Computer Science and Technology

NBS Special Publication 500-85

Executive Guide to ADP Contingency Planning

Computer Science and Technology

NBS Special Publication 500-85

Executive Guide to ADP Contingency Planning

James K. Shaw
Stuart W. Katzke

Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, DC 20234

U.S. DEPARTMENT OF COMMERCE
Malcolm Baldrige, Secretary

National Bureau of Standards
Ernest Ambler, Director

Issued January 1982

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.

National Bureau of Standards
Special Publication 500-85
Nat. Bur. Stand. (U.S.), Spec. Publ. 500-85, 16 pages (Jan. 1982)
CODEN: XNBSAV

Library of Congress Catalog Card Number:
81-600182

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1982

FOREWORD

This publication has been prepared for executives and managers who depend on ADP resources and services to accomplish the organizational objectives for which they are responsible. The goal is to help in understanding the need for Automatic Data Processing (ADP) contingency planning, to specify management's scope of involvement, to indicate in summary form the contents of ADP contingency plans and how one proceeds in developing such plans.

There are, indeed, many existing methods and procedures concerning contingency planning, each of which may be adequate when used for the specific purposes intended by the authors. The process shown in this document is based on the method described in Federal Information Processing Standards Publication (FIPS PUB) 87, Guidelines for ADP Contingency Planning [6]. The primary intended audience of FIPS PUB 87 comprises line managers and others within the Federal data processing community who are specifically responsible for ADP resources. The material herein has been made sufficiently general in nature so as to be useful to all managers throughout the organizational structure engaged in any activity which receives ADP support.

This document is part of a continuing series of publications on the subject of computer security prepared by the Institute for Computer Sciences and Technology.

ABSTRACT

This document provides, in the form of questions and answers, the background and basic essential information required to understand the developmental process for Automatic Data Processing (ADP) contingency plans. The primary intended audience consists of executives and managers who depend on ADP resources and services, yet may not be directly responsible for the daily management or supervision of data processing activities or facilities. The publication should also be especially beneficial to individuals responsible for ensuring compliance with Office of Management and Budget Circular A-71, Transmittal Memorandum Number 1, July 27, 1978.

Key words: ADP security; backup operations; computer security; contingency planning; emergency response; Federal Information Processing Standards Publication; recovery actions.

CONTENTS

BASIC TERMS

Backup operation is a method for accomplishing essential tasks subsequent to disruption of the ADP facility and for continuing operations until the facility is sufficiently restored.

Computer security refers to the technological safeguards and managerial procedures which can be applied to computer hardware, programs, data and facilities to assure the availability, integrity and confidentiality of computer based resources and to assure that intended functions are performed without harmful side effects.

Critical functions, systems, and resources are those without which the organization cannot continue to operate, or even survive.

Emergency response is the immediate action taken upon occurrence of events such as natural disasters, fire, civil disruption, and bomb threats in order to protect lives, limit the damage to property, and minimize the impact on ADP operations.

Recovery consists of the restoration of the ADP facility or other related assets following physical destruction or major damage.

Risk analysis is an evaluation of the threats to and the loss potential of an ADP facility leading to an estimate of annual loss. Risk analysis results are used in the selection of cost effective remedial measures.

WHY ADP CONTINGENCY PLANNING

1. What is contingency planning?

Contingency planning is an accepted and recommended management practice which provides for well thought out responses either to preclude or, at least, to mitigate the harmful effects of potential disruptive events. Prior to preparing contingency plans for data processing activities, it is necessary to perform a risk analysis to determine the critical ADP systems and to weigh the threats and vulnerabilities as they relate to the organization. Potential emergency situations can then be anticipated, strategies for coping with them can be developed, and finally, a predetermination of expected responses to each type of emergency can be made. Contingency planning should, of course, include the actions which must be taken in response to major disasters such as floods and hurricanes. However, it is essential to remember that due to their greater frequency of occurrence, minor, more mundane events such as hardware and software failures, and operator errors, cause far greater disruption of service. Contingency planning, if it is to be effective, should include the means to prevent, or to recover from, minor disruptions as well as catastrophic situations.

