FEDERAL RESERVE BANK
OF NEW YORK

A-Cir. No. 10305

July 28, 1989

SUPERVISORY POLICY ON CONTINGENCY PLANNING FOR FINANCIAL INSTITUTIONS

To All State Member Banks, Bank Holding Companies, Edge Act Corporations, and Others Concerned, in the Second Federal Reserve District:

In view of the increasing dependence on automated systems, it is imperative that financial institutions address the inherent risks associated with the loss or extended disruption of services. Accordingly, the Federal bank regulatory agencies have issued a joint policy statement alerting directors and management of financial institutions of the need for in-house contingency planning and also for the coordination of contingency planning between financial institutions and their service bureaus where necessary. The statement also addresses various issues and responsiblities relating to the development and implementation of such plans.

Enclosed is a copy of the statement issued by the Federal Financial Institutions Examination Council in this matter. Questions may be directed to the Specialized Examinations Department of this Bank (Tel. No. 212-720-7946).

JAMES K. HODGETTS,
Chief Compliance Examiner.

Federal Financial Institutions Examination Council

1776 G Street, NW, Suite 701 • Washington, DC 20006

Interagency Policy on Contingency Planning for Financial Institutions

TO: Chief Executive Officers of all Federally Supervised Financial Institutions, Senior Management of each FFIEC Agency, and all Examining Personnel

PURPOSE:

The purpose of this policy statement is to alert the Board of Directors and management of each financial institution to the need for contingency planning for their institution. This includes both institutions that provide their own information processing and those that receive processing from service bureaus. The policy statement also addresses issues that should be considered when developing a viable contingency plan.

BACKGROUND:

Contingency planning is a process of establishing strategies to:

- o minimize disruptions of service to the institution and its customers,
- o minimize financial loss, and
- o ensure a timely resumption of operations in the event of a disaster.

These strategies are the same for institutions with in-house data centers and those using service bureaus.

In recent years information technology has expanded rapidly throughout the corporate structure of financial institutions. It includes operations such as central computer processing, distributed processing, end user computing, local area networking, and nationwide telecommunications. These operations often represent critical services to institutions and their customers. The loss or extended disruption of these business operations poses substantial risk of financial loss and could lead to the failure of an institution. As a result, contingency planning now requires an institution-wide emphasis, as opposed to focusing on centralized computer operations.

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Federal Home Loan Bank Board, National Credit Union Administration, Office of the Comptroller of the Currency

Additionally, there are many service bureaus that provide information processing services to multiple financial institutions. The disruption of the processing capabilities of one of these service bureaus could impact a considerable number of institutions. Accordingly, contingency planning by financial institution servicers is equally important.

CONCERNS:

Many financial institutions and service bureaus have not sufficiently addressed the risks associated with the loss or extended disruption of business operations. More specifically:

- Many contingency plans do not address all of the critical functions throughout the institution.
- Many serviced institutions have not established or coordinated contingency planning efforts with their service bureaus.
- Many service bureaus have not established contingency plans.
- Many contingency plans have not been adequately tested.

POLICY:

The board of directors and senior management of financial institutions are responsible for:

- Establishing policies, procedures and responsibilities for comprehensive contingency planning.
- Reviewing and approving the institution's contingency plans annually, documenting such reviews in board minutes.

If the institution receives information processing from a service bureau, management also must:

- Evaluate the adequacy of contingency plans for its service bureau.
- Ensure that the institution's contingency plan is compatible with its service bureau's plan.

The appendix to this policy provides an example of a process that management may consider in developing contingency plans. It is an outline and is not all encompassing. Each financial institution needs to assess its own risks and develop strategies accordingly. This planning process needs to address each critical system and operation, whether performed on site, at a user location, or by a service bureau.

APPENDIX

Contingency Planning Process

I. Obtain commitment from senior management to develop the plan.

II. Establish a management group to oversee development and implementation of the plan.

III. Perform a risk assessment.

Consider possible threats such as:
- o natural - fires, flood, earthquakes, . . .
- o technical - hardware/software failure, power disruption, communications interference, . . .
- o human - riots, strikes, disgruntled employee, . . .

Assess impacts from loss of information and services.
- o financial condition
- o competitive position
- o customer confidence
- o legal/regulatory requirements

Analyze costs to minimize exposures.

IV. Evaluate critical needs.
- o functional operations
- o key personnel
- o information
- o processing systems
- o documentation
- o vital records
- o policies/procedures

V. Establish priorities for recovery based on critical needs.

VI. Determine strategies to recover.
- o facilities
- o hardware
- o software
- o communications
- o data files
- o customer services
- o user operations
- o MIS
- o end-user systems
- o other processing operations

VII. Obtain written backup agreements/contracts.
- o facilities
- o hardware
- o software
- o vendors
- o suppliers
- o disaster recovery services
- o reciprocal agreements

VIII. Organize and document a written plan.

Assign responsibilities.
- o management
- o personnel
- o teams
- o vendors

Document strategies and procedures to recover.
- o procedures to execute the plan
- o priorities for critical vs. non-critical functions
- o site relocation (short-term)
- o site restoration (long-term)
- o required resources
  - human
  - financial
  - technical (hardware/software)
  - data
  - facilities
  - administrative
  - vendor support

IX. Establish criteria for testing and maintenance of plans.

Determine conditions and frequency for testing.
- o batch systems
- o on-line systems
- o communications networks
- o user operations
- o end-user systems

Evaluate results of tests.

Establish procedures to revise and maintain the plan.

Provide training for personnel involved in the plan's execution.

X. Present the contingency plan to senior management and the Board for review and approval.

Additional guidelines are available in the section 7 of the FFIEC EDP Examination Handbook. Also, many materials on contingency/disaster recovery planning have been published by trade associations, accounting firms, and the disaster recovery industry. These can be valuable guides to comprehensive contingency planning.