Federal Financial Institutions Examination Council

FFIEC

Business Continuity Planning BCP

MARCH 2003

IT Examination Handbook

TABLE OF CONTENTS

INTRODUCTION

This Federal Financial Institutions Examination Council (FFIEC) *Business Continuity Planning* booklet provides guidance and examination procedures to assist examiners in evaluating financial institution and service provider risk management processes to ensure the availability of critical financial services.

Operating disruptions can occur with or without warning, and the results may be predictable or unknown. Because financial institutions play a crucial role in the United States economy, it is important their business operations are resilient and the effects of disruptions in service are minimized in order to maintain public trust and confidence in our financial system.[1] Effective business continuity planning establishes the basis for financial institutions to maintain and recover business processes when operations have been disrupted unexpectedly.

Business continuity planning is the process whereby financial institutions ensure the maintenance or recovery of operations, including services to customers, when confronted with adverse events such as natural disasters, technological failures, human error, or terrorism. The objectives of a business continuity plan (BCP) are to minimize financial loss to the institution; continue to serve customers and financial market participants; and mitigate the negative effects disruptions can have on an institution's strategic plans, reputation, operations, liquidity, credit quality, market position, and ability to remain in compliance with applicable laws and regulations. Changing business processes (internally to the institution and externally among interdependent financial services companies) and new threat scenarios require financial institutions to maintain updated and viable BCPs.

Reviewing a financial institution's BCP is an established part of examinations performed by the FFIEC member agencies.[2] However, new business practices, changes in technology, and increased terrorism concerns, have focused even greater attention on the need for effective business continuity planning and have altered the benchmarks of an effective plan. For example, an effective BCP should take into account the potential for wide-area disasters that impact an entire region and for the resulting loss or inaccessibility of staff. It also should consider and address interdependencies, both market-based and geographic, among financial system participants as well as infrastructure service providers. In most cases, recovery time objectives are now much

[1] This booklet uses the terms "institution" and "financial institution" to describe insured banks, thrifts, and credit unions, as well as technology service providers that provide services to such entities.

[2] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision.

shorter than they were even a few years ago, and for some institutions recovery time objectives are based on hours and even minutes.

Many financial institutions are incorporating business continuity considerations into business process development to mitigate proactively the risk of service disruptions. In creating an effective BCP, financial institutions should not assume a reduced demand for services during the disruption. In fact, demand for some services (e.g., ATMs) may increase.

This booklet rescinds and replaces Chapter 10 of the *1996 FFIEC Information Systems Examination Handbook, Corporate Contingency Planning.* This update is necessary due to advances since 1996 in technology, changes in business practices, and increased concerns over terrorism.

This booklet also provides an opportunity to incorporate lessons learned from Year 2000 activities. The Year 2000 activities recognized that while technology was the primary basis for concern, an enterprise-wide, process-oriented approach that considers technology, business processes, testing, and communication strategies is critical to building a viable BCP.

Each primary section of the booklet begins with an "Action Summary" that summarizes and highlights the major themes in that section. While not a substitute for reading the entire booklet, these Action Summaries may be used to more quickly assess the most important points discussed in that section.

BOARD AND SENIOR MANAGEMENT RESPONSIBILITIES

Action Summary

A financial institution's board of directors and senior management are responsible for:

- Allocating sufficient resources and knowledgeable personnel to develop the BCP;
- Setting policy by determining how the institution will manage and control identified risks;
- Reviewing BCP test results;
- Approving the BCP on an annual basis; and
- Ensuring the BCP is kept up-to-date and employees are trained and aware of their role in its implementation.

Senior management and the board of directors are responsible for identifying, assessing, prioritizing, managing, and controlling risks. They should ensure necessary resources are devoted to creating, maintaining, and testing the plan. The board fulfills its business continuity planning responsibilities by setting policy, prioritizing critical business functions, allocating sufficient resources and personnel, providing oversight, approving the BCP, reviewing test results, and ensuring maintenance of a current plan. The effectiveness of business continuity planning depends on management's commitment and ability to clearly identify what makes existing business processes work. Each financial institution must evaluate its own unique circumstances and environment to develop a comprehensive BCP.

The board and senior management should designate personnel to participate in BCP development. Properly allocating resources will challenge an institution throughout the development and maintenance of a BCP. A large, complex institution may need a business continuity planning department with a team of departmental liaisons throughout the enterprise. A smaller, less complex institution may only need an individual business continuity planning coordinator. While the planning personnel may recommend certain prioritization, ultimately the board of directors and senior management are responsible for understanding critical business processes and subsequently establishing plans to meet business process requirements in a safe and sound manner.

BUSINESS CONTINUITY PLANNING PROCESS

Action Summary

A financial institution's business continuity planning process should reflect the following objectives:

- Business continuity planning is about maintaining, resuming, and recovering the business, not just the recovery of the technology.
- The planning process should be conducted on an enterprise-wide basis.
- A thorough business impact analysis and risk assessment are the foundation of an effective BCP.
- The effectiveness of a BCP can only be validated through testing or practical application.
- The BCP and test results should be subjected to an independent audit and reviewed by the board of directors.
- A BCP should be periodically updated to reflect and respond to changes in the financial institution or its service provider(s).

Financial institutions should conduct business continuity planning on an enterprise-wide basis. In enterprise-wide business continuity planning an institution considers every critical aspect of its business in creating a plan for how it will respond to disruptions. It is not limited to the restoration of information technology systems and services, or data maintained in electronic form, since such actions, by themselves, cannot always put an institution back in business. Without a BCP that considers every critical business unit, including personnel, physical workspace, and similar issues, an institution may not be able to resume serving its customers at acceptable levels. Institutions that outsource the majority of their data processing, core processing, or other information technology systems or services are still expected to implement an appropriate BCP addressing the equipment and processes that remain under their control.

Financial institutions should also recognize their role in supporting systemic financial market business processes (e.g., inter-bank payment systems, and key market clearance and settlement activities) and that service disruptions at their institution may significantly affect the integrity of key financial markets. The FFIEC agencies encourage all institutions to work with affected interdependent parties to coordinate BCP development and testing. The FFIEC agencies expect financial institutions that play a major role in critical financial markets to have robust planning and coordinated testing with other industry participants. Critical markets include, but may not be limited to, the markets for

federal funds; foreign exchange; commercial paper; and government, corporate, and mortgage-backed securities.

Firms that play significant roles in critical financial markets are those that participate in sufficient volume or value such that their failure to perform critical activities by the end of the business day could present systemic risk. The agencies believe that many, if not most, of the 15-20 major banks and the 5-10 major securities firms, and possibly others, play at least one significant role in at least one critical market. In the context of sound practices, some of the agencies are considering the benefit of providing additional guidance to help firms identify the category into which they fall for the specific activities they perform.