2. Why should I be concerned about contingency planning?

The growing dependence during the past two decades of virtually all Federal agencies on ADP resources continues today at an unprecedented rate. This expanding dependence increases the importance of plans to prevent loss of ADP service to vital agency functions and activities.

Until very recently computers were widely regarded as simply a faster and more cost effective means of performing already established manual procedures. Also, when a computer failure occurred, it was possible to revert to the old manual processes with little more effect on the organization than inconvenience. Today, however, the computer must be considered a means of doing what cannot otherwise be done without it. Further, reverting to manual processes upon loss of the ADP resources, for whatever reason, is usually not practical and often quite impossible. It is critical that management recognize this dependence on the ADP resources in order to fully appreciate its own role in contingency planning. The plans should offer adequate assurance that any reasonably anticipatable interruption of an ADP facility's services will not preclude the continued execution of the agency's mission.

3. What role should management have in the ADP contingency plan development process?

The key ingredient of a successful ADP contingency plan is support of the plan by *both* ADP management and senior organizational management. The fact that support by ADP management is necessary is apparent; the requirement for organizational management support, though perhaps not immediately obvious, is also absolutely essential. The primary reason is that ADP services are essential to virtually all echelons of the organization. Without ADP support, many of the organizational functions cannot be performed. Consequently, management must determine the critical functions of the organization and the interaction and relationships that the ADP activity has with each of these. ADP management must not be placed in the position of having to determine unilaterally which functions throughout the organization are critical and which should be given first priority in an emergency. This is a responsibility of senior management. In summary, management should:

- Prior to the preparation of an ADP contingency plan, direct that a comprehensive risk analysis be accomplished (See 11).
- Direct that all affected elements of the organization participate in the planning process.
- Direct the periodic comprehensive testing of the plan and revision as necessary.

4. Who prepares the ADP contingency plan?

Responsibility for plan preparation should be in the data processing activity. Some input and assistance from other activities will be necessary, but the overall responsibility for preparing, maintaining and testing the plan should be assigned to the data processing activity.

5. What types of events can disrupt the ADP services on which I depend?

Data processing services are susceptible to a diverse variety of actions which, if not anticipated, create unwelcome disruptions and unnecessary expense in recovery. A brief, nonexhaustive list includes air conditioning failure, power failure, natural disasters, accidents such as sprinkler activation and Halon discharge, lost or destroyed data, forms or other supplies unavailable, strikes, personnel unavailable due to weather, and malicious attacks by terrorists or disgruntled employees.

6. Are there specific government directives which require contingency plans for ADP activities?

Several requirements impact contingency planning, both indirectly and specifically. These are:

- Public Law 93-579 (Privacy Act of 1974), Subsection 3(e)(5) requires that agencies maintaining systems of records subject to the Privacy Act shall: "maintain all records . . . with such accuracy, relevance, timeliness and completeness as is reasonably necessary . . ." Further, subsection (3)(e)(10) stipulates that agencies shall: "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity . . ."

- Federal Property Management Regulations (FPMR). The General Services Administration (GSA) has published comprehensive requirements for ADP contingency planning in 41 CFR, Chapter 101, subparts 101-35 and 101-36, FPMR.

- Office of Management and Budget (OMB) Circular A-71, Transmittal Memorandum Number 1, July 27, 1978 contains a wide range of requirements on computer security, including contingency planning. In particular, it requires that each agency must include in its security program policies and responsibilities for assuring that appropriate contingency plans are developed, tested and maintained.

7. What guidance is available on developing a contingency plan?

Two guidelines published by the National Bureau of Standards are particularly relevant to contingency planning: FIPS PUB 31, Guidelines for Automatic Data Processing Physical Security and Risk Management [7], and FIPS PUB 87, Guidelines for ADP Contingency Planning [6]. Other sources are found in the *Bibliography*.

