U.S. Department
of Commerce

National Bureau
of Standards

Computer Science and Technology

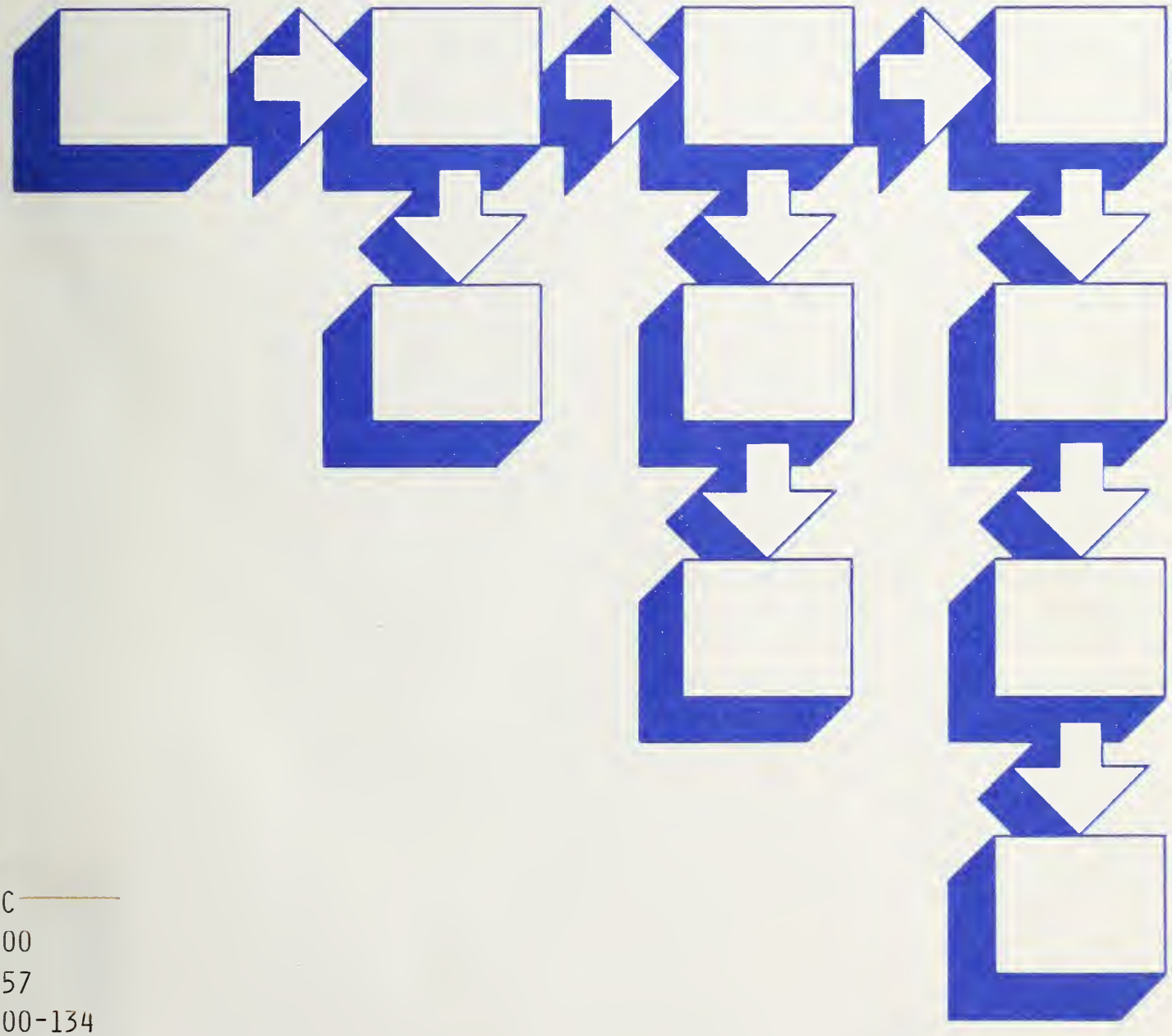
NBS
PUBLICATIONS

NAT'L INST. OF STAND & TECH
A11106 978057

NBS Special Publication 500-134

Guide on Selecting ADP Backup Processing Alternatives

Irene E. Isaac



QC
100
.U57
500-134
1985
c. 2

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

The National Bureau of Standards[1] was established by an act of Congress on March 3, 1901. The Bureau's overall goal is to strengthen and advance the nation's science and technology and facilitate their effective application for public benefit. To this end, the Bureau conducts research and provides: (1) a basis for the nation's physical measurement system, (2) scientific and technological services for industry and government, (3) a technical basis for equity in trade, and (4) technical services to promote public safety. The Bureau's technical work is performed by the National Measurement Laboratory, the National Engineering Laboratory, the Institute for Computer Sciences and Technology, and the Institute for Materials Science and Engineering.

The National Measurement Laboratory

Provides the national system of physical and chemical measurement; coordinates the system with measurement systems of other nations and furnishes essential services leading to accurate and uniform physical and chemical measurement throughout the Nation's scientific community, industry, and commerce; provides advisory and research services to other Government agencies; conducts physical and chemical research; develops, produces, and distributes Standard Reference Materials; and provides calibration services. The Laboratory consists of the following centers:

- Basic Standards[2]
- Radiation Research
- Chemical Physics
- Analytical Chemistry

The National Engineering Laboratory

Provides technology and technical services to the public and private sectors to address national needs and to solve national problems; conducts research in engineering and applied science in support of these efforts; builds and maintains competence in the necessary disciplines required to carry out this research and technical service; develops engineering data and measurement capabilities; provides engineering measurement traceability services; develops test methods and proposes engineering standards and code changes; develops and proposes new engineering practices; and develops and improves mechanisms to transfer results of its research to the ultimate user. The Laboratory consists of the following centers:

- Applied Mathematics
- Electronics and Electrical Engineering[2]
- Manufacturing Engineering
- Building Technology
- Fire Research
- Chemical Engineering[2]

The Institute for Computer Sciences and Technology

Conducts research and provides scientific and technical services to aid Federal agencies in the selection, acquisition, application, and use of computer technology to improve effectiveness and economy in Government operations in accordance with Public Law 89-306 (40 U.S.C. 759), relevant Executive Orders, and other directives; carries out this mission by managing the Federal Information Processing Standards Program, developing Federal ADP standards guidelines, and managing Federal participation in ADP voluntary standardization activities; provides scientific and technological advisory services and assistance to Federal agencies; and provides the technical foundation for computer-related policies of the Federal Government. The Institute consists of the following centers:

- Programming Science and Technology
- Computer Systems Engineering

The Institute for Materials Science and Engineering

Conducts research and provides measurements, data, standards, reference materials, quantitative understanding and other technical information fundamental to the processing, structure, properties and performance of materials; addresses the scientific basis for new advanced materials technologies; plans research around cross-country scientific themes such as nondestructive evaluation and phase diagram development; oversees Bureau-wide technical programs in nuclear reactor radiation research and nondestructive evaluation; and broadly disseminates generic technical information resulting from its programs. The Institute consists of the following Divisions:

- Ceramics
- Fracture and Deformation [3]
- Polymers
- Metallurgy
- Reactor Radiation

[1]Headquarters and Laboratories at Gaithersburg, MD, unless otherwise noted; mailing address Gaithersburg, MD 20899.
[2]Some divisions within the center are located at Boulder, CO 80303.
[3]Located at Boulder, CO, with some elements at Gaithersburg, MD.