Financial institutions not directly participating in critical financial markets, but nonetheless performing financial services or supporting financial market activities deemed critical to regional or national financial sectors, are also expected to establish BCPs and recovery capabilities commensurate with their role. Smaller, less complex institutions generally do not need the same level of planning, but are expected to fulfill their responsibility by developing an appropriate BCP and periodically conducting adequate tests.

Management should update BCPs as business processes change. For example, financial institutions of all sizes are increasingly relying on distributed network solutions to support business processes. This increased reliance can include desktop computers maintaining key applications. While distributed networking provides flexibility in allowing institutions to deliver operations to where employees and customers are located, it also means that end-users should keep BCP personnel up-to-date on what constitutes current business processes and significant changes. Technological advancements are allowing faster and more efficient processing, thereby reducing acceptable business process recovery periods. In response to competitive and customer demands, many financial institutions are moving toward shorter recovery periods and designing technology recovery solutions into business processes. These technological advancements increase the importance of enterprise-wide business continuity planning.

The FFIEC agencies encourage financial institutions to adopt a process-oriented approach to business continuity planning that involves:

1. Business impact analysis (BIA);
2. Risk assessment;
3. Risk management; and
4. Risk monitoring.

This framework is usable regardless of the size of the institution. Business continuity planning should focus on all critical business functions that need to be recovered to

resume operations. Continuity planning for technology alone should no longer be the primary focus of a BCP, but rather viewed as one critical aspect of the enterprise-wide process. The review of each critical business function should include the technology that supports it.[3]

BUSINESS IMPACT ANALYSIS

Action Summary

A business impact analysis (BIA) is the first step in developing a BCP. It should include:

- Identification of the potential impact of uncontrolled, non-specific events on the institution's business processes and its customers;
- Consideration of all departments and business functions, not just data processing; and
- Estimation of maximum allowable downtime and acceptable levels of data, operations, and financial losses.

The institution's first step in developing a BCP is to perform a BIA. The amount of time and resources necessary to complete the BIA will depend on the size and complexity of the financial institution. The institution should include all business functions and departments in this process, not just data processing.

The BIA phase identifies the potential impact of uncontrolled, non-specific events on the institution's business processes. The BIA phase also should determine what and how much is at risk by identifying critical business functions and prioritizing them. It should estimate the maximum allowable downtime for critical business processes, recovery point objectives and backlogged transactions, and the costs associated with downtime. Management should establish recovery priorities for business processes that identify essential personnel, technologies, facilities, communications systems, vital records, and data. The BIA also considers the impact of legal and regulatory requirements such as the privacy and availability of customer data and required notifications to the institution's primary federal regulator and customers when facilities are relocated.[4]

---

[3] See *Guidelines for Establishing Standards for Safeguarding Customer Information*, 66 FR 8616 (February 1, 2001). The risk assessment required by the interagency guidelines may be helpful in performing the BCP risk assessment. Board of Governors of the Federal Reserve System, 12 CFR parts 208, 211, 225, and 263; Federal Deposit Insurance Corporation, 12 CFR parts 308 and 364; National Credit Union Administration, 12 CFR part 748; Office of the Comptroller of the Currency, 12 CFR part 30; Office of Thrift Supervision, 12 CFR parts 568 and 570.

[4] See *Policy Statement of the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of Thrift Supervision Concerning Branch*

Personnel responsible for this phase should consider developing uniform interview and inventory questions that can be used on an enterprise-wide basis. Uniformity can improve the consistency of responses and help personnel involved in the BIA phase compare and evaluate business process requirements. This phase may initially prioritize business processes based on their importance to the institution's achievement of strategic goals and maintenance of safe and sound practices. However, this prioritization should be revisited once the business processes are modeled against various threat scenarios so that a BCP can be developed.

When determining a financial institution's critical needs, reviews should be conducted for all functions, processes, and personnel within each department. Each department should document the mission critical functions performed. Departments should consider the following questions:

- What specialized equipment is required and how it is used?
- How would the department function if mainframe, network and/or Internet access were not available?
- What single points of failure exist and how significant are those risks?
- What are the critical outsourced relationships and dependencies?
- What is the minimum number of staff and space that would be required at a recovery site?
- What special forms or supplies would be needed at a recovery site?
- What communication devices would be needed at a recovery site?
- What critical operational or security controls require implementation prior to recovery?
- Is there any potential impact from common recovery sites serving multiple lines of business or departments?
- Have employees received cross training and has the department defined back-up functions/roles employees should perform if key personnel are not available?
- Are emotional support and family care needs adequately considered?

Closing Notices and Policies, 64 FR 34844 (June 30, 1999); *Establishment and Relocation of Domestic Branches and Offices*, Board of Governors of the Federal Reserve System, 12 CFR part208.6; Federal Deposit Insurance Corporation, 12 CFR part 303.44; Office of the Comptroller of the Currency, 12 CFR part5.30; and Office of Thrift Supervision, 12 CFR part545.95.

RISK ASSESSMENT

Action Summary

The risk assessment is the second step in developing a BCP. It should include:

- A prioritizing of potential business disruptions based upon severity and likelihood of occurrence;
- A gap analysis comparing the institution's existing BCP, if any, to what is necessary to achieve recovery time and point objectives; and
- An analysis of threats based upon the impact on the institution, its customers, and the financial markets, not just the nature of the threat.

The risk assessment step is critical and has significant bearing on whether business continuity planning efforts will be successful. If the threat scenarios developed are unreasonably limited, the resulting BCP may be inadequate. During the risk assessment step, business processes and the business impact analysis assumptions are stress tested with various threat scenarios. This will result in a range of outcomes, some that require no action for business processes to be successful and others that will require significant BCPs to be developed and supported with resources (financial and personnel).

Financial institutions should develop realistic threat scenarios that may potentially disrupt their business processes and ability to meet their client's expectations (internal, business partners, or customers).[5] Threats can take many forms, including malicious activity as well as natural and technical disasters. Where possible, institutions should analyze a threat by focusing on its impact on the institution, not the nature of the threat. For example, the effects of certain threat scenarios can be reduced to business disruptions that affect only specific work areas, systems, facilities (i.e., buildings), or geographic areas. Additionally, the magnitude of the business disruption should consider a wide variety of threat scenarios based upon practical experiences and potential circumstances and events. If the threat scenarios are not comprehensive, BCPs may be too basic and omit reasonable steps that could improve business processes' resiliency to disruptions.

Threat scenarios need to consider the impact of a disruption and probability of the threat occurring. Threats range from those with a high probability of occurrence and low impact to the institution (e.g., brief power interruptions), to those with a low probability

[5] A summary of threats and basic safeguards is contained in Appendix C.

of occurrence and high impact on the institution (e.g., hurricane, terrorism). High probability threats are often supported by very specific BCPs. However, the most difficult threats to address are those that have a high impact on the institution but a low probability of occurrence. Using a risk assessment, BCPs may be more flexible and adaptable to specific types of disruptions that may not be initially considered.