8. How does contingency planning fit into the overall ADP security program?

A successful ADP security program consists of a number of elements. The sum total of all elements provides a synergistic effect on the overall security program. Contingency planning is but one of these elements; others are:

- Statement of security policy objectives

- Assignment of security responsibilities

- Definition of security requirements
- Performance of risk analyses
- Selection and implementation of safeguards (administrative, physical, and technical)
- Performance of periodic audits and evaluations
- Security considerations during ADP system development or procurement, to include quality assurance, configuration management and documentation practices
- Personnel hiring/termination practices and training

Many functions now thought of as belonging to ADP security have traditionally been categorized as a part of good management. Contingency planning is certainly one of these, as prudent managers have always planned for the actions to be taken should unexpected events occur. Unfortunately, however, the ever increasing growth in dependence on the ADP resources has not been matched by a corresponding growth in awareness of the need to preserve those vital resources. Actions and events occurring now, however, make it increasingly important to recognize ADP resources for what they are, i.e., a vital element of the organizations which they support and, to a growing extent, one without which such organizations may not survive.

DEVELOPING THE PLAN

9. Since contingency plans should be developed by all Federal ADP facilities, can't I use those developed by other agencies and avoid duplication?

Although many similarities exist among ADP facilities, the disparities in equipment, relative criticality of functions, types of customers, geographical locations and other factors tend to make each facility unique. This uniqueness precludes the use of a single contingency plan by more than one activity.

10. How should one begin developing a contingency plan?

Two things are essential to the development of adequate, cost-effective, and workable contingency plans. First, the functions supported by ADP which are critical to the

mission of the parent organization must be identified. These usually represent a relatively small percentage of the total ADP workload. Second, the resources essential to the accomplishment of these specific functions must also be identified. A formal risk analysis, as described in FIPS PUB 65, Guideline for ADP Risk Analysis [5], or other similar methodologies, will provide the data from which identification of both critical functions and critical resources can be derived. Once this is done, preparation of the plan may be begun in a logical, systematic manner. Generally, the plan is developed in three parts–Preliminary Planning, Preparatory Actions, and the Action Plan. Each part is described below (See 13).

11. Who performs a risk analysis?

A risk analysis for the ADP operation should generally be accomplished under the aegis of personnel within the ADP activity, quite appropriately with the advice and consent of the individual assigned the responsibility for the security of the installation under the provisions of OMB Circular A-71, TM No. 1. Additionally, it is essential that management direct participation by other organizational activities as required to support the process.

12. What strategies should be considered in ADP contingency planning?

In order to develop an effective plan, those charged with doing so must have a clear understanding of what the goals are before commencing preparation of the plan. To accomplish this, management must approve of a number of strategies to cover a variety of unexpected and unusual situations which might occur (Strategy selection is included in Preliminary Planning (See 13)). For example, for backup operations the approved strategies might be mutual aid agreements, no backup hardware, use of commercial contingency centers, having more than one ADP site, etc.

13. What are the critical elements of a contingency plan?

It is difficult to categorize any one element or part of a contingency plan as being more important than another. Essentially, each part of the plan is critical and must be accomplished with equal diligence for the plan to be successful. The three major parts of the contingency plan, as specified in FIPS PUB 87, are:

- Preliminary Planning (Part One). This part establishes the ground rules for the remainder of the plan, i.e., it describes the purpose, scope and assumptions relevant to the plan. It also assigns responsibilities,

and describes the organizational strategy for coping with emergencies. The strategies selected will, to a large extent, directly influence the development and amount of detail in the following two parts of the plan.

