationship among the levels of a hierarchically organized disaster recovery plan. According to the scope of the plan and the installation(s) involved, manuals may be physically combined or further subdivided as appropriate without the overall plan structure being violated.

**3.07** The following concepts of hierarchically organized recovery plans must be understood:

(a) The recovery manual contents of the plan at levels above and below are available at any plan level; eg, in a multiple site organization, individually prepared site manuals would each contain a copy of the common executive recovery manual and all application manuals for applications within the site.

(b) In a simple recovery plan structure where modularity and redundancy are irrelevant, a single recovery manual is sufficient. However, the information and procedures that would have been divided into the various manuals of a complex plan must still be present.

**3.08** The remainder of this part discusses the layout and contents of the manuals constituting a hierarchically organized disaster recovery plan. For simplicity, the plan is limited to three levels: the executive, the site, and the application. The layout of the manuals is similar and can be divided into three topics:

- General Information, Overview, Objectives, and Scope
- Activities Supported
- Information Items and Checklists.

### B. Application Recovery Manual

**3.09** ***Objectives and Scope:*** The application recovery manual is the supporting document for the recovery plans which are pertinent to the application subsystem and its user function. A joint statement must be made by the application staff support group and the user as to what they expect to achieve with the plan in place. The limits of the application recovery plan must be stated in the manual.

## RECOVERY MANUALS – AN OVERVIEW

### HIERARCHICALLY ORGANIZED DISASTER RECOVERY PLAN

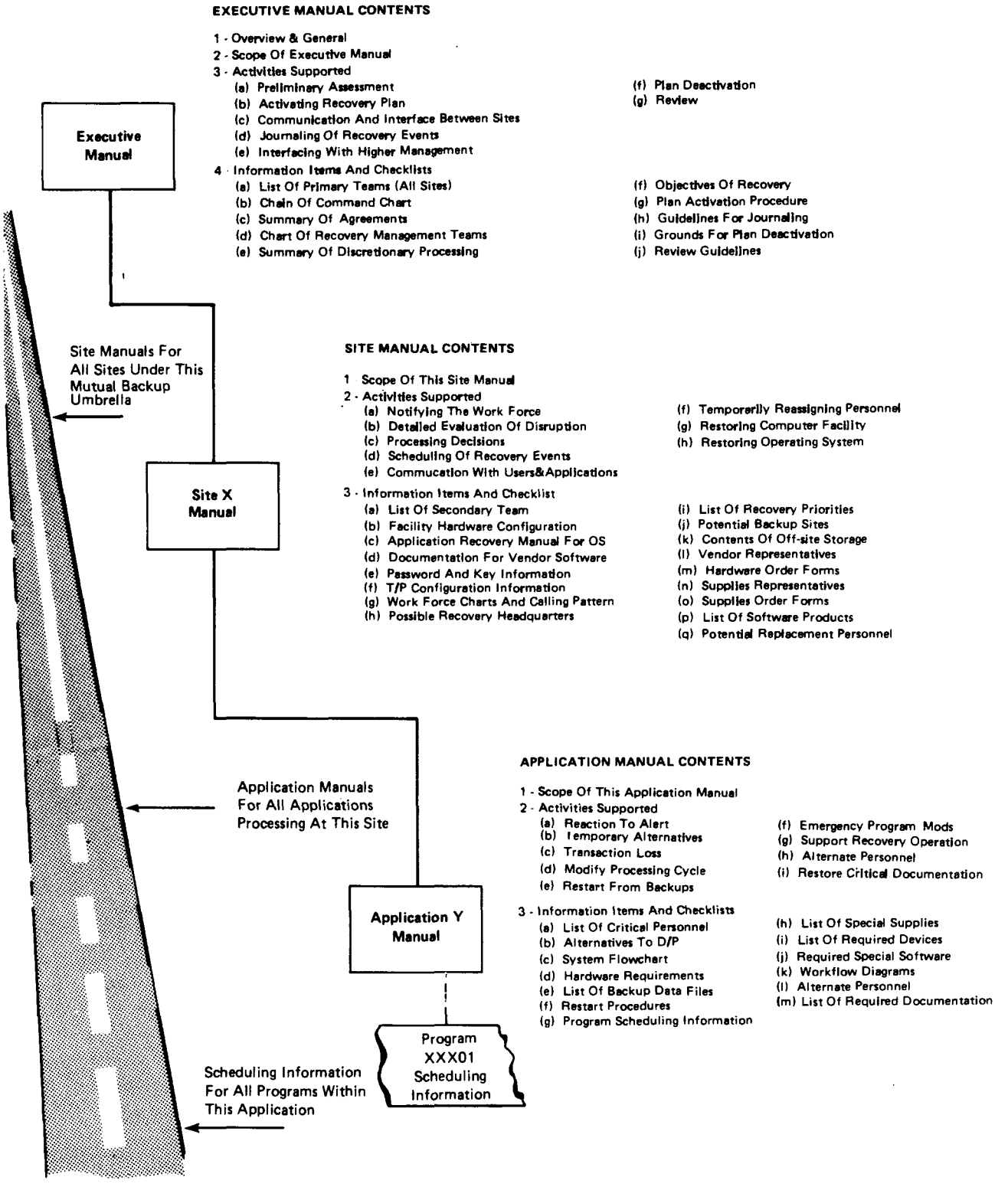



**Fig. 1—Recovery Manuals—An Overview: Hierachically Organized Disaster Recovery Plan**

### 3.10 *Activities Supported:*

(a) ***Reacting to Recovery Plan Activation:*** In cases where an application software system is maintained by a staff group, that group must be prepared to react along with the user to the special conditions of a disaster recovery operation. A manager should be chosen within each application who will be able to interface on behalf of the application with the site disaster recovery management team. This person should be authorized to make decisions and direct any recovery operations which are within the scope of the application.