It is at this point in the business continuity planning process that financial institutions should perform a "gap analysis." In this context, a gap analysis is a methodical comparison of what types of plans the institution (or business line) needs to maintain, resume, or recover normal business operations in the event of a disruption, versus what the existing BCP provides. The difference between the two highlights additional risk exposure that management and the board need to address in BCP development.

The risk assessment considers:

- The impact of various business disruption scenarios on both the institution and its customers;
- The probability of occurrence based, for example, on a rating system of high, medium, and low;
- The loss impact on information services, technology, personnel, facilities, and service providers from both internal and external sources;
- The safety of critical processing documents and vital records; and
- A broad range of possible business disruptions, including natural, technical, and human threats.

When assessing the probability of a specific event occurring, financial institutions and technology service providers should consider the geographic location of facilities and their susceptibility to natural threats (e.g., location in a flood plain), and the proximity to critical infrastructures (e.g., power sources, nuclear power plants, airports, points of interest, major highways, railroads).

The risk assessment should include all the financial institution or service provider's locations and facilities. Worst-case scenarios, such as destruction of the facilities and loss of life, should be considered. At the conclusion of this phase, the institution will have prioritized business processes and estimated how they may be disrupted under various threat scenarios.

RISK MANAGEMENT

BUSINESS CONTINUITY PLAN DEVELOPMENT

Action Summary

Risk management is the development of a written, enterprise-wide BCP. The institution should ensure that the BCP is:

- Written and disseminated so that various groups of personnel can implement it in a timely manner;
- Specific regarding what conditions should prompt implementation of the plan;
- Specific regarding what immediate steps should be taken during a disruption;
- Flexible to respond to unanticipated threat scenarios and changing internal conditions;
- Focused on how to get the business up and running in the event that a specific facility or function is disrupted, rather than on the precise nature of the disruption; and
- Effective in minimizing service disruptions and financial loss.

After conducting the BIA and risk assessment, management should prepare a written BCP. The plan should document strategies and procedures to maintain, resume, and recover critical business functions and processes and should include procedures to execute the plan's priorities for critical vs. non-critical functions, services and processes. A well-written BCP should describe in some detail the types of events that would lead up to the formal declaration of a disruption and the process for invoking the BCP. It should describe the responsibilities and procedures to be followed by each continuity team and contain contact lists of critical personnel. The BCP should describe in detail the procedures to be followed to recover each business function affected by the disruption and should be written in such a way that various groups of personnel can implement it in a timely manner.

As previously discussed, a BCP is more than recovery of the technology, but rather a recovery of all critical business operations. The plan should be flexible to respond to changing internal and external conditions and new threat scenarios. Rather than being developed around specific events (e.g. fire vs. tornado), the plan will be more effective if it is written to adequately address specific types of scenarios and the desired outcomes. A BCP should describe the immediate steps to be taken during an event in order to minimize the damage from a disruption, as well as the action necessary to recover. Thus, business continuity planning should be focused on maintaining, resuming, and recovering

the institution's operations after a disruption. Specific scenarios should include how the financial institution would respond if:

- Critical personnel are not available;
- Critical buildings, facilities, or geographic regions are not accessible;
- Equipment malfunctions (hardware, telecommunications, operational equipment);
- Software and data are not accessible or are corrupted;
- Vendor assistance or service provider is not available;
- Utilities are not available (power, telecommunications); and
- Critical documentation and/or records are not available.

Financial institutions should carefully consider the assumptions on which the BCP is based. Institutions should not assume a disaster will be limited to a single facility or a small geographic area. Institutions should not assume they will be able to gain access to facilities that have not been damaged or that critical personnel (including senior management) will be available immediately after the disruption. Assuming public transportation systems such as airlines, railroads and subways will be operating may also be incorrect. Financial institutions should not assume the telecommunications system will be operating at normal capacity.

A BCP consists of many components that are both internal and external to a financial institution. The activation of a continuity plan and restoration of business in the event of an emergency is dependent on the successful interaction of various components. The overall strength and effectiveness of a BCP can be decreased by its weakest component. An effective business continuity plan coordinates across its many components, identifies potential process or system dependencies, and mitigates the risks from interdependencies.[6]

Typically, the business continuity coordinator or team facilitates the identification of risk and the development of risk mitigation strategies across business areas. Internal causes of interdependencies can include line of business dependencies, telecommunication links, and/or shared resources (i.e., print operations or e-mail systems). External sources of interdependencies that can negatively impact a business continuity plan can include telecommunication providers, service providers, customers, business partners and suppliers.[7]

[6] A more comprehensive discussion of interdependencies is contained in Appendix D.

[7] A more complete discussion of business continuity plan components is contained in Appendix E.

OTHER POLICIES, STANDARDS AND PROCESSES

Action Summary

Other financial institution policies, in addition to the BCP, should incorporate business continuity planning considerations. These include:

- System Development Life Cycles;
- Change control policies;
- Data synchronization procedures;
- Employee training and communication plans;
- Insurance policies;
- Government, media, and community relations policies; and
- Security.

In addition to documenting BCPs, other policies, standards and practices should address continuity and availability considerations. These include Systems Development Life Cycle ("SDLC"), change control, and data synchronization.

SYSTEMS DEVELOPMENT LIFE CYCLE AND PROJECT MANAGEMENT

As part of the SDLC process, management should incorporate business continuity considerations into project plans. Evaluating business continuity needs during the SDLC process allows for advance preparation when an institution is acquiring or developing a new system. Evaluating business continuity requirements during the SDLC stages facilitates the development of a more robust system that will permit easier continuation of business in the event of a disruption.

During the development and acquisition of new systems, SDLC standards and project plans should address, at a minimum, issues such as:

- Business unit requirements for resumption and recovery alternatives;
- Information on back-up and storage;
- Hardware and software requirements at recovery locations;
- BCP and documentation maintenance;
- Disaster recovery testing; and
- Staffing and facilities.

CHANGE CONTROL

Change management and control policies and procedures should appropriately address changes to the operating environment. Just as all program changes should be fully authorized and documented, business continuity considerations should be included in the change control process and implementation phase. Whenever a change is made to an application, operating system, or utility that resides in the production environment, a methodology should exist to ensure all back-up copies of those systems are updated to reflect the new environment. In addition, if a new or changed system is implemented and results in new hardware, capacity requirements, or other technology changes, management should ensure the BCP is updated and the recovery site can support the new production environment.

DATA SYNCHRONIZATION

Data synchronization can become a challenge when dealing with an active/back-up environment. The larger and more complex an institution is (i.e., shorter acceptable operational outage period, greater volume of data, greater distance between primary and back-up location), the more difficult synchronization can become. If back-up copies are produced as of the close of a business day and a disruption occurs relatively late the next business day, all the transactions that took place after the back-up copies were made would have to be recreated, perhaps manually, in order to synchronize the recovery site with the primary site.