- Preparatory Actions (Part Two). This part contains sections which describe *how* the organization is to respond to an emergency. For example, instructions should be developed which specify how to maintain the contents of off-site storage, how to form backup teams, how to determine applications and system software requirements needed for different situations, and how to establish communications requirements. This part of the plan is prepared in as much detail as possible since it should be read and studied beforehand by those who ultimately must respond to an emergency.

- Action Plan (Part Three). This part consists of three sections which document *what* to do when an emergency happens. It is not intended to be a tutorial, but should state concisely the actions necessary to effect the organizational strategies which were selected earlier and documented in part one of the plan. The three sections of this part are:

  – Emergency Response Actions. This category includes those actions which employees must take immediately upon the occurrence of an emergency to protect lives and other resources. These actions are typically necessary upon the occurrence of major events such as tornadoes, floods, fire and earthquakes, as well as in instances of more common happenings such as power outages, bursting water pipes, etc.

  – Backup Operations Actions. This category includes those actions necessary to effect temporary operations at an alternate location when operations at the home facility are no longer possible for whatever reason. These may entail transportation of files, office supplies, equipment, a variety of other materials, and the employees to the alternate site, and the initiation of ADP operations for an indeterminate period of time.

  – Recovery Actions. This section should describe what must be done to restore permanent operations at the home facility following a disaster or major disruption of service. Included may be plans to rebuild the facility, lease alternate facilities and equipment, etc.

14. How large and how detailed should the typical ADP contingency plan be?

The value of a plan is not necessarily proportional to its size. The indiscriminate inclusion of material of doubtful

value in the plan will seriously downgrade its usefulness to the organization. While no recommendation is made concerning the length of a contingency plan, most organizations should find that the plan will fit comfortably in a regular loose-leaf notebook. Continuous effort will be required to keep the plan trim and concise, yet sufficiently detailed to communicate the relevant information.

OTHER CONSIDERATIONS

15. What effect will the ADP contingency plan have on the normal day-to-day operation?

Generally, little effect will be noticed. During development and documentation of the plan, some personnel will have to be diverted from their routine tasks to participate. Careful testing of the plan should cause minimal disruption. For example, to test the backup operations actions, the needed backup files and materials would be taken to the alternate site for processing while regular operations continue at the home site. Also, to test emergency response actions for fires, bursting pipes, etc., it is not necessary to cease operations. Frequently, testing can be accomplished in conjunction with other regularly scheduled events, e.g., if the ADP activity closes for the weekend, emergency power down procedures can be tested very effectively when preparing to shut down the system for the weekend.

16. My ADP support is furnished by a service agency (or through interagency agreement). How does contingency planning affect me?

It is especially important to consider ADP contingency planning in this case. *Do not assume* that the ADP activity (whether Governmental or commercial) which normally provides your service will be able to support you if their ADP operation is damaged or destroyed. Quite often, emergency support is not part of the agreement; consequently, if ADP support is necessary to the successful operation of your function, *you* must initiate the action to ensure the availability of service during an emergency. If a responsive contingency plan is not extant, and emergency support is first sought when needed, days, or even weeks, may be necessary to restore a semblance of normality to your activity. Each activity that receives ADP support should develop a contingency plan to address all aspects of emergency coverage, and the plan should be subjected periodically to rigorous testing and review. A key point to remember is that even though day-to-day ADP support from a service

agency may be outstanding, it cannot be assumed that similar service will be available if the servicing activity has an emergency situation.

17. My ADP equipment is part of a distributed data processing (DDP) network. How does contingency planning affect me?

Managers of DDP nodes should consider ADP contingency planning from two perspectives:

- As a stand-alone entity if the equipment is capable of processing applications without being connected to the network. For this situation, contingency planning should be essentially the same as that for a large computer center, although obviously the scope may be smaller. Many DDP nodes accomplish considerable stand-alone processing which, routinely, may include ADP systems that are critical to the parent organization.