NBS
RESEARCH INFORMATION
CENTER

Computer Science and Technology

NBS Special Publication 500-134

Guide on Selecting ADP Backup Processing Alternatives

Irene E. Isaac

Center for Programming Science and Technology
Institute for Computer Sciences and Technology
National Bureau of Standards
Gaithersburg, MD 20899

Issued November 1985

U.S. DEPARTMENT OF COMMERCE
Malcolm Baldrige, Secretary

National Bureau of Standards
Ernest Ambler, Director

Reports on Computer Science and Technology

The National Bureau of Standards has a special responsibility within the Federal Government for computer science and technology activities. The programs of the NBS Institute for Computer Sciences and Technology are designed to provide ADP standards, guidelines, and technical advisory services to improve the effectiveness of computer utilization in the Federal sector, and to perform appropriate research and development efforts as foundation for such activities and programs. This publication series will report these NBS efforts to the Federal computer community as well as to interested specialists in the academic and private sectors. Those wishing to receive notices of publications in this series should complete and return the form at the end of this publication.

Library of Congress Catalog Card Number: 85-600618
National Bureau of Standards Special Publication 500-134
Natl. Bur. Stand. (U.S.), Spec. Publ. 500-134, 41 pages (Nov. 1985)
CODEN: XNBSAV

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1985

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402

TABLE OF CONTENTS

Page

1. INTRODUCTION.....1-1

2. MANAGEMENT RESPONSIBILITY.....2-1

2.1 Establish a Project Plan and Project Team.....2-1

2.2 Conduct Risk Analysis.....2-2

2.3 Identify Critical Applications.....2-3

2.4 Rank Critical Applications.....2-4

2.5 Develop an Off-Site Storage Program.....2-4

2.6 Certification of the Alternate Processing Strategy.....2-4

3. REQUIREMENTS DEFINITION.....3-1

3.1 Availability and Reliability of the Alternate Facility..3-1

3.2 Compatibility of Hardware and Software.....3-2

3.3 Physical Capacity of the Alternate Facility.....3-2

3.4 Environmental Support.....3-3

3.5 Telecommunications Support.....3-3

3.6 Location of the Alternate Facility.....3-3

3.7 Sufficiency of Test Periods.....3-4

3.8 Security Capabilities.....3-5

3.9 Cost Effectiveness.....3-5

3.10 Completeness of Contracts and Agreements.....3-6

3.11 Quality of Assistance Provided.....3-6

4. DESCRIPTION OF THE ALTERNATIVES.....4-1

4.1 Service Bureaus 4-1

4.2 Time Brokers.....4-2
4.3 Dedicated Contingency Centers (Hot Sites).....4-2
4.4 Membership in Shared Contingency Facilities.....4-4
4.5 Empty Shells (Cold Sites).....4-5
4.6 Reciprocal Agreements (Mutual Aid Agreements).....4-7
4.7 Separate Locations Under the Same Management.....4-8
4.8 Fortress Concept with Full Redundancy.....4-9
4.9 Reversion to Manual Processing.....4-9
4.10 Use of Microcomputers.....4-10
4.11 Other Possibilities 4-10
4.12 Insurance.....4-11

APPENDIX A - BACKUP PROCESSING SELECTION CHECKLIST.....A-1

APPENDIX B - REFERENCES AND ADDITIONAL READINGS.....B-1

FIGURES

Figure 1.....1-2

Figure 2.....3-8

Figure 3.....4-12

Figure 4.....A-4

ACKNOWLEDGEMENTS

The author would like to express her thanks to the many Disaster Recovery Centers that allowed a review of their facilities and those who provided information for inclusion in this document. Thanks go to Mr. Dennis Steinauer, Mr. Eugene Troy, Ms. Zella Ruthberg, Dr. Stuart Katzke, Ms. Wilma Osborne, and Ms. Elizabeth Parker of the National Bureau of Standards for their constructive review of this document.

Abstract

This publication addresses the issue of selecting ADP backup processing support in advance of events that cause the loss of data processing capability. The document emphasizes the need for managers at all levels of the organization to support the planning, funding, and testing of an alternate processing strategy. It provides a general description of the alternatives, and recommends criteria for selecting the most suitable alternate processing method.

Key words: Backup operations; contingency planning; disaster recovery.

1. INTRODUCTION

This document provides managers and others responsible for developing automatic data processing (ADP) contingency plans with an approach for selecting an alternate processing capability. It describes the alternatives that are currently available and provides guidance on developing selection criteria. A checklist for evaluating the suitability of the alternatives is provided.

Contingency planning, which is required of all Federal agencies [13], involves the preparation of procedures that will facilitate a timely recovery from events that disrupt data processing services. Contingency planning requires that both management and technical solutions be applied to the problem of continuing data processing services after the occurrence of a harmful event. When senior management understands the importance of developing and testing contingency plans and provides the resources for this purpose, the plan has a greater chance of success.

Contingency planning requires the preparation of emergency response, backup processing, and recovery actions procedures. This guide focuses on the backup processing aspect of contingency planning. FIPS PUB 87 [10] provides guidance in preparing all three elements of the contingency plan.

Planning an alternate processing strategy requires an understanding and identification of critical processing requirements. Once such requirements have been defined, the selection process can begin. This document specifies requirements categories that planners may use as a guide for defining site-specific requirements. These requirements will serve as criteria for selecting the most suitable alternate processing support.

A description of the alternatives is provided, along with a discussion of the selection criteria significant for each. The alternatives include:

- Service Bureaus
- Time Brokers
- Dedicated Contingency Centers
- Membership in Shared Contingency Facilities
- Empty Shells
- Reciprocal Agreements
- Separate Facilities Under the Same Management
- Fortress Concept with Full Redundancy
- Reversion to Manual Processing
- Use of Microcomputers
- Portable Sites
- Empty Buildings

Selection of any one of these alternatives or combination of alternatives, ranging from temporary use of a service bureau to

the construction of a new facility, will typically depend upon the severity and longevity of a harmful event. No matter what circumstances arise, it is prudent to develop backup procedures and to select alternate processing support in advance. A well-documented, thoroughly tested, and workable strategy will help reduce long delays and hasten a rapid return to normal operations.

For large organizations, it may take a great deal of time to develop an ADP backup processing plan. Regardless of the size of the organization, with a good deal of conscientious effort and commitment from all levels of the organization, a workable backup capability can affect successful recovery from disaster.

Figure 1 illustrates the selection process and serves as a guide on the use of this document.