Management and testing of contingency arrangements are critical to ensure the recovery environment is synchronized with the primary work environment. This testing includes ensuring software versions are current, interfaces exist and are tested, and communication equipment is compatible. If the two locations, underlying systems, and interdependent business units are not synchronized, there is the likely possibility that recovery at the back-up location could encounter significant problems. Proper change control, information back up, and adequate testing can help avoid this situation. In addition, management should ensure the back-up facility has adequate capacity to process transactions in a timely manner in the event of a disruption at the primary location.

EMPLOYEE TRAINING AND COMMUNICATION PLANNING

Financial institutions should provide business continuity training for personnel to ensure all parties are aware of their responsibilities should a disaster occur. Key employees should be involved in the business continuity development process, as well as periodic training exercises. The training program should incorporate enterprise-wide training as well as specific training for individual business units. Employees should be aware of which conditions call for implementing all or parts of the BCP, who is responsible for implementing BCPs for business units and the institution, and what to do if these key employees are not available at the time of a disaster. Cross training should be utilized to

anticipate restoring operations in the absence of key employees. Employee training should be regularly scheduled and updated to address changes to the BCP.

Communication planning should identify alternate communication channels to utilize during a disaster, such as pagers, cell phones, e-mail, or two-way radios. An emergency telephone number, e-mail address, and physical address list should be provided to employees to assist in communication efforts during a disaster. The list should provide all alternate numbers since one or more telecommunications systems could be unavailable. Additionally, the phone list should provide numbers for vendors, emergency services, transportation, and regulatory agencies. Wallet cards, Internet postings, and calling trees are possible ways to distribute information to employees. Further, institutions should establish reporting or calling locations to assist them in accounting for all personnel following a disaster.

Financial institutions should consider developing an awareness program to let customers, service providers, and regulators know how to contact the institution if normal communication channels are not in operation. The plan should also designate personnel who will communicate with the media, government, vendors, and other companies and provide for the type of information to be communicated.

INSURANCE

Insurance is commonly used to recoup losses from risks that cannot be completely prevented. Generally, insurance coverage is obtained for risks that cannot be entirely controlled, yet could represent a significant potential for financial loss or other disastrous consequences. The decision to obtain insurance should be based on the probability and degree of loss identified during the BIA. Financial institutions should determine potential exposure for various types of disasters and review the insurance options available to ensure appropriate insurance coverage is provided. Management should know the limits and coverage detailed in insurance policies to make sure coverage is appropriate given the risk profile of the institution. Institutions should perform an annual insurance review to ensure the level and types of coverage are commercially reasonable, and consistent with any legal, management, and board requirements. Also, institutions should create and retain a comprehensive hardware and software inventory list in a secure off-site location in order to facilitate the claims process.

Financial institutions should be aware of the limitations of insurance. Insurance can reimburse an institution for some or all of the financial losses incurred as the result of a disaster or other significant event. However, insurance is by no means a substitute for an effective BCP, since its primary objective is not the recovery of the business. For example, insurance cannot reimburse an institution for damage to its reputation.

.

GOVERNMENT AND COMMUNITY

An institution may need to coordinate with community and government officials and the news media to ensure the successful implementation of the BCP. Ideally, these relationships should be established during the planning or testing phases of business continuity planning. This establishes proper protocol in case a city-wide or region-wide event impacts the institution's operations. Financial institutions are encouraged to contact state and local authorities during the risk assessment process to inquire about specific risks or exposures for all their geographic locations and special requirements for accessing emergency zones. During the recovery phase, facilities access, power, and telecommunications systems would be coordinated with various entities to ensure timely resumption of operations. Facilities access should be coordinated with the police and fire department and, depending on the nature and extent of the disaster, possibly the Federal Emergency Management Agency (FEMA).

RISK MONITORING

Action Summary

Risk monitoring is the final step in business continuity planning. It should ensure that the institution's BCP is viable through:

- Testing the BCP at least annually;
- Subjecting the BCP to independent audit and review; and
- Updating the BCP based upon changes to personnel and the internal and external environments.

Risk monitoring ensures a BCP is viable through testing, independent review, and periodic updating.

OVERALL TESTING STRATEGY

The development of testing strategies requires a business decision regarding the level and frequency of testing needed to ensure recovery objectives can be achieved during a business interruption or disaster. The frequency and complexity of testing is based on the risks to the institution. Even small, serviced institutions should participate in tests with their core service providers and test other critical components of the BCP. Unmanned recovery testing, where back-up tapes are sent to the recovery site to be run by service provider employees, is not a sufficient test of an institution's BCP. Additional testing of other aspects of the BCP should be performed to the extent feasible.

Testing strategies should detail the conditions and frequency for testing applications and business functions, including the supporting information processing. The strategy should

include test objectives, scripts, and schedules, as well as provide for review and reporting of test results. Management should ensure recovery testing is conducted at least annually, or more frequently, depending on the operating environment and criticality of the applications and business functions.

Management should evaluate the risks and merits of various types of testing and develop strategies based on identified resumption and recovery needs. The business continuity planning process should evaluate whether the institution is anticipating operating at full or reduced capacity. Financial institutions should not assume a reduced demand for services during a disruption. In fact, demand for some services (e.g., ATMs) may increase. If the plan is to operate at a reduced capacity at an alternate site, risks should be evaluated for exceeding that capacity and priorities established as to what will or will not be processed.

The process should also evaluate the necessity for enterprise-wide, service provider, and key market participants testing, rather than relying solely on isolated business unit testing. Comprehensive testing requires evaluating interdependencies between critical business functions and systems, and evaluating the criticality of testing those systems in tandem. Management should test its ability to recover current data from back-up media. Institutions should include security measures and procedures within the scope of the test, including ensuring secure copies of the back-up media remain available in the event of an actual problem during testing.

TESTING SCOPE AND OBJECTIVES

Management should clearly define what functions, systems, or processes are going to be tested and what will constitute a successful test. The objective of a testing program is to ensure that the BCP remains accurate, relevant, and operable under adverse conditions. Testing should include applications and business functions that were identified during the impact analysis. The business impact analysis determines the recovery point objectives and recovery time objectives, which then help determine the appropriate recovery strategy.

Testing objectives should start small, and gradually increase in complexity and scope. The scope of individual tests can be continually expanded to eventually encompass enterprise-wide testing, including vendors and key market participants. Achieving the following objectives provides progressive levels of assurance and confidence in the plan. At a minimum, a clearly stated testing plan should:

- Not jeopardize normal business operations;
- Gradually increase the complexity, level of participation, functions, and physical locations involved;

- Demonstrate a variety of management and response proficiencies, under simulated crisis conditions, progressively involving more resources and participants;
- Uncover inadequacies, so that configurations and procedures can be corrected; and
- Consider deviating from the test script to interject unplanned events, such as the loss of key individuals or services.

SPECIFIC TEST PLANS

Management should develop a test plan for each BCP testing method used. The test plan should identify quantifiable measurements of each test objective. The test plan should be reviewed prior to the test to ensure it can be implemented as designed without endangering the production environment.