(b) ***Considering Temporary Alternatives:*** An application staff/user group must consider the possibility that the normal computer facility may not be available. This group must identify, wherever possible, manual or other mechanical alternatives that will allow the user to survive the outage. These alternatives must be documented within the application recovery manual.

(c) ***Accounting for Loss of Transactions:*** During a disaster-caused processing disruption, batch master file update systems and transaction-driven data base systems could experience an interruption in the ability to process transactions. Plans should be made and documented in the recovery manual to temporarily store transactions and post them later, or to cease accepting them until processing can resume. Also to be considered is the possibility that some transactions could be permanently lost. An application management group must decide and document how much transaction loss their system can tolerate.

(d) ***Processing Cycle Modification:*** During a disaster recovery operation, available computer time to process a batch software system may be a small percentage of the time normally required. The user and the application programming staff should identify and agree on individual jobs and streams within the application system which can be delayed or bypassed during an emergency. Care must be taken during this process to avoid bypassing control streams which could leave an application system vulnerable to fraud or error. When discretionary processing can be found, it must be documented in the recovery manual for the application.

(e) ***Restarting an Application Software System:*** If the level of processing disruption is severe enough to destroy data files, then some application systems must be restarted from backups. Copies of critical data sets, such as master files, should have been safely stored at the off-site storage location. Since the backup master file is usually the grandfather of the current file, the entire software system must be cycled twice using copies of recent transactions if copies exist. This is necessary to make the master file current so new transactions can be entered. Similar problems exist when restarting transaction-driven data base systems. Restart procedures can be confusing and are always time-consuming. They must be preplanned and documented in the application recovery manual.

(f) ***Emergency Program Modification:*** The need for program modification will inevitably occur during the stress of recovery processing. Programs should be reviewed with the intent of locating routines where code changes might be necessary. The emergency code should be outlined and filed in the recovery manual. Paper and/or fiche copies of source code must be retained in a location separate from the primary magnetic library area; this process must be documented.

(g) ***Supporting Recovery at Backup Processing Locations:*** Recovery processing for an application software system could be scheduled at a distant backup processing site. On-site programming support may be needed. Transportation alternatives should be examined for application support people, specialized equipment, and supplies. Lodging and finance problems should be considered and planned for. Alternatives and procedures should be documented in the application recovery manual.

(h) ***Providing Alternate Personnel:*** A disaster at a computer facility could result in a shortage of trained personnel. Each application must consider the possible need to be able to identify alternate personnel to fill staff and clerical positions critical to the functioning of the application.

(i) ***Restoring Critical Documentation:*** A disaster at a computer facility could destroy documentation critical to the functioning of an application subsystem. This documentation might

include implementation guides, operations guides, technical staff handbooks, etc. Documentation that is pertinent and critical to an application system must be backed up off-site and recoverable. Details of recovery must be included in the application recovery manual.

**3.11** ***Information Items and Checklists:***

(a) Name and number of all user/staff personnel and alternates who use or maintain critical components of the application system.

(b) Outline of user alternatives to data processing services.

(c) Application system flowchart with discretionary processing identified.

(d) Application system hardware requirements by work volume.

(e) Checklist of application system restart (backup) data files, with retention periods and rotation cycles, and its off-site storage locations. Backups should be taken by data file name, not by device or media.

(f) Detailed list of procedures for restarting the application system using recovery (backup) data sets with provisions for handling disrupted transaction flow.

(g) Scheduling information for all programs constituting the application system. Requirements for this item may be satisfied by ensuring access to run books or inclusion of a summarization of the run book for each program.

(h) Checklist of required special supplies.

(i) Checklist of required out-of-ordinary devices.

(j) Checklist of required vendor-supplied software.

(k) Work flow diagrams showing manual interaction to the system.

(l) List of possible alternate personnel, selected from user groups, etc.

(m) Checklists of recoverable documentation which is critical to proper functioning of application system including details of recovery.

**C. Site Recovery Manual**

**3.12** ***Overview:*** The site recovery manual should address the potential recovery problems of the computer facility itself, its operating system, and the people who run it. A statement as to the scope of the site recovery plan should define the physical and managerial bounds of this aspect of the plan. The relationship of the site recovery plan to the overall disaster recovery plan should be stated as well as the specific objectives of the site recovery manual. Each site recovery manual must provide support and reference to disaster investigations by security.

**3.13** ***Activities Supported:***

(a) ***Notifying the Work Force:*** A disaster at a computer facility, depending on the size and type of the installation, could require that a large number of people be individually located, notified, and given instructions. The work force for the next scheduled shift may have to be told not to report. The members of the shift present during the event must be accounted for. Programmers or other support personnel may have been on-site out of normal hours and must be accounted for. A work force calling and notification system must be developed. A last-resort scheme utilizing public broadcasting should be outlined. All such situations must be documented in the site recovery manual.