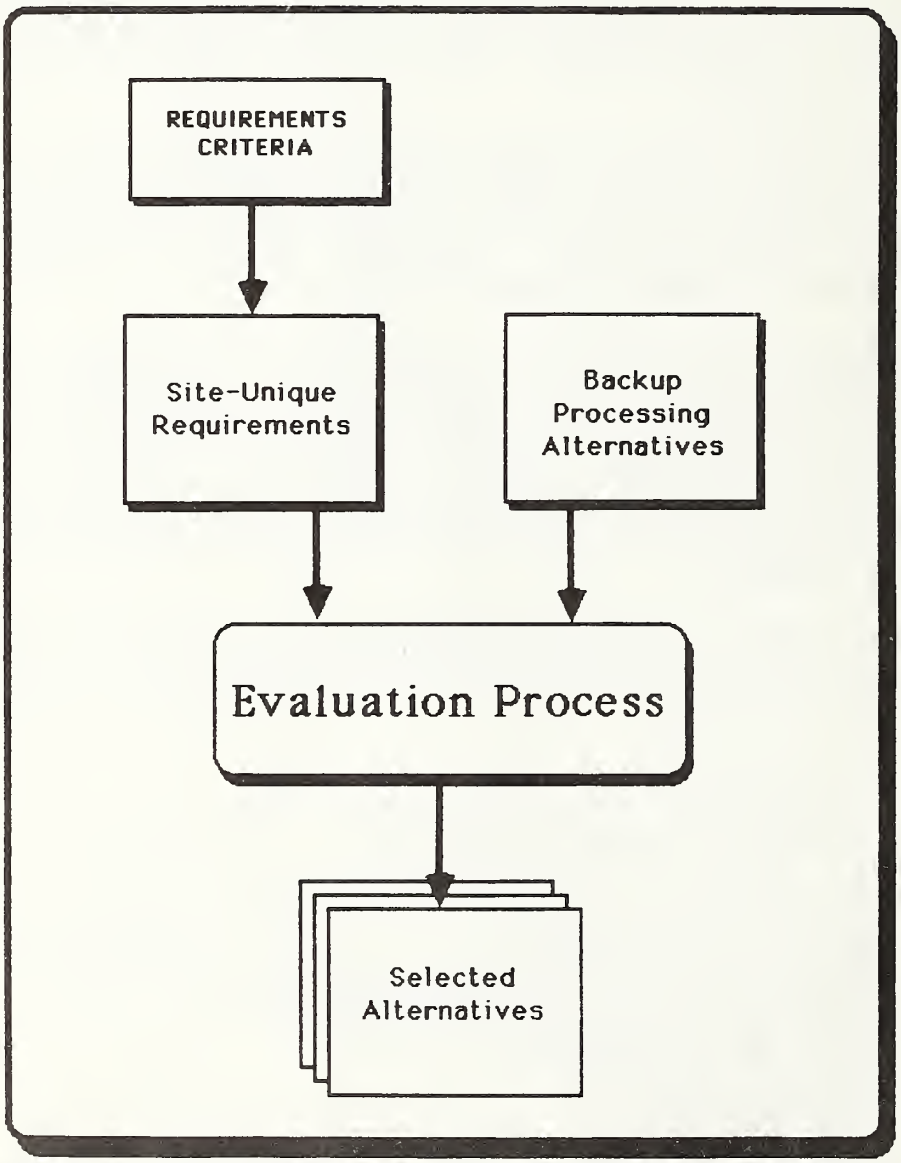


Figure 1. The Selection Process

2. MANAGEMENT RESPONSIBILITY

The ADP facility generally provides vital services to many functional areas within an organization--services without which the organization could not survive. In view of the trend toward greater dependence on ADP services, senior managers should recognize the importance of a workable, cost-effective alternate processing strategy. This strategy should serve to reduce further harm that can result from the loss or damage to ADP resources.

Senior management must take responsibility for the planning, funding, implementation, testing, and certification of an alternate processing strategy. Specifically, senior management should do the following:

- Assign responsibility to manage the development of an alternate processing strategy.
- Demonstrate to all levels of the organization a firm commitment to planning and supporting an alternate processing strategy.
- Commit the resources necessary to develop the alternate processing strategy.
- Monitor development of the strategy.
- Require and verify periodic testing of the alternate processing strategy.
- Require and verify periodic review, updating, and certification of the alternate processing strategy. Updates to the plan may result from tests, addition of new applications, or changing dependence of the organization upon ADP.

The process of developing an alternate processing strategy involves many people in addition to the planners. The scope of the project should be defined to include all system users, support offices (e.g., Legal), and the ADP facility. Senior management should leave no doubt that support is required at all levels of the organization.

2.1 ESTABLISH A PROJECT PLAN AND PROJECT TEAM

It is essential that project plans be developed which will be effective in developing an alternate processing strategy. The project plan should define the objectives and scope of the contingency planning effort; specify a general plan of action, constraints, and dependencies; assign responsibility; and establish milestones, reporting schedules, and cost estimates.

A project team responsible for contingency planning should be designated in writing and a team leader assigned. This working group will have primary responsibility for the following actions:

- Coordinating the planning with appropriate organizational components.
- Defining the requirements necessary to continue critical processing.
- Selecting appropriate alternate proessing support.
- Managing comprehensive tests of the selected alternative.
- Writing backup operations procedures.
- Reporting project results to management.

Drawing upon the knowledge of individuals with varied skills will increase the probability of a successful recovery. Team members may be appointed from various components of the organization such as:

- data processing,
- application owners,
- computer security,
- personnel,
- internal audit,
- quality assurance,
- procurement,
- legal, and
- public affairs.

Planning a backup strategy should not be used as a training ground where junior staff are left to "sink-or-swim." Individuals selected from the functional areas listed above should be aware of their own component's mission and its relationship to the overall organizational mission.

Managers should recognize that development of an alternate processing strategy can be a time-consuming process that requires coordination with various components of the organization. The working group should be allowed sufficient time in which to effectively complete the project.

2.2 CONDUCT A RISK ANALYSIS

Risk analysis is the process of identifying, either quantitatively or qualitatively, the impact of potential threats to organizations operating ADP facilities. Risk analysis serves to point out the risks that exist within the organization and the damage which can result from an occurrence of an unfavorable

event. Some risk analysis methodologies also involve estimation of the frequency of occurrence of adverse circumstances. A risk analysis procedure is provided in FIPS PUB 65, Guideline for Automatic Data Processing Risk Analysis [11].

A risk analysis provides senior management with information on which to base decisions on whether it is best to prevent the occurrence of a harmful event, to reduce the impact of such occurrences, or to simply recognize that a potential for loss exists (i.e., accept the risk) [11]. The risk analysis should help managers compare the cost of the probable consequences to the cost of effective safeguards.

Another benefit of risk analysis is that the documentation collected during the data gathering stage can be used to develop contingency plans as well. Data collection activities generally include critical applications identification, hardware configuration listings, data communications diagrams, computer facility area layouts, listings of special forms and supplies, and off-site storage inventories [11]. All of these are important in the development of contingency plans.

2.3 IDENTIFY CRITICAL APPLICATIONS

Critical applications are those without which the organization could not function. Specifically, an application may be considered critical if it is required to:

- Accomplish a mission of the organization (e.g., the application supports a requirement stemming from an Executive Order).
- Maintain vital public services (e.g., payment of benefits).
- Maintain national security (e.g., command and control systems).
- Process high dollar value transactions where ADP interruptions can be costly (e.g., electronic funds transfer, inventory control, or shipping and warehousing).

Prior identification of applications which support major business functions will help reduce delays and hasten the prompt restart of critical processing. Attention should be given to ensuring that critical applications and software are sufficiently protected against loss. Details for protecting vital software are discussed in Section 2.5.

2.4 RANK CRITICAL APPLICATIONS

Once critical applications have been identified, they must be ranked based on their relative importance to the mission of the organization. This priority list will serve as an optimum processing guide, enabling the backup processing strategy to be implemented with fewer delays. Thus, the losses that can result from interrupted data processing may be significantly reduced.

Since processing priorities can change as the period of interruption increases, it may be useful to develop several priority lists that span different processing cycles (e.g., daily, monthly, quarterly, and year-end cycles). When the disruption period is short, rescheduling critical applications is a relatively simple task for most organizations. Conversely, as the interruption period increases, more applications are affected and rescheduling becomes increasingly more difficult. The priority lists can take into account the timing of the disruption and the delay periods that can be tolerated for each critical application.

2.5 DEVELOP AN OFF-SITE STORAGE PROGRAM

Storing critical data off-site reduces the vulnerability to natural hazards, human error, sabotage, and other threats. The ability to recover data vital to the computer operation is absolutely necessary if continued service is to be provided during backup and recovery situations. The risk is not only the loss of data but the length of time necessary to reconstruct these data. Having access to media stored away from the primary computer facility ensures that critical data files can be restored if master files are lost or destroyed.

Vital application and system software should also be maintained at an off-site storage facility. Care must be taken to ensure that files and programs stored off-site are current versions. Storing multiple generations of files and programs is recommended so that the period spanned is long enough to ensure recovery.

An ideal off-site repository is one dedicated to the storage of backup computer media. Such installations are usually environmentally controlled and provide transportation of media to and from the primary site. Ideally, the off-site storage facility should be located far enough away not to be affected by the same hazards, but close enough to allow a quick response when time is critical.

2.6 CERTIFICATION OF THE ALTERNATE PROCESSING STRATEGY

Senior management is responsible for certifying the alternate processing strategy. The certification process requires that backup performance standards and test procedures be

developed for each critical application by an independent third-party quality assurance group. This group should perform a comprehensive test of each application including its operational procedures.