TEST PLAN REVIEW

Management should prepare and review a script for each test prior to testing to identify weaknesses that could lead to unsatisfactory or invalid tests. As part of the review process, the testing plan should be revised to account for any changes to key personnel, policies, procedures, facilities, equipment, outsourcing relationships, vendors, or other components that impact a critical business function.

VALIDATION OF ASSUMPTIONS

The testing plan's assumptions should be validated to ensure they are appropriate for business continuity requirements. This validation requires the participation of appropriate business, operations, and technology staff. Plan assumptions requiring validation include:

- Criticality of services;
- Volume of transactions;
- Interrelationships among business functions;
- Selecting the business continuity planning strategy related to use of facilities and other outages; and
- Availability and adequacy of resources required to provide the planned service level, such as the time required to establish facilities, obtain back-up files, or reconstruct documents.

ACCURACY OF INFORMATION

All documented data and lists in the BCP should be checked periodically for accuracy, including furniture, equipment, telecommunications connections, applications, and operating systems at both the primary and alternate sites. Version numbers of applications and operating systems should be specified on this list.

COMPLETENESS OF PROCEDURES

The test procedures should be checked periodically to make sure they include:

- Emergency response procedures, including escalation and notification processes;
- Alternate processing procedures, including security procedures at an alternate site; and
- Full recovery procedures, including returning to normal processing.

TESTING METHODS

Testing methods vary from minimum preparation and resources to the most complex. Each bears its own characteristics, objectives, and benefits. The type of testing employed by a financial institution should be determined by, among other things, its age and experience with business continuity planning, size, complexity, and nature of its business. Examples of testing methods in order of increasing complexity include:

Orientation/Walk-through

An orientation/walk-through is the most basic type of test. Its primary objective is to ensure that critical personnel from all areas are familiar with the BCP. It is characterized by:

- Discussion about the BCP in a conference room or small group setting;
- Individual and team training; and
- Clarification and highlighting of critical plan elements.

Tabletop/Mini-drill

A tabletop/mini-drill is somewhat more involved than an orientation/walk-through because the participants choose a specific event scenario and apply the BCP to it. It includes:

- Practice and validation of specific functional response capability;

- Focus on demonstration of knowledge and skills, as well as team interaction and decision-making capability;
- Role playing with simulated response at alternate locations/facilities to act out critical steps, recognize difficulties, and resolve problems in a non-threatening environment;
- Mobilization of all or some of the crisis management/response team to practice proper coordination; and
- Varying degrees of actual, as opposed to simulated, notification and resource mobilization to reinforce the content and logic of the plan.

Functional Testing

Functional testing is the first type that involves the actual mobilization of personnel at other sites in an attempt to establish communications and coordination as set forth in the BCP. It includes:

- Demonstration of emergency management capabilities of several groups practicing a series of interactive functions, such as direction, control, assessment, operations, and planning;
- Actual or simulated response to alternate locations or facilities using actual communications capabilities;
- Mobilization of personnel and resources at varied geographical sites; and
- Varying degrees of actual, as opposed to simulated, notification and resource mobilization.

Full-scale Testing

Full-scale testing is the most comprehensive type of test. In a full-scale test, the institution implements all or portions of its BCP by processing data and transactions using back-up media at the recovery site. It involves:

- Validation of crisis response functions;
- Demonstration of knowledge and skills, as well as management response and decision-making capability;
- On-the-scene execution of coordination and decision-making roles;
- Actual, as opposed to simulated, notifications, mobilization of resources, and communication of decisions;
- Activities conducted at actual response locations or facilities;

- Enterprise-wide participation and interaction of internal and external management response teams with full involvement of external organizations;
- Actual processing of data utilizing back-up media; and
- Exercises generally extending over a longer period of time to allow issues to fully evolve as they would in a crisis, and allow realistic role- play of all the involved groups.

CONDUCTING A TEST

Testing requires some centralized coordination, usually by the BCP coordinator or team. The team or coordinator is responsible for overseeing the accomplishment of targeted objectives and following up with the appropriate areas on the results of the test.

Generally, it is advisable to have the maximum number of personnel that will be involved in implementing the BCP also participate in the test. This participation increases awareness, buy-in, and ownership in achieving successful BCP implementation. It is also advisable to rotate personnel involved in testing in order to prepare for the loss of key individuals, both during a disaster and as a result of retirements, promotions, terminations, resignations, or re-assignment of responsibilities. The involvement and oversight of independent staff such as auditors will help to ensure the validity of the testing process and the accuracy of the reporting.

ANALYZING AND REPORTING TEST RESULTS

A useful test can only be achieved if the test results are analyzed and compared against stated objectives, and acted upon.

Management should report the test results and the resolution of any problems to the board. Management reports should consider all the test results. Test analyses should include:

- An assessment of whether the test objectives were completed;
- An assessment of the validity of test data processed;
- Corrective action plans to address problems encountered;
- A description of any gaps between the BCP and actual test results;
- Proposed modifications to the BCP; and
- Recommendations for future tests.

UPDATING A BUSINESS CONTINUITY PLAN

A BCP is a "living" document; changing in concert with changes in the business activities it supports. The plan should be reviewed by senior management, the planning team or coordinator, team members, internal audit, and the board of directors at least annually. As part of that review process, the team, or coordinator should contact business unit managers throughout the financial institution at regular intervals to assess the nature and scope of any changes to the institution's business, structure, systems, software, hardware, personnel, or facilities. It is to be expected that some changes will have occurred since the last plan update. Software applications are commercially available to assist the BCP coordinator in identifying and tracking these organizational changes so that the BCP can be updated.

All such organizational changes should be analyzed to determine how they may affect the existing continuity plan, and what revisions to the plan may be necessary to accommodate these changes. The agencies expect that BCP updates will be documented to show that the plan reflects the institution, as it currently exists. Lastly, the financial institution should ensure the revised BCP is distributed throughout the organization.

AUDIT AND INDEPENDENT REVIEWS

The audit department or other qualified, independent party should review the adequacy of the business continuity process to ensure the board's expectations are met. This review should include assessing the adequacy of business process identification, threat scenario development, business impact analysis and risk assessments, the written plan, testing scenarios and schedules, and communication of test results and recommendations to the board. In order to discharge these responsibilities, the audit department or other independent party should directly observe tests of the BCP. The board should receive and carefully review audit reports on the effectiveness of the institution's process that identify any areas of weakness.

SUMMARY

In summation, the following six factors are the critical aspects of effective business continuity planning:

- Business continuity planning should be conducted on an enterprise-wide basis.
- A thorough business impact analysis and risk assessment are the foundation of an effective BCP.
- Business continuity planning is more than the recovery of the technology; it is the recovery of the business.
- The effectiveness of a BCP can only be validated through thorough testing.
- The BCP and test results should be subjected to independent audit.
- A BCP should be periodically updated to reflect and respond to changes in the institution.