(b) ***Evaluating the Processing Disruption in Detail:*** The primary members of the disaster recovery management team must examine the physical condition of the computer facility and determine what the level of disruption will be to the processing of their application(s). Factual information concerning the hardware and configuration of the computer(s) and the needs of the applications must be part of the site recovery manual.

(c) ***Deciding What Must Run, What Can Run—Where and When?*** The disaster recovery management team will be responsible for making critical decisions regarding what applications will be processed at backup sites and/or in a facility of reduced capacity. To make these decisions, the team will need to know what the priorities are in the view of higher management. The application priority list must be documented in the site recovery manual.

(d) ***Scheduling Recovery Events:*** The disaster recovery management team must develop a schedule of recovery events. The schedule will be based on the processing decisions they will have made. The schedule must satisfy logistics problems of time and distance between backup sites, off-site storage, supplies, people, etc, and evolve into a processing schedule to be used at the backup processing site(s). Scheduling will require a list of preselected potential backup processing sites, their configurations, performance, and level of discretionary processing.

(e) ***Communication with Users/Applications:*** The site recovery manual must dictate the rules and define the channels for communication between the disaster recovery management team and the application groups. A representative from each application should be assigned to the recovery team as a secondary member (see paragraph 2.06). This secondary member should be on call and prepared to offer consulting assistance and to receive instructions from the primary team. The channel of communication must be documented in the site recovery manual.

(f) ***Temporary Reassigning Personnel:*** A disaster could result in the need for replacement of personnel in areas such as clerical support, machine operators, programming, systems analysis, and supervision. The disaster recovery management team must have the authority to temporarily reassign people to any location which may require help during a recovery operation. The guidelines for establishing the authority of the recovery team in this area must be documented in the site recovery manual.

(g) ***Restoring the Data Center:*** The disaster recovery team must give high priority to restoration of the processing capability of the stricken computer facility. Obviously, there will be times when this is impossible. However, impact to the applications will always be less if the facility does not have to physically move to a backup location. The disaster recovery management team should appoint a group from secondary members of their team to work full time on the restoration. Supporting documents should be part of the site recovery manual.

(h) ***Restoring the Operating System:*** Fewer problems will be encountered recovering application software systems if they can be restarted on the same or a similar operating system to that which they normally run. This implies that the operating system be recoverable and/or transportable. To ensure that the operating system is recoverable, it must be treated like any application system that uses the hardware and an application recovery plan and manual must be developed for it. This is also the case for software subsystems such as IMS, CICS, etc. In addition to making the operating system recoverable, consideration should be given to making the software "transportable" (capable of being easily installed on another computer). These topics must be covered in application recovery manuals which are required subsets of the site recovery manual.

### 3.14 *Information Items and Checklists:*

(a) Name and number of all secondary disaster recovery management team members and alternates for this site.

(b) Detailed hardware configuration charts with engineering change level and other data pertinent to machine configuration.

(c) Application recovery manual(s) addressing the recoverability requirements of the operating system and major subsystems such as IMS, CICS, etc.

(d) Detailed documentation for vendor supplied software enhancements and packages.

(e) Passwords and keys, or at least how to obtain them, for security files.

(f) Teleprocessing interface configuration including pertinent information concerning the associated network. Precompleted service orders for replacement circuits are recommended.

(g) Work force charts with an identified calling pattern for work groups having access to the installation.

(h) List of predetermined potential disaster recovery headquarters locations.

(i) Predetermined and agreed-to-list of application recovery priorities. (See Section 007-590-302, Impact Analysis.)

(j) List of predetermined potential backup processing sites for all applications subject to recovery.

(k) List of contents of off-site storage locations.

(l) Name and number of hardware vendor representatives.

(m) Precompleted hardware order forms.

(n) Name and number of supplies' vendor representatives.

(o) Precompleted supplies (paper, printer ribbons, etc) order forms.

(p) List of leased software products which will need modification to run on a different CPU.

(q) List of potential replacement personnel in various areas of expertise in operations positions.

(r) Detailed procedures for operating system restoration and/or generation.

(s) Security personnel contact list for disaster investigation.

**D. Executive Recovery Manual**

**3.15** ***Overview:*** When multiple computer sites having similar processing environments exist within the same management structure, the problem of potential backup sites can be addressed by organizing the sites into a mutual backup umbrella. With this approach, the executive disaster recovery manual provides documentation for those elements of recovery that pertain to all sites. A statement should be made in the executive manual defining the scope of the overall disaster recovery plan. All participating sites should be noted as well as the managers, by title, who committed the sites to the plan. A general statement should be included which summarizes the recovery plan, explains the concept of hierarchical plan structure and modularized recovery manuals, and states who (organizationally) is responsible for what.

**3.16** ***Activities Supported:***

(a) ***Preliminary Assessment of Processing Disruption:*** The executive manual must contain the guidelines for determining when the disaster recovery plan should be activated. These guidelines should be designed so that the site disaster recovery coordinator can use them to make a correct analysis, over the phone if necessary, of the situation. Likewise, the highest level manager responsible for operation of the site should be able to use the guidelines as the basis for deciding whether or not to activate the disaster recovery plan.

