

PS

STATE OF TENNESSEE  
DEPARTMENT OF FINANCIAL INSTITUTIONS



# BULLETIN

NO. A-91-1

August 19, 1991

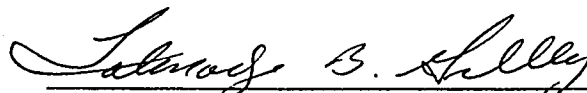
**POLICY STATEMENT BY THE COMMISSIONER  
OF FINANCIAL INSTITUTIONS**

Attached is an issuance of the Federal Financial Institutions Examination Council regarding the need for contingency planning by all financial institutions. Conformance with this policy is already required for all federally insured institutions. The Department will be utilizing the FFIEC supervisory policy on contingency planning for all state-chartered banks, credit unions, savings and loan associations and their servicers. A rule to implement these policies is currently being drafted.

Contingency planning is the process of establishing strategies to minimize disruption of services and financial loss, and to ensure timely resumption of operations in the event of a disaster. Such planning requires an institution-wide emphasis, and is equally important for financial institution servicers as well as financial institutions.

It is the responsibility of the Board of Directors to ensure that a comprehensive contingency plan has been implemented. The contingency plan will be evaluated by EDP Examiners during their review of your institution.

Thank you for your cooperation in this important part of your institutional planning. If you have any questions regarding this bulletin, please contact Ben Wooten, EDP Director, or Elizabeth Ann Clark, Staff Attorney.

  
\_\_\_\_\_  
Talmadge B. Gilley, CFE  
Commissioner

## Federal Financial Institutions Examination Council

SP-5

**Subject:** 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 service and those that receive processing from service companies. The policy statement also addresses issues that should be considered when developing a viable contingency plan.

### Background

Contingency planning is the process of identifying risks from disruption of operations and services. The objectives are to:

- minimize disruptions of service to the institution and its customers,
- minimize financial loss, and,
- 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 merely focusing on centralized computer operations.

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 servicer 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.

The appendix to this policy statement provides an example of a process that management may consider in developing contingency plans. It is a brief 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 another company.

DATE: July 1989

SP-5

## 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:

- natural — fires, flood, earthquakes, ...
- technical — hardware/software failure, power disruption, communications interference, ...
- human — riots, strikes, disgruntled employee, ...

Assess impacts from loss of information and services:

- financial condition
- competitive position,
- customer confidence
- legal/regulatory requirements.

Analyze costs to minimize exposures.

- IV. Evaluate critical needs.

- functional operations
- key personnel
- information

- processing systems
- documentation
- vital records
- policies/procedures

V. Establish priorities for recovery based on critical needs.

VI. Determine strategies to recover.

- facilities
- hardware
- software
- communications
- data files
- customer services
- user operations
- MIS
- end-user systems
- other processing operations.

VII. Obtain written backup agreements/contracts.

- facilities
- hardware
- software
- vendors
- suppliers
- disaster recovery services
- reciprocal agreements

VIII. Organize and document a written plan.

Assign responsibilities.

- management
- personnel
- teams
- vendors

Document strategies and procedures to recover.

- procedures to execute the plan
- priorities for critical vs. non-critical functions
- site relocation (short-term)
- site restoration (long-term)
- 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.

- batch systems
- on-line systems
- communications networks
- user operations
- 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.