Federal Financial Institutions Examination Council

2100 Pennsylvania Avenue, NW, Suite 200 · Washington, DC 20037 · (202) 634-6526 · FAX (202) 634-6556

CORPORATE BUSINESS RESUMPTION AND CONTINGENCY PLANNING (SP-5)

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

PURPOSE

This statement emphasizes to the board of directors and senior management of each financial institution the importance of corporate business resumption and information systems contingency planning functions. This includes planning for the recovery of critical information systems processing and operations supported by external service providers. This statement also addresses issues that management should consider when developing a viable contingency plan.

BACKGROUND

Information systems technology has evolved into a critical facet of the corporate structure of financial institutions. Transaction processing and business applications are no longer restricted to mainframe computer environments. The use of distributed platforms (including mid-range computers, client/server technology, and local and wide area networks) for rnission-critical business functions expands the scope of contingency planning.

Corporate and customer services throughout financial institutions are now more dependent on direct access to information and accounts. This includes contemporary financial delivery systems and services such as PC-banking, corporate cash management, and Internet promotion. These services represent key transactional, strategic, and reputational issues for the financial institutions. Often these services depend on a combination of internal and external information processing services. Outsourcing arrangements and other technology alliances involve unique considerations which also expand the boundaries of contingency planning.

Business recovery planners must recognize this new environment and the risks it may pose to the financial institution. The importance of these operations and service units requires effective business recovery planning from a corporate-wide perspective.

[Enc. Cir. No. 10053]

DEFINITION

Contingency planning is the process of identifying critical information systems and business functions and developing plans to enable those systems and functions to be resumed in the event of a disruption. The process includes testing the recovery plans to ensure they are effective. During the testing process management should also verify that business unit plans complement the information system plans.

GOALS

The goal of an effective contingency plan and recovery process is to facilitate and expedite the resumption of business after a disruption of vital information systems and operations. The principle objectives are to:

Minimize disruptions of service to the institution and its customers.

Ensure timely resumption of operations.

Limit losses to earnings and capital.

It is important for both financial institutions and their service bureaus to regularly assess risks associated with the loss or extended disruption of business operations and to evaluate their vulnerability to those risks. To achieve contingency planning and business resumption goals and objectives, senior management should ensure that:

Contingency plans are comprehensive and address all of the critical functions and operations in an institution. This includes assessing the response capability of key disaster recovery service vendors (e.g., the vendor(s) providing alternate processing sites; storage and transportation of back-up media between the storage vendor, alternate processing site and the institution).

An effective business resumption and contingency plan has been coordinated with their information processing and service providers.[2]

Contingency plans are thoroughly tested at least annually.

Test results and recommendations from such testing are reviewed.

Appropriate corrective actions are implemented.

---

[2] This concern refers to situations where service bureaus are contracted to process core applications or critical business lines. This is especially important to the Fedwire software application when the service provider is not affiliated with the institution through at least 80 percent common ownership. The institution must be able to continue its operations for these functional business lines if the service provider arrangement is terminated.

POLICY

The board of directors and senior management of each financial institution is responsible for:

Establishing policies and procedures, and assigning responsibilities to ensure that comprehensive corporate business resumption, contingency planning, and testing takes place.

Annually reviewing the adequacy of the institution's business recovery and contingency plans and test results.

Documenting such reviews and approvals in the board minutes.

Furthermore, if the financial institution receives information processing from a service bureau, senior management also has a responsibility to:

Evaluate the adequacy of contingency planning and testing for its service bureau.

Ensure that the institution's contingency plan is compatible with that of its service bureau.

Please refer to the *FFIEC Information Systems Examination Handbook* for specific guidance on developing an organization-wide contingency plan.

Revised: March 1997