(b) ***Activating the Disaster Recovery Plan:*** The executive recovery manual must include a list of procedures to be followed by the Site Computer Security Administrator or the Corporate Computer Security Administrator, if one exists, when activating the plan. Procedures listed in the site plan must include: notification of primary recovery team members, scheduling the first meeting of the team, reporting to higher management, and the beginning of journaling of recovery events.

(c) ***Communication and Interfaces Between Sites:*** When a computer installation that is part of a preplanned mutual backup umbrella enters a disaster recovery operation, a high degree of management communication and cooperation between the stricken site and its backups must be initiated and maintained. Guidelines must be developed and documented in the executive recovery manual defining the interfaces and levels of authority between sites so that expectations are spelled out and misunderstandings avoided.

(d) ***Journaling of Recovery Activities and Events:*** A journal of all recovery activities and events must be kept. A history will be useful during the recovery operation because high-stress conditions will tax memories and make sequencing of events difficult. The journal will be useful during a disaster recovery operation postmortem when areas of plan improvement can be identified. The document will also be used by other Bell System companies who wish to improve their recovery plans. Guidelines for the journal must be documented in the executive recovery manual.

(e) ***Interfacing with Higher Management:*** During a disaster recovery operation, the recovery management team will often require the help of higher management in areas such

as streamlining the interactions between departments, approving the spending of money, handling labor problems, etc. Conversely, higher management may need to direct certain areas of the recovery operation. In either case, a special interface through chain of command must be authorized and documented in the executive recovery manual.

(f) ***Deactivation of Disaster Recovery Plan:*** A disaster recovery operation will place considerable strain on sites and departments not otherwise affected by the initial event. These groups may apply pressure to "return to normal" prematurely. The executive disaster recovery manual should provide guidelines with which the recovery team can know when to deactivate the operation.

(g) ***Review the Effects of the Recovery:*** Objectives and standards should be developed and documented that measure the performance of a recovery operation. These measurements may be applied during the recovery operation to help locate areas of improvement. These measurements must also be applied during the postmortem phase.

**3.17** ***Information Items and Checklists:***

(a) Name and phone number of primary disaster recovery management team members and alternates at all sites within a mutual backup umbrella

(b) Chain-of-command call list to be used for interfacing with higher management

(c) Summary of backup processing agreements between sites participating in a mutual backup scheme

(d) Summary of discretionary processing time available at all sites within a mutual backup umbrella

(e) Organizational chart of corporate disaster recovery organization

(f) Documented objectives and standards for measuring the performance of a recovery operation

(g) List of procedures for activating the disaster recovery plan

(h) List of guidelines for creating a journal of recovery events and possibly some prepared forms

(i) List of grounds for and procedures for deactivating the disaster recovery plan

(j) List of objectives and guidelines for performing a postmortem of the recovery operation after the plan has been deactivated

(k) Disaster investigation procedures.

## 4. MODELING DISASTER RECOVERY OPERATIONS

**4.01** This part focuses on the sequence of events composing a disaster recovery operation, as it might be expected to occur at a multiapplication computer facility. The scenario approach to disaster recovery planning is used. Scenarios, as a methodology for recovery planning, are important because they lead to a detailed analysis of the requirements of individual recovery activities and expose inadequacies.

**4.02** The scenario discussed here is hypothetical and the discussion will be abstract. The multiapplication facility is used in this example because it is most typical. The scenario technique can work equally well for any size and type of computer facility.

**4.03** The sequence of events of the disaster recovery operation is illustrated in Figures 2 through 5. These figures are intended to be used as a model for developing scenarios of potential recovery operations at actual computer facilities.

**4.04** The disaster recovery operation is divided into four phases. Each phase is distinct from the others in that it consists of a "reasonably" predictable series of events that can be expected to occur as the result of some triggering event or decision. For example, the first phase of the recovery operation is triggered by the disastrous event itself, and the second phase is triggered by a major decision executed during the first phase.

**4.05** ***Phase 1:***

(a) Refer to Fig. 2. Phase 1 of a disaster recovery operation is initiated by the disaster. Some event occurs at the computer facility which impacts the processing environment. The event

may be highly disruptive or the level of disruption might only be suspected.

(b) In any case, someone at the site, who is physically able, notifies the site disaster recovery coordinator through normal supervisory channels. It is the responsibility of the site disaster recovery coordinator or the designated alternate to make a preliminary assessment of the situation according to preconceived guidelines which are documented in the Executive Disaster Recovery Manual. The site disaster recovery coordinator then reports to the highest data processing manager within the orgaization.

(c) Using the findings and recommendations of the recovery coordinator and the guidelines specified in the Executive Disaster Recovery Manual, the highest data processing manager or designated alternate then makes the decision to activate the disaster recovery plan. The decision to activate the disaster recovery plan concludes Phase 1. At this time, security should be notified to ensure investigation of the declared disaster. It should be possible to accomplish the activities of this phase within a few hours of the disruptive event.