APPENDIX A: EXAMINATION PROCEDURES

EXAMINATION OBJECTIVE: Determine the quality and effectiveness of the organization's business continuity planning process. These procedures will disclose the adequacy of the planning process for the organization to maintain, resume, and recover operations after disruptions ranging from minor outages to full-scale disasters. This workprogram can be used to assess the adequacy of the business continuity planning process on an enterprise-wide basis or across a particular line of business. Depending on the examination objectives, a line of business can be selected to sample how the organization's continuity planning process works on a micro level or for a particular business function or process.

This workprogram is intended to be comprehensive and assist examiners in determining the effectiveness of a financial institution's business continuity planning process. However, examiners may choose to use only particular components of the workprogram based upon the size, complexity, and nature of the institution's business.

Objective 1: Determine examination scope and objectives for reviewing the business continuity planning program.

1. Review past reports for outstanding issues or previous problems. Consider

   - Regulatory reports of examination;
   - Internal and external audit reports, including SAS 70 reports;
   - Business continuity test results; and
   - Organization's overall risk assessment and profile.

2. Review management's response to issues raised since the last examination. Consider

   - Adequacy and timing of corrective action;
   - Resolution of root causes rather than just specific issues; and
   - Existence of any outstanding issues.

3. Interview management and review the business continuity request information to identify:

- Any significant changes in business strategy or activities that could affect the business recovery process;
- Any material changes in the audit program, scope, or schedule related to business continuity activities;
- Changes to internal business processes;
- Key management changes;
- Information technology environments and changes to configuration or components;
- Changes in key service providers (technology, communication, back-up/recovery, etc.) and software vendor listings; and
- Any other internal or external factors that could affect the business continuity process.

4. Determine management's consideration of newly identified threats and vulnerabilities to the organization's business continuity process. Consider
   - Technological and security vulnerabilities;
   - Internally identified threats; and
   - Externally identified threats (including known threats published by information sharing organizations).
5. Establish the scope of the examination by focusing on those factors that present the greatest degree of risk to the institution or service provider.

Objective 2: Determine the existence of an appropriate enterprise-wide business continuity plan (BCP).

1. Review the written BCP(s) and verify that the BCP(s):
   - Address(es) the recovery of each business unit/department/function:
     - According to its priority ranking in the Risk Assessment; and
     - Considering interdependencies among systems.
   - Take(s) into account:
     - Personnel;

- Facilities;
- Technology (hardware, software, operational equipment);
- Telecommunications/networks;
- Vendors;
- Utilities;
- Documentation (data and records);
- Law enforcement;
- Security;
- Media; and
- Shareholders.

- Include(s) emergency preparedness and crisis management aspects:
  - Has an accurate employee/manager contact tree;
  - Clearly defines responsibilities and decision-making authorities for designated teams and/or staff members, including those who have authority to declare a disaster;
  - Explains actions to be taken in specific emergency situations;
  - Defines the conditions under which the back-up site would be used;
  - Has procedures in place for notifying the back-up site;
  - Designates a public relations spokesperson; and
  - Identifies sources of needed office space and equipment and list of key vendors (hardware/software/communications, etc.).

2. Determine if adequate procedures are in place to ensure the BCP(s) is (are) maintained in a current fashion and updated regularly.

Objective 3: Determine the quality of BCP oversight and support provided by the board of directors and senior management.

1. Determine if the board has established an enterprise-wide business continuity planning process appropriate for the size and complexity of the organization which defines the organization's business continuity strategy.

2. Determine if a senior manager has been assigned responsibility to oversee the development, implementation, testing, and maintenance of the BCP.

3. Determine if the board has ensured that adequate resources, including sufficient human resources, are devoted to the business continuity process.

4. Determine if the board reviews and approves the written BCP(s) and testing results at least annually and documents these reviews in the board minutes.

5. Determine if senior management periodically reviews and prioritizes each business unit, business process, department, and subsidiary for its critical importance and recovery prioritization. If so, determine how often reviews are conducted.

6. If applicable, determine if senior management has evaluated the adequacy of the BCPs for its service providers, and ensured the organization's BCP is compatible with those service provider plans, commensurate with adequate recovery priorities.

Objective 4: Determine if an adequate business impact analysis (BIA) and risk assessment have been completed.

1. Determine if all functions and departments were included in the BIA.

2. Review the BIA to determine if the identification and prioritization of business functions are adequate.

3. Determine if the BIA identifies maximum allowable downtime for critical business functions, acceptable levels of data loss and backlogged transactions, and the cost and recovery time objectives associated with downtime.

4. Review the risk assessment and determine if it includes scenarios and probability of occurrence of disruptions of information services, technology, personnel, facilities, and service providers from internal and external sources, including:

   - Natural events such as fires, floods, and severe weather;

   - Technical events such as communication failure, power outages, and equipment and software failure; and

   - Malicious activity including network security attacks, fraud, and terrorism.

5. Ensure the risk assessment and BIA have been reviewed and approved by senior management and the board.

6. Ensure reputation, operational, compliance, and other risks are considered in plan(s).

Objective 5: Determine if appropriate risk management over the business continuity process is in place.

1. Determine if adequate risk mitigation strategies have been considered for:

   - Alternate locations and capacity for:
     - Data centers and computer operations;
     - Back-room operations;
     - Work locations for business functions; and
     - Telecommunications.
   - Back-up of:
     - Data;
     - Operating systems;
     - Applications;
     - Utility programs; and
     - Telecommunications.
   - Off-site storage of:
     - Back-up media;
     - Supplies; and
     - Documentation, e.g., BCP(s), operating and other procedures, inventory listings, etc.
   - Alternate power supplies:
     - Uninterruptible power supplies (UPS); and
     - Back-up generators.

2. Determine if satisfactory consideration has been given to geographic diversity for:

   - Alternate processing locations;
   - Alternate locations for business processes and functions; and

- Off-site storage.

3. Ensure appropriate policies, standards, and processes address business continuity planning issues including:

   - Systems Development Life Cycle, including project management;
   - The change control process;
   - Data synchronization, back up, and recovery;
   - Employee training and communication planning;
   - Insurance; and
   - Government and community coordination.

4. Determine if personnel are adequately trained as to their specific responsibilities under the plan(s) and whether emergency procedures are posted in prominent locations throughout the facility.

5. Determine if the continuity strategy includes alternatives for interdependent components and stakeholders, including:

   - Utilities;
   - Telecommunications;
   - Third-party technology providers;
   - Key suppliers/business partners; and
   - Customers/members.

6. Determine if there are adequate processes in place to ensure the plan(s) are maintained to remain accurate and current.

   - Designated personnel are responsible for maintaining changes in processes, personnel, and environment(s).
   - The board of directors reviews and approves the plan(s) annually and after significant changes and updates.
   - Process includes notification and distribution of revised plans to personnel and recovery locations.