Such tests should produce measurable results that demonstrate how well the strategy satisfies the requirements of each critical application. Once the test objectives have been met, written certification should be submitted to the Approving Official for signature. The certification document should state that the backup alternative satisfies the organization's performance measurements.

3. REQUIREMENTS DEFINITION

Selection of an alternate processing capability cannot proceed until requirements for the support of critical applications have been defined. Once documented, these requirements should be used to evaluate the services provided by each of the alternatives.

This section identifies requirements criteria that contingency planners should use as a guide for defining site-specific needs. For each criterion, specific considerations are discussed. The requirements criteria addressed include:

- o Availability and reliability of the alternate facility
- o Compatibility of hardware
- o Compatibility of software
- o Physical capacity of the alternate facility
- o Environmental support
- o Telecommunications support
- o Location of the alternate facility
- o Sufficiency of test periods
- o Security capabilities
- o Cost-effectiveness
- o Completeness of contracts and agreements
- o Quality of assistance offered

3.1 AVAILABILITY AND RELIABILITY OF THE ALTERNATE FACILITY

Availability addresses the amount of lead time required before the backup facility can be used. Some backup facilities, for example, will offer immediate occupancy after notification of disaster, while others may not provide use of their system resources for several days. Therefore, it will be necessary to estimate the delays which can be tolerated before significant losses begin to accrue. Before placing dependence on an alternate facility, planners should ensure that the site will be available within the acceptable delay period.

The maximum length of time an alternate site will provide backup processing support is another consideration not to be overlooked. The backup site should be one that will allow the affected facility enough time to process its critical workload while its data processing facility is being restored. It will be very disruptive to move to one location only to find that yet another unexpected move is required.

Another important point is that of reliability. Consult client references to verify the reputation and solvency of a commercial facility before entering into a contract, i.e., does the alternate site meet its business commitments? Will it be around when needed? Knowing, at least in a general way, that the vendor being considered is reliable will provide confidence in the backup strategy being developed.

3.2 COMPATIBILITY OF HARDWARE AND SOFTWARE

It will be important that planners define the minimum hardware and software characteristics, system resources, and peripheral equipment needed for backup processing. The alternate facility should be one that can provide the minimum hardware and software configurations, including operating system, compilers, utilities, data base management, and telecommunications. The likelihood that processing delays will be minimized is far greater when fewer configuration differences exist at the alternate site.

In addition, the selected site should be monitored periodically for changes in hardware and software that might result in incompatibility. Uncoordinated changes can cause even the most well-developed plan to go awry.

3.3 PHYSICAL CAPACITY OF THE ALTERNATE FACILITY

A backup facility should be one that has enough space to accommodate, with relative permanence, the affected organization while its data facility is being restored. An alternate site should provide enough work space not only to perform computer operations, but office and administrative functions, such as: input/output control, data entry, programming, and scheduling.

Conversely, if the backup facility being considered does not have ample capacity, the affected organization should arrange for the use of office space at another nearby location. A cohesive work environment may be lost, however, when tasks normally performed at one location are divided. On the other hand, when physical separation of administrative operations is unavoidable, a control group should be assigned the responsibility of coordinating the workflow between locations to ensure efficiency and effectiveness.

Some backup processing facilities provide office space, but do not provide office furniture and equipment. Everything needed to effectively perform administrative and office functions must be provided by the affected organization including business furniture, equipment, expendable supplies, typewriters, and terminals. The backup strategy should include some approach for meeting this need (e.g., lease arrangements).

An added convenience is the ability to store backup data, software, forms, and supplies at the backup facility. In any case, backup copies of material that are essential to the continuance of critical processing should be stored away from the primary site, at another nearby location.

3.4 ENVIRONMENTAL SUPPORT

When evaluating the suitability of the unequipped site, it is essential to ensure the adequacy of the following environmental systems:

- Raised flooring.
- Electrical power and lighting. (FIPS PUB 94 [12] provides guidance on electrical power and grounding for ADP installations.)
- Temperature and climate control.
- Monitoring and surveillance systems.
- Fire suppression and detection systems.
- Emergency backup power systems.

3.5 TELECOMMUNICATIONS SUPPORT

Telecommunications capabilities may not be available or compatible at the alternate site. Therefore, a key element in backup planning is to determine whether it is vital to continue online communications processing. If so, planners must decide what is needed to continue the teleprocessing function. These requirements must be planned in advance because it may take a long time to install communications lines at an alternate facility. It will, indeed, be an advantage to select a site where communications facilities have already been installed.

Moreover, growth of computer networks places increasing importance on the need to design a backup network processing plan. The consequences of a single-node failure can be reduced significantly if the remaining portion of the network is able to function. Duplication of communications hardware, software, and data distributed over multiple sites may reduce the impact of disaster.

3.6 LOCATION OF THE ALTERNATE FACILITY

There are several considerations that should be reflected in the backup site selection. The optimum facility location is:

- Close enough to allow the backup function to become operational quickly.
- Unlikely to be affected by the same contingency.
- Close enough to serve its users.

- Convenient to airports, major highways, or train stations when located out of town.

If an out-of-town facility is selected, some of the personnel may be reluctant to leave home and family after an occurrence of a severe disaster (e.g., flood, tornado, hurricane). Thus, delays can be expected when key personnel are unavailable. To preclude this, management should identify key job functions and cross-train employees to increase the availability of capable standby or replacement personnel. Assigning an alternate system manager for each critical system can further increase the organization's potential for successful recovery.

3.7 SUFFICIENCY OF TEST PERIODS

The alternate data processing facility must allow adequate time in which to test backup operations procedures. It is not uncommon to discover during testing deficiencies in procedures despite careful planning. A test is seldom completed without problems on the first attempt.

Therefore, the best method to ensure the backup strategy will perform as expected is to test and certify it at the alternate facility at regular, prearranged intervals. A planned sequential ordering of tests, beginning with the most fundamental steps of the plan and ending with full-scale processing at the alternate facility, will determine whether the plan will work as expected.

Changes in data processing operations which result in modifications to equipment, programs, and documentation further require that tests be conducted to ensure continued:

- Adequacy of the plan.
- Compatibility of hardware and software at the alternate processing facility.
- Recovery of critical applications using backup files and software previously stored offsite.
- Adequacy of training for personnel.

Indeed, successful implementation of a backup processing strategy can be assured only when all procedures have been thoroughly tested. Testing assures familiarity with and confidence in the plan during a crisis and serves to reduce confusion and anxiety.

3.8 SECURITY CAPABILITIES

Safeguards applied to the ADP systems, central computer facility, and connected terminal areas at an alternate location must meet the same requirements established for the data and applications at the primary facility.

Most commercial backup facilities provide some level of physical security. However, most do not accept responsibility for losses the user might incur due to theft or manipulation of data and place responsibility for its protection on the client. Therefore, security controls at the alternate facility should be carefully evaluated.

If protective measures are judged to be inadequate, arrangements should be made with the management at the backup site to upgrade security. Controls may be adequate for an interim period if supplemented by "quick fix" physical measures. Contingency planners may wish to look elsewhere for backup processing support if management at the alternate site is unwilling or unable to support increased security measures. On the other hand, planners may wish to accept the current security environment if it does not violate security regulations.

3.9 COST-EFFECTIVENESS

The issue of cost has two roles in the consideration of backup processing support. The first is a tool in comparing various alternatives. The second is in the justification of any backup capability. When comparing alternatives, the objective is to select the alternative with the smallest annualized cost. The cost of an alternate processing method should not exceed the amount of damage expected from the loss of data processing support.

Many of the costs for backup processing support can be quantified, thereby allowing cost comparisons. It will be important to understand all of the fees involved, such as membership, testing, notification, installation assistance, and other services. Agreements between cooperative organizations are generally less costly and do not require nearly as much advanced allocation of funds as do commercial facilities.