4.06 ***Phase 2:***

(a) Once the disaster recovery plan has been activated, the site disaster recovery coordinator notifies all members of the primary disaster recovery management team. The list of their names and phone numbers and those of their designated alternates is contained in the Executive Disaster Recovery Manual. A location for the first meeting of the primary team is chosen from preselected options, and the initial meeting is held.

(b) The first priority of the disaster recovery management team is to locate all personnel within the organization or vendors who could have been at the site. Preliminary instruction should be given to personnel as they are located. This time-consuming activity must follow a predetermined plan (eg, organizational work force charts, calling tree, or other). The task should be performed by clerical personnel assigned to the recovery team.

(c) The next priority of the primary recovery management team is to survey the physical damage to the elements of the processing environment. This may be difficult due to building damage; however, with the aid of local fire officials, corporate securities, etc, along with the asset analysis developed as outlined in Section 007-590-302, a damage report by component can be assembled and a preliminary disruption analysis can be made.

(d) At this stage, the primary recovery management team should have a good picture of how serious the processing disruption is. The team should relay the results of their preliminary analysis to higher management so that emergency interdepartmental interfaces can be established.

(e) A preliminary disaster recovery "ALERT" is declared. The purpose of the alert is to give all expected participants in the recovery operation time to prepare to receive instructions and begin recovery. Included in the preliminary alert are potential backup processing sites, the off-site storage facility, vendors, critical application representatives, etc.

(f) Using the information contained in the site recovery manual and the application recovery manual(s), the primary disaster recovery management team must perform a detailed processing disruption analysis. They must determine:

- Their processing capability
- What is needed to meet the minimum needs of the company
- How much difference they will have to make up at the backup processing locations.

Participating in this analysis will be designated members of the secondary recovery team as requested by the primary team.

(g) After the detailed disruption analysis is complete, the primary disaster recovery management team must make a group of decisions that are vitally important to a successful recovery operation. They must decide:

- What applications can be processed within existing capabilities including backup facilities
- What applications will process

- Where applications will process.

These critical decisions must be made based on the emergency processing priority list produced during application analysis as per Section 007-590-302. The decisions must also be based on the application scheduling information contained in the application recovery manuals. Those applications which have failed to provide the necessary information will not be considered for emergency processing.

(h) From these critical decisions come the instructions which direct all aspects of the recovery operation. This decision block is the final activity of Phase 2 of the recovery operation.

**4.07** ***Phase 3:***

(a) The third phase of the recovery operation deals with the activities of separate work groups, who are directed by the primary disaster recovery management team. Each group is assigned a specific area of responsibility. Some are organized on short notice; others exist as part of normal operations but work under a modified chain of command during the emergency.

(b) Individual groups and their sequence of activities are represented in this scenario as different legs of the operation that have a common origin and a common destination. The common origin is the point where instructions are issued from the primary recovery team. The common destination is the achievement of successful emergency processing cycles.

(c) Only three legs of Phase 3 activities are defined in this example. Included are the activities of the application/user group(s), the backup processing site(s), and the off-site storage facility. In a scenario developed for an actual installation, numerous other activities will probably be defined by each individual installation. Therefore, each installation affected should refer to Fig. 4 for suggestions as to what kinds of activities to define in Phase 3 of a disaster recovery scenario.

**4.08** ***Phase 4:***

(a) A disaster recovery operation can be said to have reached its fourth phase when successful emergency processing cycles are being achieved. This condition will be defined differently for the various applications and installations. For the batch subsystem, it would mean that the master file is current and all critical stream programs have been integrated into a working processing schedule. For the on-line transaction processing system, it would mean that response time is acceptable and data bases are up to date. For the network monitoring facility, it would mean that the adequate data is being collected and translated to maintain the integrity of the communications network.

(b) The achievement of successful processing cycles carries with it a sense of stability to the recovering processing environment. This is the time when the recovery management team should initiate the long-term rebuilding program. The long-term program, although initiated by the primary team, should be conducted by another group made up of appropriate members of the secondary recovery team. This effort will be long and complex and must not interfere with the foremost responsibility of the primary recovery team which is successful emergency processing.

(c) The primary team should define points in the emergency processing cycle when it is appropriate to evaluate the current status. This may be after each shift or may be on a daily basis or even longer, providing it is done regularly. The evaluations may produce a decision to modify the emergency processing environment, the schedule, priorities, or even to deactivate all or part of the recovery operation.

**4.09** ***Phase 5:***

(a) Recovery can be said to have been achieved when normal day-to-day operations have been restored. Two positive signs of recovery are:

- All groups who were reassigned to temporary work locations have been allowed to return to their normal locations.

- Discretionary processing (testing and other development work) is returning to predisruption levels.

(b) Once recovery has been achieved, a postmortem of the disaster and the recovery operation must be conducted. The effectiveness of the recovery plan(s) must be determined and the areas of improvement identified.