7. Determine if audit involvement in the business continuity program is effective, including:

   - Audit coverage of the business continuity program;
   - Assessment of business continuity preparedness during line(s) of business reviews;
   - Audit participation in testing in an observer role; and
   - Audit review of testing plans and results.

Objective 6: Determine whether the BCP(s) include(s) appropriate testing to ensure the business process(es) will be maintained, resumed, and/or recovered as intended.

1. Determine if the BCP(s) is tested at least annually.

2. Verify that all critical business units/departments/functions are included in the testing.

3. Verify that tests include:

   - Setting goals and objectives in advance;
   - Realistic conditions and activity volumes;
   - Use of actual back-up system and data files while maintaining off-site back-up copies for use in case of an event concurrent with the testing;
   - Participation and review by internal audit;
   - A post-test analysis report and review process that includes a comparison of test results to the original goals;
   - Development of a corrective action plan(s) for all problems encountered; and
   - Board of directors review.

4. Determine if interdependent departments, vendors, and key market providers have been involved in testing at the same time to uncover potential conflicts and/or inconsistencies.

5. Determine if the level of testing is adequate for the size and complexity of the organization. Determine if the testing includes:

- Testing the operating systems and utilities (infrastructure);
- Testing of all critical applications (application level);
- Data transfer between applications (integrated testing); and
- Testing the complete environment and workload (stress test).

6. Determine whether testing at an alternative location includes:

   - Network connectivity;
   - Items processing and backroom operations connectivity and information; and
   - Other critical data feed connections/interfaces.

7. Determine whether testing of the information technology infrastructure includes:

   - Rotation of personnel involved; and
   - Business unit personnel involvement.

8. Determine whether management considered testing with:

   - Critical service providers;
   - Customers;
   - Affiliates;
   - Correspondent institutions; and
   - Payment systems and major financial market participants.

Objective 7: Determine if the information technology environment has a properly documented BCP that complements the enterprise-wide and other departmental BCPs.

1. Verify that the IT BCP properly supports and reflects the goals and priorities found in the business unit BCP(s).

2. Determine if all critical resources and technologies are covered by the BCP(s), including voice and data communication networks, customer delivery channels, etc.

3. Determine if the BCPs include the entire network and communication connections.

4. Determine if the BCP establishes processing priorities to be followed in the event not all applications can be processed.

Objective 8: Determine whether the BCP(s) include(s) appropriate hardware backup and recovery.

1. Describe the arrangements for alternative processing capability in the event any specific hardware, the data center, or any portion of the network becomes disabled or inaccessible, and determine if those arrangements are in writing.

2. If the organization is relying on in-house systems at separate physical locations for recovery, verify if the equipment is capable of independently processing all critical applications.

3. If the organization is relying on outside facilities for recovery, determine if the recovery site:

   - Has the ability to process the required volume;
   - Provides sufficient processing time for the anticipated workload based on emergency priorities; and
   - Allows the organization to use the facility until it achieves a full recovery from the disaster and resumes activity at the organization's own facilities.

4. Review the contract between applicable parties, such as recovery vendors.

5. Determine how the recovery facility's customers would be accommodated if simultaneous disaster conditions were to occur to several customers during the same period of time.

6. Determine whether the organization ensures that when any changes (e.g. hardware or software upgrades or modifications) in the production environment occur that a process is in place to make or verify a similar change in each alternate recovery location.

7. Determine whether the organization is kept informed of any changes at the recovery site that might require adjustments to the organization's software or its recovery plan(s).

Objective 9: Determine whether the business continuity process includes appropriate data and application software backup and recovery.

1. Determine if:

   - Duplicates of the operating systems are available both on- and off-site.
   - Duplicates of the production programs are available both on- and off-site, including both source (if applicable) and object versions.
   - All programming and system software changes are included in the back up.
   - Back-up media is stored off-site in a place from which it can be retrieved quickly at any time.
   - Frequency and number of back-up generations is adequate in view of the volume of transactions being processed and the frequency of system updates.
   - Duplicates of transaction files are maintained on- and off-site.
   - Data file back-ups are taken off-site in a timely manner and not brought back until a more current back-up is off-site.

2. Review the written IT continuity plan(s) and determine if the plan(s) addresses the back-up of the systems and programming function (if applicable), including:

   - Back-up of programming tools and software; and
   - Off-site copies of program and system documentation.

Objective 10: Determine whether the BCP(s) include(s) appropriate preparation to ensure the data center recovery processes will work as intended.

1. Determine if the data center has a properly documented BCP(s). Verify that the information technology BCP(s) properly supports and reasonably reflects the goals and priorities found in the corporate BCP(s).

2. Determine if the plan addresses how backlogged transactions and other activity will be brought current.

3. Determine if there are plans in place that address the return to normal operations and original business locations once the situation has been resolved and permanent facilities are again available.

4. Determine if adequate documentation is housed at the alternate recovery location including:

   - Copies of each BCP;
   - Copies of necessary system documentation; and
   - Copies of necessary operating procedures.

Objective 11: Determine that the BCP(s) include(s) appropriate security procedures.

1. Determine whether adequate physical security and access controls exist over data back-ups and program libraries throughout their life cycle, including when they are created, transmitted/delivered to storage, stored, retrieved and loaded, and destroyed.

2. Determine if appropriate physical and logical access controls have been considered and planned for the inactive production system when processing is temporarily transferred to an alternate facility.

3. Determine if the intrusion detection and incident response plan considers resource availability, and facility and systems changes that may exist when alternate facilities are placed in use.

4. Determine if the methods by which personnel are granted temporary access (physical and logical) during continuity planning implementation periods are reasonable.

   - Evaluate the extent to which back-up personnel have been reassigned different responsibilities and tasks when business continuity planning scenarios are in effect and if these changes require a revision to the levels of systems, operational, data, and facilities access.
   - Review the assignment of authentication and authorization credentials to determine if they are based upon primary job responsibilities and if they also include business continuity planning responsibilities.

Objective 12: Determine whether the BCP(s) address(es) critical outsourced activities.

1. Determine if the BCP(s) address(es) communications and connectivity with technical service providers in the event of a disruption at the institution.

2. Determine if the BCP(s) address(es) communications and connectivity with technology service providers (TSPs) in the event of a disruption at the service provider's facility(ies).

3. Determine if there are documented procedures in place for accessing, downloading, and uploading information with TSPs, correspondents, affiliates and other service providers, from primary and recovery locations, in the event of a disruption.

4. Determine if the institution has a copy of the TSP's BCP(s) and incorporates it, as appropriate, into their plans.

5. Determine if management has received and reviewed testing results of their TSPs.

6. When testing with the critical service providers, determine whether management considered testing:

   - From the institution's primary location to the TSPs' alternative location;
   - From the institution's alternative location to the TSPs' primary location; and
   - From the institution's alternative location to the TSPs' alternative location.