There are three basic cost elements associated with alternate processing support. The first two components are incurred whether or not the backup facility is put into operation; the last cost component is incurred only when the facility is activated.

- Initial Costs--The cost of initial setup, including membership, construction, or other fees.

- o Recurring Operating Costs--Recurring costs for maintaining and operating the facility, including rent, utilities, repair, and ongoing backup operations.

- o Activation Costs--Costs involved in the actual use of the backup capability, including disaster notification fees, facility usage charges, overtime, transportation, and other costs.

The first two cost elements can each be converted to an annual figure and then combined to produce a single annual cost. If the third figure is to be annualized, it must be multiplied by the annual frequency that the facility is expected to be activated. The product should be a small figure.

It is important to point out that costs alone should not dictate the choice of an alternate method of processing. All of the requirements necessary to continue critical processing should be weighed. Nonetheless, maintenance of the backup strategy should be treated as a recurring operating expense.

3.10 COMPLETENESS OF CONTRACTS AND AGREEMENTS

It is imperative to ensure that all services necessary to bring about a successful backup strategy are covered by contract. At the time of a disaster, it will be too late, too expensive, or too time-consuming to make changes. The organization's legal staff should assist in developing contracts and agreements for alternate processing support.

Since contracts vary widely among vendors, it is easy to make assumptions that can have harmful results. To avoid misunderstandings, nothing should be taken for granted and all agreements should be in writing. These precautions apply not only to commercial backup facilities but to non-commercial organizations (e.g., government organizations) that agree to provide reciprocal data processing support. All services that each of the organizations will provide the other should be included in the agreement. Furthermore, the fact that data processing facilities are under the same management does not preclude the need for developing detailed support agreements.

3.11 QUALITY OF ASSISTANCE PROVIDED

Restarting critical applications will be the affected site's greatest concern. There are several support details that can affect the speed at which critical tasks can be restarted. Therefore, it will be helpful if the alternate facility can assist in:

- o Finding housing for personnel when the alternate facility is located out-of-town.

- Installing equipment.
- Operating the hardware.
- Loading software and master files.

Such assistance is not absolutely necessary, but would be of added benefit. An important point is to ensure that every person impacted by any one of these actions is aware of them, and understands how to accomplish each of the tasks for which they have responsibility.

A summary of the actions necessary to develop a successful backup processing strategy is presented in Figure 2.

Planning a Backup Processing Strategy
o Conduct risk analysis.
o Identify critical application systems; involve users.
o Rank critical applications based on their importance.
o Define critical time delays that can be tolerated without degrading the mission.
o Store critical data, programs, and documentation off-site.
o Ensure the backup site can provide sufficient computer resources to handle the critical workload.
o Ensure the site being considered will be available within sufficient time to meet processing schedules.
o Ensure the backup site can provide a compatible hardware configuration.
o Ensure the operating system software at the alternate facility is compatible.
o Ensure the alternate site can provide enough space to accommodate essential staff.
o Ensure the adequacy of environmental systems at the alternate facility.
o Determine telecommunications requirements, ensuring minimal communications support can be provided by the alternate facility.
o Evaluate the location of the backup facility, planning resolutions to possible problems that can occur when using a remote facility.
o Develop a comprehensive test plan ensuring the backup facility will allow adequate time for testing.
o Ensure that security controls at the alternate facility provide a sufficient level of protection for data and equipment.
o Understand all pricing agreements, allocating funds for backup support in advance of an emergency.
o Ensure that all agreements are in writing.

Figure 2. Summary of Actions

4. DESCRIPTION OF THE ALTERNATIVES

The preceding section discussed the requirements and criteria for evaluating alternate processing methods. This section describes the alternatives and discusses the criterion that is significant for each alternative. Contingency planners should use their site-specific requirements, developed for each of the categories presented in Section 3, to evaluate the suitability of each of the alternatives described. Such an evaluation will help ensure that the most appropriate backup processing capability is selected. Selecting more than one alternative may be necessary to meet all critical processing requirements. A summary of advantages and disadvantages of each of the alternatives is provided at the end of this section in Figure 3. The alternatives described in this section include:

- Service Bureaus
- Time Brokers
- Dedicated Contingency Centers
- Membership in Shared Contingency Facilities
- Empty Shells
- Reciprocal Agreements
- Separate Facilities Under the Same Management
- Fortress Concept with Full Redundancy
- Reversion to Manual Processing
- Use of Microcomputers
- Portable Sites
- Empty Buildings

4.1 SERVICE BUREAUS

Service bureaus provide contingency services for a fee. Most, however, are used primarily for production processing. All of the processing is completed in a time-shared environment, supported by batch and interactive programming systems. Telecommunications is usually the predominant means of transmitting work to the service bureau.

4.1.1 Availability

Most service bureaus limit their services to current subscribers and, with very few exceptions, are unable to accept quickly a new data processing workload. Unless the service bureau can accept the additional work, and unless their capabilities to process an organization's critical applications are fully tested, the service bureau will be of little assistance in time to avoid serious processing delays. Thus, an organization may consider the service bureau as a short-term solution for processing selected applications.

4.1.2 Costs

A contract is generally negotiated which requires subscribers to pay a monthly membership fee for a predetermined period of time, usually one year. The user must pay an additional daily time-share fee if contingency services are actually required. Generally, subscribers of government-operated service bureaus pay only for services used.

4.2 TIME BROKERS

Time brokers serve as a resource for obtaining backup support. Time brokers find, for a fee, available processing time on other systems. Processing arrangements are made entirely through this third party service. Time brokers, however, do not guarantee that hardware and software configurations will fully satisfy critical requirements.

4.3 DEDICATED CONTINGENCY CENTERS (HOT SITES)

These are fully equipped computer centers (sometimes referred to as "Hot Sites") which include one or more computers and standard peripheral equipment. Most contingency centers are large enough to accommodate several users. Contingency centers are equipped with raised flooring, electric power, and air conditioning. Some have fire protection and warning devices, telecommunications lines, intrusion detection systems, and physical security. These centers are equipped with computer hardware that is compatible with that of a large number of subscribing organizations. This type of facility is intended to serve an organization that has sustained total destruction and cannot defer computer services.

4.3.1 Availability

Contingency centers provide backup computer resources when subscribing members notify the center of an emergency. There are two basic methods of notification: writing and telephoning. Many centers will not enter into a contract with a non-member currently experiencing a disaster. Some centers impose a limit on the number of subscribers, particularly in areas likely to be affected by wide-spread natural hazards such as floods, tornados, earthquakes, and hurricanes.

In addition, most centers impose a limit on the length of time the customer may use the equipment and space after notification of disaster (e.g., six weeks). For an additional fee, the period of usage can sometimes be extended, provided the resources have not been requested by another subscriber. The potential for conflict exists, however, if several subscribing organizations have concurrent need for the facility. In cases

where two or more clients suffer simultaneous disaster, a system of priority will determine customer service rights. For example, some contingency centers will provide services based on the order in which the notifications are received. Other centers may allow the affected organizations to decide which one will use the facility. If agreed upon, these organizations may share the alternate site.

Some vendors of "hot sites" also offer empty shells for backup processing which allows the site experiencing disaster to remain at the alternate location beyond the time originally designated. This kind of arrangement is beneficial when the amount of time needed to restore the primary data facility exceeds the contracted period.

4.3.2 Compatibility of Hardware

Contingency centers provide a basic hardware configuration that should be compatible with its subscribing organizations. On request, a center can usually provide additional peripheral equipment at an added cost to the customer. Some vendors may attempt to match the need for added or special equipment with other subscribers to reduce the expense to individual organizations.