## DISASTER RECOVERY OPERATION – MODEL SCENARIO

### PHASE 1

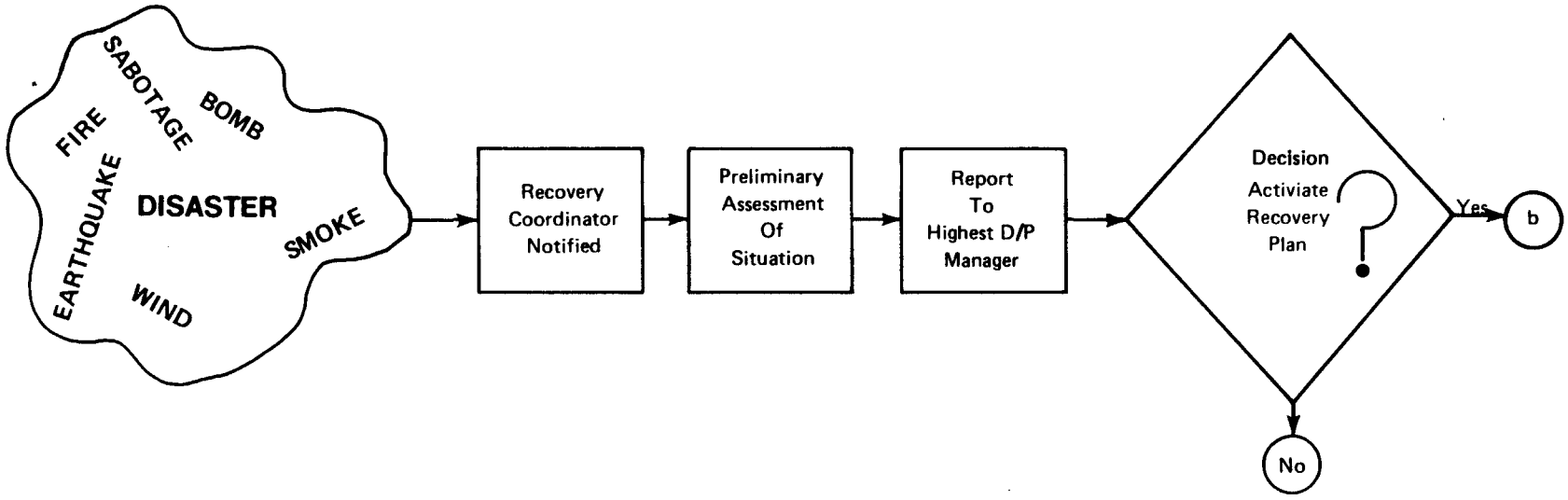



Fig. 2—Disaster Recovery Operation—Model Scenario—Phase 1

## DISASTER RECOVERY OPERATION – MODEL SCENARIO

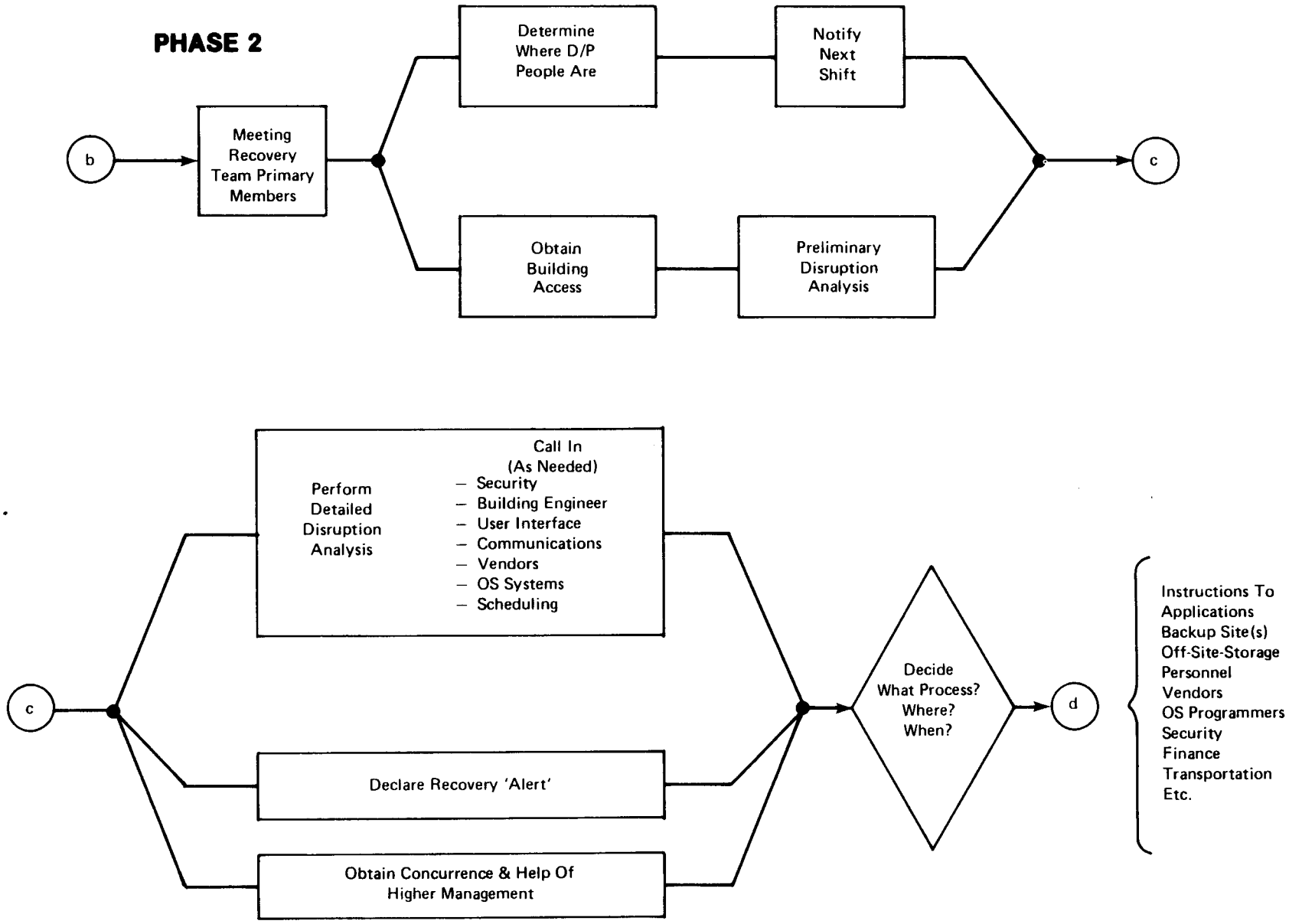