- As an element of the DDP network. The contingency plan should reflect the degree of interaction between the node and other computers in the network, and include those actions necessary to be effected when connections are downgraded or severed. Consider eventualities such as one or more communications links severed, one or more of the other nodes down, or various combinations of both. During times of disruption, some processing may have to be postponed; however, quite often, it is possible to operate in a downgraded (i.e., stand-alone) mode by batching transactions for later transmission. Additionally, alternative routing through other than normally used communications channels may be possible, thus permitting continuation of normal processing.

18. How is contingency planning related to the normal ADP application systems design process?

If, during the initiation, requirements definition, and design phases of systems development, recovery checkpoints are specified and documented, contingency planning will undoubtedly be easier to accomplish. For example for recovery purposes, during the course of normal operations, files must be periodically dumped for transfer to the alternate storage site. If sufficient recovery checkpoints are designated at the very beginning, a subsequent retrofit operation in the documentation and procedures can be precluded. Effective systems designers and analysts know that no system is completely fail-safe; therefore, they will design such safeguards and procedures into their systems as will facilitate backup and recovery operations when the need arises.

BIBLIOGRAPHY

The following publications deal mostly with ADP contingency planning, but also provide a wide variety of information on varying aspects of computer security. The list is not intended to be all inclusive; rather it is meant to provide those interested in ADP security, particularly contingency planning, with a starting point of publications generally available and pertinent to the task at hand.

1. Broadbent, D., Contingency Planning, The National Computing Centre, Oxford Road, Manchester, United Kingdom (1979).
2. Browne, P. S., Security: Checklist for Computer Center Self Audits, AFIPS Press, Montvale, NJ 07645 (1979). Order from AFIPS, 1815 N. Lynn St., Suite 800, Arlington, VA 22209.
3. Canning, R., Computer Security: Backup and Recovery Methods. EDP Analyzer. 10(1); January, 1972.
4. Disaster Preparedness, Office of Emergency Preparedness Report to Congress, Stock Number 4102-0006, Government Printing Office, Washington, DC (1972).
5. Guideline for ADP Risk Analysis, National Bureau of Standards (U.S.), Federal Information Processing Standards Publication (FIPS PUB) 65, National Technical Information Service, Springfield, VA (1979).
6. Guidelines for ADP Contingency Planning, National Bureau of Standards (U.S.), Federal Information Processing Standards Publication (FIPS PUB) 87, National Technical Information Service, Springfield, VA (1981).
7. Guidelines for ADP Physical Security and Risk Management, National Bureau of Standards (U.S.), Federal Information Processing Standards Publication (FIPS PUB) 31, National Technical Information Service, Springfield, VA (1974).
8. Lord, K. W., Jr., The Data Center Disaster Consultant, QED Information Sciences, Inc., Wellesley, MA 02181 (1977).
9. Martin, J., Security, Accuracy and Privacy in Computer Systems, Prentice-Hall, Inc., Englewood Cliffs, NJ (1973).
10. Martincic, J. A., A Disaster Recovery Plan, Journal of System Management, February, 1976.
11. National Bureau of Standards Building Science Series 46, Building Practices for Disaster Mitigation (February, 1973).
12. Nielson, N. R., Ruder, B., Madden, J. D. and Wong, P. J., Computer System Integrity, SRI International, Menlo Park, CA (1978).
13. Prichard, J. A. T., Contingency Planning, The National Computing Centre (U.K.), Computer Security Services (1976).
14. Report to the Congress of the United States, U.S. General Accounting Office, Most Federal Agencies Have Done Little Planning for ADP Disasters (AFMD-81-16), December 18, 1980.
15. Schabeck, T. A., Emergency Planning Guide for Data Processing Centers, Assets Protection Journal, 500 Sutter Street, Suite 503, San Francisco, CA 94102 (1979).

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)

U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards
Washington, DC 20234

OFFICIAL BUSINESS

Penalty for Private Use, $300

POSTAGE AND FEES PAID
U.S. DEPARTMENT OF COMMERCE
COM—215

FIRST CLASS