4.3.3 Location

Although "hot sites" provide hardware and software configurations that are compatible with numerous data facilities, it may be difficult for some organizations to locate a compatible contingency center within a reasonable distance. If a nearby center cannot be located and a remote facility is chosen, contingency planners should be aware of the added costs, inconvenience, and delays that may result.

4.3.4 Costs

Customers under contract with contingency centers are required to pay a monthly membership fee for a predetermined time frame. Membership fees are but a small part of the costs, however. Some sites impose a disaster notification fee which the customer pays when the center is notified of an occurrence of disaster. Once the customer is located at the contingency center, a daily occupancy or usage fee is incurred. Costs may be imposed when test periods not covered by the contract are requested. Fees may also be incurred for use of the center's communications facilities.

4.3.5 Physical Capacity

Most contingency centers are large enough to provide for the temporary relocation of personnel. Subscribing organizations will usually be required to document how they intend to use this auxiliary space. The square footage of space provided will be limited to that agreed upon contractually. Additional floor space may be available upon request, but it will be preemptable in case another member has suffered a disaster. The contingency center may also require that members document the number and dimensions of office furniture that will be needed. The center will usually assist in developing floor layouts showing the placement of furniture and equipment. Most contingency centers do not provide storage facilities for office merchandise. In such cases, members are assisted in establishing agreements with local vendors to deliver the necessary furnishings to the alternate site when needed. All of the information required by the contingency center should be included in the contingency plan as well.

Some contingency centers can provide space to store office supplies, forms, and manuals. Such an arrangement must be made in advance.

4.3.6 Sufficiency of Test Periods

Most contingency centers allow subscribing organizations to test critical applications during predefined periods. Since the time allowed for testing varies among vendors, it is imperative that prospective clients understand the terms of the contract regarding allowable test periods.

4.4 MEMBERSHIP IN SHARED CONTINGENCY FACILITIES

Shared contingency facilities are essentially the same as dedicated contingency centers. The difference lies in the fact that membership is typically formed by a group of similar organizations which use, or could use, identifical hardware. Each participating organization proportionately funds the facility and configures it to satisfy its critical processing requirements. Such a facility could even be used to provide services to participants who are not faced with a contingency, but wish to process jobs that do not fit into the normal processing schedule.

4.4.1 Availability

Limited membership reduces the likelihood of a simultaneous need to use the facility, making this an attractive alternative.

4.4.2 Costs

An advantage of this backup processing alternative is that the budget impact for ADP contingency planning can be reduced for each organization when the cost is shared among several organizations. Further, operating costs may be lower than those of a commercial contingency center since the shared contingency facility is a non-profit operation.

4.4.3 Other Considerations

Organizations forming this type of facility must construct the entire backup system. The site must be equipped with hardware, telecommunications lines, and environmental support systems. In addition, a staff must remain on-site to ensure the backup facility is ready for operation at all times. For this reason, this alternative may prove expensive and difficult to maintain.

4.5 EMPTY SHELLS (COLD SITES)

Empty shells are large, unfurnished spaces which can be leased to house computers and telecommunications equipment. They are equipped with raised flooring, utilities, and communications lines. The client, however, must supply the necessary hardware and prepare the shell for processing (including arrangements to complete wiring, plumbing, cut outs, etc). It is also the responsibility of the affected organization to perform environmental testing at the empty shell to ensure that communications lines, air conditioning, chillers, power, and other systems perform properly. In addition, users are required to restore the site to its original state before leaving.

4.5.1 Availability

An owner of an empty shell may limit the number of subscribers and often will not enter into contract with a non-member currently experiencing disaster. Most shell owners allow a member that has lost processing capability up to six months occupancy, if needed. Conversely, other members may be locked out when the shell is being used. Some vendors permit extensions on the time a user may occupy the site, provided no other members require the facility.

Extensive planning is necessary to prepare the empty shell for backup processing. Organizations evaluating this alternative must consider how they will function while the shell is being

prepared. The time necessary to prepare the empty shell (i.e., delivery and installation of computer equipment) may constrain the organization's ability to meet the scheduling requirements of critical applications.

If critical processing can be deferred while the equipment is being installed, however, the empty shell may be a viable alternative. Otherwise, it may be considered for use in accomplishing long-term processing requirements, using another short-term alternative in the interim.

A number of vendors of computer hardware offer both empty shell and contingency center services. When vendors of hardware offer both of these backup processing capabilities, there is usually a limit on the length of time the contingency center may be occupied before the client is required to equip the empty shell. Some hardware vendors also lease time in their contingency centers for overload operations. Customers for this service have a lower priority and must vacate the premises immediately when other customers experience a disaster. These variations in services are pointed out to illustrate that a wide range of alternatives are available, and that vendors have varying approaches to disaster and contingency planning problems. Although every hardware vendor may not provide these services, the options are worth researching.

4.5.2 Compatibility of Hardware

The empty shell does not present a problem of hardware compatibility because the user must provide the computer equipment and hardware. Nevertheless, some consideration should be given to the convenience and timeliness of having computer hardware delivered and installed at the shell facility.

Vendors of hardware will usually expedite shipment of replacement computers when a data facility has experienced disaster. Prompt replacement, however, will depend upon pre-loss planning. Planners should establish an agreement with vendors regarding their plans for replacing equipment. Hardware replacement may be difficult if it has reached obsolenscence, is unavailable because it was manufactured in small quantities, manufacturers are no longer in existence, or it has been customized for the organization.

4.5.3 Costs

Shell subscribers pay a monthly membership fee for the right to use the facility. The shell owner may impose a notification fee as well. Once located at the alternate site, the user will be required to pay a daily usage fee.

4.5.4 Sufficiency of Test Periods

Because shell sites have no computers, full-scale testing of applications at the facility cannot be accomplished. Nevertheless, it is recommended that tests ranging from events that cause minor processing interruption to events that leave the data facility inoperable be simulated at the primary facility. This kind of rehearsal will identify some obvious errors and omissions in the backup strategy and familiarize personnel with their assigned tasks.

4.5.5 Security Capabilities

Empty shells are sometimes shared, creating the potential for a physical security control problem. If the shell is otherwise a viable alternative, procedures should be developed to provide additional security.

4.5.6 Other Considerations

If the shell is located out-of-town, licensed tradespeople familiar with local building codes may be needed to perform tasks necessary to prepare the site for processing. Determine, in advance, whether workers from the area will be needed and contract for their services.

4.6 RECIPROCAL AGREEMENTS (MUTUAL AID AGREEMENTS)

Reciprocal agreements are formally written, signed documents between two or more facilities. Each has agreed to allow the other use of its computer resources during an emergency. A reciprocal agreement requires that both organizations recognize, that during an emergency, both will operate in a reduced mode if resources are shared simultaneously. For this reason, it is essential that both organizations identify their critical workload and processing requirements in advance of a harmful event.

4.6.1 Availability

There is danger in placing too much dependence on this alternative because the reciprocating organization may be at such a high level of system utilization that it cannot support the workload of another site. In spite of good intentions, the affected data center will be forced to look for other alternatives if the backup facility does not honor its agreement. Reciprocal agreements are usually unenforceable.

4.6.2 Hardware and Software Compatibility

Hardware and operating system software must be compatible. Any changes in hardware or software by either facility may result in system incompatibility; therefore, the alternate site should be monitored for changes.

4.6.3 Costs

Reciprocal agreements do not require nearly as much advanced funding as do commercial facilities. Thus, this alternative may appear to be a practical option from a cost point of view. The prudent planner, however, should not consider cost alone but should evaluate other factors before selecting this alternative.

4.6.4 Sufficiency of Test Periods

This backup capability must be fully tested if it is to be approached with confidence. Some organizations allow themselves to be lulled into a sense of complacency and false security once a reciprocal agreement is in place, and they do not test backup procedures at the alternate site. Unfortunately, when full-scale testing is ignored, there is no guarantee that this option will work--it probably will not.