**Fig. 3—Disaster Recovery Operation—Model Scenario—Phase 2**

DISASTER RECOVERY OPERATION – MODEL SCENARIO

## PHASE 3

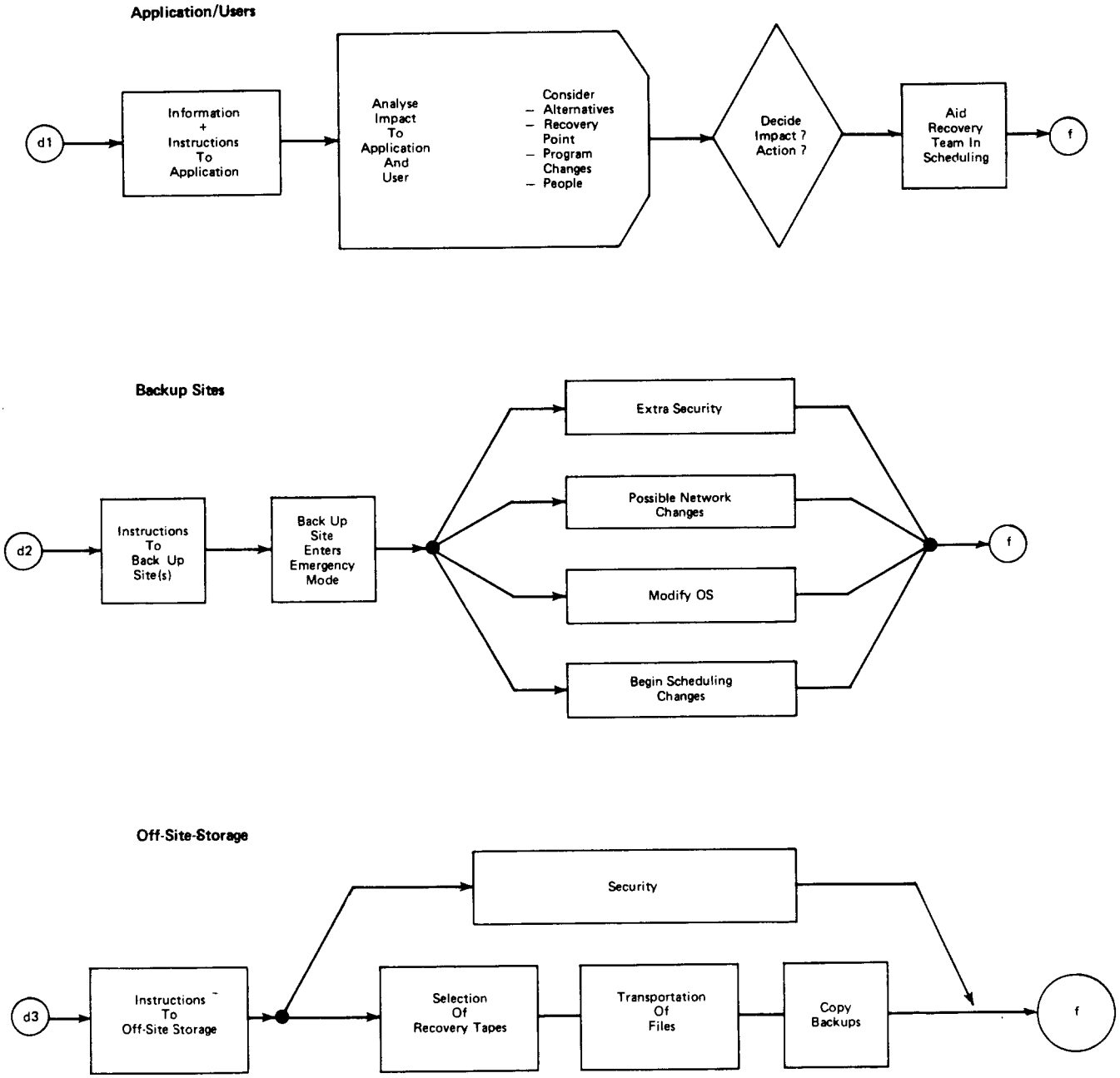
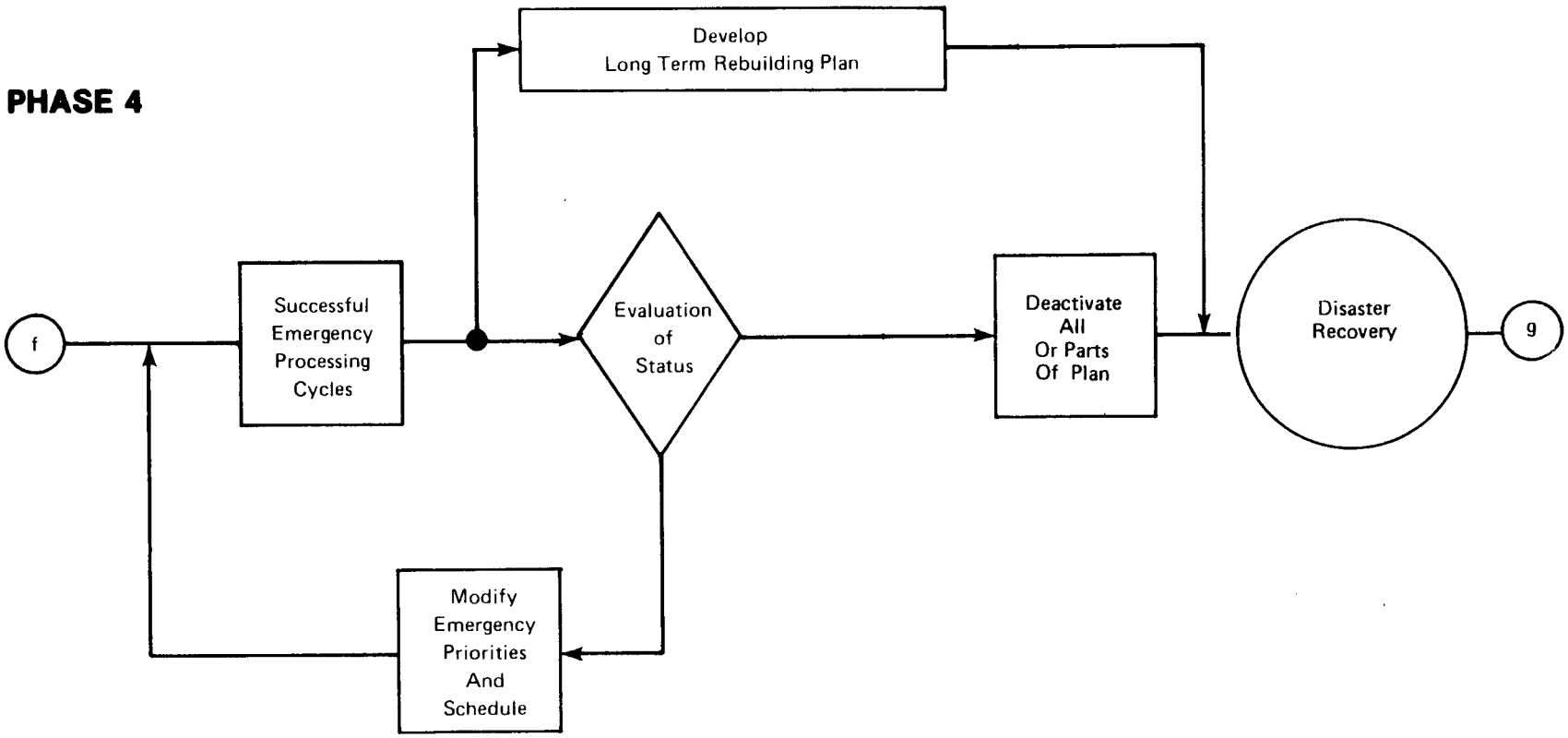