4.6.5 Security Capabilities

Security controls must provide an acceptable level of protection before this alternative can be considered viable. Organizations processing vastly different classification levels, for example, may find that reciprocal agreements conflict with the security objectives of maximum control and minimum risk.

4.6.6 Other Considerations

Organizations must consider that reciprocal agreements may be difficult to maintain because of differing organizational objectives. Organizations should review the agreement, at least annually, for continued applicability. At the time of review, the agreements should be revalidated with signatures of appropriate executives from each organization.

4.7 SEPARATE LOCATIONS UNDER THE SAME MANAGEMENT

This approach consists of two or more data processing installations which are managed by the same organization, but are geographically located far enough apart so that they are not likely to be physically affected by the same disaster. Hardware need not be completely redundant or identical, but must be

sufficient at each location to support the critical workload. The fact that a facility is part of the same organization does not preclude the need for detailed planning, however.

The ability to schedule an acceptable workload and the ease in transporting materials and personnel to the alternate site, as pointed out with other alternatives, is a major consideration when evaluating this option. Further, it is important that the alternate facility be monitored for any change in software or hardware configurations that could result in incompatibilities.

While this alternative might appear to have the same disadvantages as reciprocal agreements, there is an added benefit in having the same management regulate both facilities. Its decisions would extend to both centers. When economically feasible, this alternative may provide the best possible solution to backup processing.

4.8 FORTRESS CONCEPT WITH FULL REDUNDANCY

With this alternative all resources are put into one location. There is complete duplication of all hardware, software, and environmental systems. Very strong physical security is built into the facility. This alternative is viable in areas where there is no danger from floods, tornados, hurricanes, earth faults, and like conditions. Otherwise, this backup capability becomes vulnerable to total outage.

This option may be favored by organizations that require heavy security, or those that process applications which require or justify considerable effort to achieve uninterrupted performance (e.g., command and control, air traffic control). This alternative can be costly because of the hardware redundancy.

4.9 REVERSION TO MANUAL PROCESSING

This approach reverts back to a manual operation. It may be a workable choice if manual procedures that duplicate the automated process are documented. If, however, manual procedures are outdated, or simply not available, it may be impractical to rewrite them.

Generally, this option is seldom used with the expectation that critical processing needs can be fully satisfied. It may, however, be a suitable option if used in conjunction with another alternative. For example, planners may find that subsistence functions of a computer system can be supported by a manual process, for a short period, until critical operations are restarted at the alternate location.

4.10 USE OF MICROCOMPUTERS

This approach to backup processing integrates operations that can be supported by microcomputers or intelligent terminals. The microcomputer, for example, can be used to perform local processing, storage, data entry and query, and word processing. It may be used as a personal computer or double as a terminal to the mainframe. Hence, integration of microcomputers into the organization may ensure less dependence on the central host for computing power. To use this alternative, contingency planners should:

- Determine which operations can be accomplished by a microcomputer.
- Select commercial data management software that can support critical application's processing.
- Select hardware that will not only support current applications but which is flexible enough to support future applications.

When microcomputers are used as part of the overall backup processing strategy, they may be able to provide interim processing capability until the host is available. There is a danger, however, of incompleteness or inconsistency between data bases. Data base owners should ensure that both the host and microcomputer versions remain compatible.

4.11 OTHER POSSIBILITIES

The next two choices (Portable Site and Empty Building) may be used in conjunction with other alternatives, (e.g., the Service Bureau or Reciprocal Agreement).

4.11.1 Portable Sites

Trailers can be equipped with minimal hardware and environmental controls and brought to a designated location for backup processing. This is an option that can provide some processing support until a longer-range plan is implemented or until the primary facility is restored.

4.11.2 Empty Buildings

These are warehouses or other buildings which can be wired, equipped, furnished, and environmentally prepared. In addition, an empty building can provide office space when there is not sufficient space at the backup computer site.

When empty buildings are the property of the organization losing the data facility, a more successful recovery may be

accomplished than when the buildings are being rented. An organization may be reluctant, for example, to spend large sums of money preparing a rented building for operation. Conversely, when the building is owned by the organization experiencing the outage, the affected facility can work there indefinitely, relatively rent free, and operate on a schedule free of pressure.

However, if the time needed to convert unused space to accommodate computer operations exceeds the processing schedules for critical applications, this option may be inappropriate to satisfy short-term processing needs. On the other hand, it may be a viable option in the face of a long outage.

4.12 INSURANCE

Insurance, although frequently mentioned in connection with backup processing alternatives, is neither a method nor a substitute for developing an alternate processing strategy. Insurance is a method for obtaining financial reimbursement for the loss of hardware and the physical facility, but it makes no allowances for the information contained on tapes and disks. Special insurance coverages (e.g., Business Interruption Insurance) may apply to the protection of data from hazardous events. Insurance underwriters often require that organizations maintain an alternate processing capability before this type of coverage is written, however.

Insurance is not an option for Federal agencies since they are self-insured.

ALTERNATIVES	ADVANTAGES	DISADVANTAGES
1. Service Bureau/ Time Broker	Provides immediate access. Moderately priced.	Short-term access. Limited security. Support may change with normal business.
2. Dedicated Contingecy Center	Operationally ready for immediate occupancy. Environmentally controlled. Some communications capabilities provided.	May not be located nearby. Short-term occupancy. Expensive.
3. Shared Contingency Center	Costs are shared. Immdediate occupancy. Members may use for overload operations.	Difficult to maintain.
4. Empty Shell	Immediate occupancy. Long-term occupancy.	Requires delivery and installation of equipment. Requires a greater time frame becoming operational.
5. Reciprocal Agreement	Provides some processing support. Inexpensive.	Agreements are unenforceable. Promotes feelings of false security.
6. Separate Sites Under Same Management	Provides immediate backup. Proven effective.	
7. Fortress Concept	Redundant hardware and environmental controls under one roof.	Expensive. Subject to total outage.
8. Reversion to Manual Processing	Some work may get processed.	Completion of work is slow. Manual procedures may not be available.
9. Use of Microcomputers	Less dependence upon host. Will allow processing of selected applications.	Database inconsistency.
10. Portable Site	Provides some processing support.	May be necessary to limit the hardware configuration.
11. Empty Building	Can be converted into a data facility and later used for overload operations. Can provide office space when it is not available at the alternate facility.	Must be environmentally controlled. Requires installation and delivery of hardware. Greater time frame becoming operational.

Figure 3. Advantages and Disadvantages of the Alternatives

APPENDIX A

BACKUP PROCESSING SELECTION CHECKLIST

The questions that follow provide a method of assessing the overall suitability of the backup processing alternatives. By answering these questions, planners can focus on the strengths and weaknesses of the alternatives being considered.

A sample worksheet is included at the end of the questionnaire to further assist in the selection. The worksheet can be completed using a simple rating scheme when used in conjunction with the questionnaire. An example of a rating scheme that may be used follows:

"1" indicates the alternative fully satisfies the requirement.

"2" indicates the alternative only marginally satisfies the requirement.

"3" indicates the alternative cannot satisfy the requirement.

Based upon the completed worksheet, selection of an appropriate backup processing alternative can be made.

AVAILABILITY

1. Will the facility be available within sufficient time after notification of disaster?

2. Is the time allocated for use of the backup facility sufficient to meet critical processing needs?

3. Is there a written policy to determine facility usage priority when two or more customers experience simultaneous disasters? If so, is the policy reasonable and acceptable?

RELIABILITY

1. Can the alternate commercial facility provide references from other customers?

2. Has the financial condition of the backup facility been investigated to ensure that it is solvent?

3. If initiating a reciprocal agreement, can each of the organizations guarantee support?

HARDWARE COMPATIBILITY

1. Is the hardware configuration compatible?

2. Will the alternate facility allow the affected organization to move in hardware that is required but that which is not a part of the current configuration?

ENVIRONMENTAL CONDITIONS

1. Is the facility sufficiently equipped with chillers, motor generators, and air conditioning to support necessary hardware?

2. Are other environmental systems such as raised flooring, surveillance systems, and fire suppression and detection systems adequate?

PHYSICAL CAPACITY

1. Does the facility have enough space to allow essential staff to temporarily relocate? If so, will office furniture and supplies be provided?

2. Are there facilities to store critical backup media and documentation?

3. Does the facility have the capacity to accommodate the installation of additional hardware, if needed?

4. Does the facility have the physical capacity to store the output media that will be generated during backup processing?

TELECOMMUNICATIONS

1. Does the alternate facility have suitable communications capabilities?

2. If not, can the required communications facilities be installed within the required time frame?

GEOGRAPHICAL CONVENIENCE

1. Is the alternate facility within an acceptable distance?

2. Is the alternate located far enough away so as not to be affected by the same disaster?

TESTING

1. Does the alternate facility allow test time?

2. If so, is the time allowed sufficient to thoroughly test backup procedures to ensure critical applications can be recovered?

SECURITY

1. Does the facility provide adequate physical security?

2. Does the facility provide acceptable software/system security capabilities?

COSTS

1. Have all costs been included in the contract?

2. Does the cost of the alternative provide the most cost-effective backup capability?

CONTRACTS AND AGREEMENTS

1. Does the contract or agreement specify the processing capacity (e.g., number of peripherals, disk storage space, memory, etc.) that will be provided?

2. Does the contract set forth all the known terms and conditions by which the affected site must adhere to while using the backup facility?

ASSISTANCE PROVIDED

1. Are there staff at the alternate facility to assist you?

2. Are personnel available to assist vendors with the installation of equipment?

REQUIREMENTS / ALTERNATIVES	Availability	Reliability	Compatibility	Physical Capacity	Environmental Support	Telecommunications Support	Location	Test Periods	Security	Cost Effectiveness	Completeness of Contract	Assistance Offered
SERVICE BUREAU												
DEDICATED CONTINGENCY CENTER												
SHARED FACILITY												
EMPTY SHELL												
RECIPROCAL AGREEMENT												
SEPARATE LOCATIONS (COMMON MANAGEMENT)												
FORTRESS CONCEPT												
REVERSION TO MANUAL PROCESSING												
USE OF MICROCOMPUTERS												
PORTABLE SITE												
EMPTY BUILDING												

Figure 4. SELECTION WORKSHEET

APPENDIX B

REFERENCES AND ADDITIONAL READINGS

[1] "An Evaluation of Data Processing Machine Room Loss and Selected Recovery Strategies," MISRC-WP-79-04 Working Paper Series, Management Information Systems Research Center, University of Minnesota, June 1978.

[2] Ball, Leslie D.; Dentch, Gail; Emerson, Mary; Lewis, Martha; McWhorter, Susan; and Turgeon, Frank, "Disaster Recovery Services," Computers & Security 1 (1982), pp. 216-225.

[3] Comptroller General's Report to the Congress, "Most Federal Agencies Have Done Little Planning for ADP Disasters," December 1980, AFMD 81-16.

[4] Courtney, Robert H., Guidelines for Contingency Planning, IBM Publication TR21.761, Kingston, New York 1980.

[5] Foreign Corrupt Practices Act of 1977 (Public Law 95-213).

[6] Friedman, Stanley, "Contingency and Disaster Planning," Computers & Security, 1 (1982), pp. 34-40.

[7] Isaacson, Gerald I., "A Guide to Commercial Backup Services," Computer Security Journal, Spring 1983, pp. 51-69.

[8] Murray, Thomas J., "Disaster Recovery Planning," Operations Management, Auerbach Publishers Inc., (52-01-01).

[9] NBS. Executive Guide to ADP Contingency Planning, Washington, DC; January 1982; NBS Special Publication 500-85.

[10] NBS. "Guidelines for ADP Contingency Plans," Washington, DC; March 27, 1981; FIPS 87. Available from NTIS, Springfield, VA; FIPS-PUB-87.

[11] NBS. "Guideline for Automatic Data Processing Risk Analysis," Washington, DC; August 1, 1979; FIPS 65. Available from NTIS, Springfield, VA; FIPS-PUB-65.

[12] NBS. "Guideline on Electrical Power for ADP Installations," Washington, DC; September 21, 1983; FIPS 94. Available from NTIS, Springfield, VA; FIPS-PUB-94.

[13] OMB Circular A-71, Transmittal Memorandum No. 1, July 27, 1978.

[14] Posner, David, "Disaster Recovery Plan Testing," Data Security Management and Practice, Auerbach Publishers, Inc., (82-04-02).

[15] Silverman, Martin E., "Contingency Planning: The Backup Site Decision," Computer Security Journal, Spring 1983, pp. 43-59.

*U.S. GOVERNMENT PRINTING OFFICE 1985 0 - 491-070 (20292)

NBS-114A (REV. 2-8C)

U.S. DEPT. OF COMM. **BIBLIOGRAPHIC DATA SHEET** (See instructions)	1. PUBLICATION OR REPORT NO. NBS/SP-500/134	2. Performing Organ. Report No.	3. Publication Date November 1985

4. TITLE AND SUBTITLE

Computer Science and Technology:
Guide on Selecting ADP Backup Processing Alternatives

5. AUTHOR(S)

Irene Isaac

6. PERFORMING ORGANIZATION (If joint or other than NBS, see instructions)

NATIONAL BUREAU OF STANDARDS
DEPARTMENT OF COMMERCE
GAITHERSBURG, MD 20899

7. Contract/Grant No.

8. Type of Report & Period Covered

Final

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (Street, City, State, ZIP)

Same as #6.

10. SUPPLEMENTARY NOTES

Library of Congress Catalog Card Number: 85-600618

☐ Document describes a computer program; SF-185, FIPS Software Summary, is attached.

11. ABSTRACT (A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here)

This publication addresses the issue of selecting ADP backup processing support in advance of events that cause the loss of data processing capability. The document emphasizes the need for managers at all levels of the organization to support the planning, funding, and testing of an alternate processing strategy. It provides a general description of the alternatives, and recommends criteria for selecting the most suitable alternate processing method.

12. KEY WORDS (Six to twelve entries; alphabetical order; capitalize only proper names; and separate key words by semicolons)

backup operations; contingency planning; disaster recovery

13. AVAILABILITY

☒ Unlimited

☐ For Official Distribution. Do Not Release to NTIS

☒ Order From Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.

☐ Order From National Technical Information Service (NTIS), Springfield, VA. 22161

14. NO. OF PRINTED PAGES

41

15. Price

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SCIENCE & TECHNOLOGY

Superintendent of Documents,
Government Printing Office,
Washington, DC 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Bureau of Standards Special Publication 500-.

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

(Notification key N-503)

NBS Technical Publications

Periodical

Journal of Research—The Journal of Research of the National Bureau of Standards reports NBS research and development in those disciplines of the physical and engineering sciences in which the Bureau is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Bureau's technical and scientific programs. Issued six times a year.

Nonperiodicals

Monographs—Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NBS, NBS annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NBS under the authority of the National Standard Data Act (Public Law 90-396).
NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published quarterly for NBS by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements are available from ACS, 1155 Sixteenth St., NW, Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Bureau on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NBS under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NBS administers this program as a supplement to the activities of the private sector standardizing organizations.

Consumer Information Series—Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.
Order the **above** *NBS publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*
Order the **following** *NBS publications—FIPS and NBSIR's—from the National Technical Information Service, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NBS pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NBS Interagency Reports (NBSIR)—A special series of interim or final reports on work performed by NBS for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service, Springfield, VA 22161, in paper copy or microfiche form.

U.S. Department of Commerce
National Bureau of Standards
Gaithersburg, MD 20899

Official Business
Penalty for Private Use $300