**Fig. 4—Disaster Recovery Operation—Model Scenario—Phase 3**

## DISASTER RECOVERY OPERATION – MODEL SCENARIO



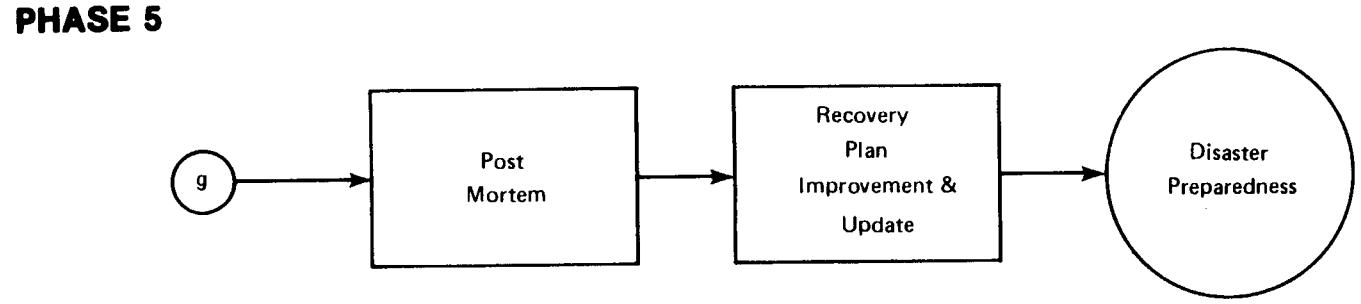




**Fig. 5—Disaster Recovery Operation—Model Scenario—Phase 4**