7. Determine if institution management has assessed the adequacy of the TSP's business continuity program through their vendor management program (e.g. contract requirements, SAS 70 reviews).

Conclusions

Objective 13: Discuss corrective action and communicate findings.

1. From the procedures performed:

   - Document conclusions related to the quality and effectiveness of the business continuity process.
   - Determine and document to what extent, if any, you may rely upon the procedures performed by the internal and external auditors in determining the scope of the business continuity procedures.

2. Review your preliminary conclusions with the examiner-in-charge (EIC) regarding:

   - Violations of law, rulings, regulations;
   - Significant issues warranting inclusion as matters requiring board attention or recommendations in the report of examination; and
   - Potential impact of your conclusions on composite and component ratings.

3. Discuss your findings with management and obtain proposed corrective action and deadlines for remedying significant deficiencies.

4. Document your conclusions in a memo to the EIC that provides report ready comments for all relevant sections of the FFIEC Report of Examination.

5. Organize your work papers to ensure clear support for significant findings and conclusions.

APPENDIX B: GLOSSARY

Back-up Generations	A methodology for creating and storing back-up files whereby the youngest (or most recent file) is referred to as the “son,” the prior file is called the “father,” and the file two generations older is the “grandfather.” This back-up methodology is frequently used to refer to master files for financial applications.
Business Continuity Plan (BCP)	A comprehensive written plan to maintain or resume business in the event of a disruption.
Business Impact Analysis (BIA)	The process of identifying the potential impact of uncontrolled, non-specific events on an institution's business processes.
Critical financial markets	Financial markets whose operations are critical to the U.S. economy, including markets for fed funds, foreign exchange, commercial paper, and government, corporate, and mortgage-backed securities.
Data synchronization	The comparison and reconciliation of interdependent data files at the same time so that they contain the same information.
Disaster recovery plan	A plan that describes the process to recover from major processing interruptions.
Emergency plan	The steps to be followed during and immediately after an emergency such as a fire, tornado, bomb threat, etc.
Encryption	The conversion of information into a code or cipher.
FEMA	Acronym for Federal Emergency Management Agency.
Gap analysis	A comparison that identifies the difference between actual and desired outcomes.
GETS	Acronym for the Government Emergency Telecommunications Service card program. GETS cards provide emergency access and priority processing for voice communications services in emergency situations.
HVAC	Acronym for heating, ventilation, and air conditioning.
Media	Physical objects that store data, such as paper, hard disk drives, tapes, and compact disks (CDs).
Mirroring	A process that duplicates data to another location over a computer network in real time or close to real time.
Object program	A program that has been translated into machine-language and is ready to be run (i.e., executed) by the computer.
PBX	Acronym for private branch exchange.
Reciprocal agreement	An agreement whereby two organizations with similar computer systems agree to provide computer processing time for the other in the event one of the systems is rendered inoperable. Processing time may be provided on a "best effort" or "as time available" basis.

Recovery point objectives	The amount of data that can be lost without severely impacting the recovery of operations.
Recovery site	An alternate location for processing information (and possibly conducting business) in an emergency. Usually distinguished as "hot" sites that are fully configured centers with compatible computer equipment and "cold" sites that are operational computer centers without the computer equipment.
Recovery time objectives	The period of time that a process can be inoperable.
Recovery vendors	Organizations that provide recovery sites and support services for a fee.
Routing	The process of moving information from its source to a destination.
SAS 70 report	An audit report of a servicing organization prepared in accordance with guidance provided in the American Institute of Certified Public Accountants' Statement of Auditing Standards Number 70.
Server	A computer or other device that manages a network service. An example is a print server, a device that manages network printing.
Source program	A program written in a programming language (such as C, Pascal, or COBOL). A compiler translates the source code into a machine-language object program.
System Development Life Cycle (SDLC)	A written strategy or plan for the development and modification of computer systems, including initial approvals, development documentation, testing plans and results, and approval and documentation of subsequent modifications.
T-1 line	A special type of telephone line for digital communication only.
UPS	Acronym for uninterruptible power supply. Typically a collection of batteries that provide electrical power for a limited period of time.
Utility programs	A program used to configure or maintain systems, or to make changes to stored or transmitted data.
Vaulting	A process that periodically writes back-up information over a computer network directly to the recovery site.

APPENDIX C: INTERNAL AND EXTERNAL THREATS

While a BCP should be focused on restoring the financial institution's ability to do business, regardless of the nature of the disruption, different types of disruptions may require a variety of responses in order to resume business. Many types of disasters impact not only the financial institution but also the surrounding community. The human element can be unpredictable in a crisis situation, and should not be overlooked when developing a BCP. Employees and their families could be affected as significantly as, or more significantly than, the institution. Therefore, institution management should consider the impact such a disruption would have on personnel the institution would rely on during such a disaster. For example, providing accommodations and services to family members of employees or ensuring that alternate work facilities are in close proximity to employee residences may make it easier for employees to implement the institution's BCP. Also, cross-training of personnel and succession planning may be just as essential as back-up procedures addressing equipment, data, operating systems, and application software.

This Appendix discusses three primary categories of internal and external threats: malicious activity, natural disasters, and technical disasters.

MALICIOUS ACTIVITY

FRAUD, THEFT, OR BLACKMAIL

Since fraud, theft, or blackmail may be perpetrated more easily by insiders, implementation of employee awareness programs and computer security policies is essential. These threats can cause the loss, corruption, or unavailability of information, resulting in a disruption of service to customers. Restricting access to information that may be altered or misappropriated reduces exposure. The institution may be held liable for release of sensitive or confidential information pertaining to its customers; therefore, appropriate procedures to safeguard information are warranted.

SABOTAGE

Personnel should know how to handle intruders, bomb threats, and other disturbances. The locations of critical operation centers should not be publicized and the facilities should be inconspicuous. A disgruntled employee may try to sabotage facilities, equipment, or files. Therefore, personnel policies should require the immediate removal from the premise of any employee reasonably considered a threat, and the immediate revocation of their computer and facility access privileges. Locked doors, motion

detectors, guards, and other controls that restrict physical access are important preventive measures.

TERRORISM

The risk of terrorism is real and adequate business continuity planning is critical for financial institutions in the event a terrorist attack occurs. Some forms of terrorism (e.g., chemical or biological contamination) may leave facilities intact but inaccessible for extended periods of time. The earlier an attack is detected the better the opportunity for successful treatment and recovery. Active monitoring of federal and state emergency warning systems, such as FEMA and the Center for Disease Control (CDC), should be considered.

Terrorism is not new, but the magnitude of disruption and destruction continues to increase. The loss of life, total destruction of facilities and equipment, and emotional and psychological trauma to employees can be devastating. Collateral damage can result in the loss of communications, power, and access to a geographic area not directly affected.

Terrorist attacks can range from bombings of facilities to cyber-attacks on the communication, power, or financial infrastructures. The goal of cyber-terrorism is to disrupt the functioning of information and communications systems. Unconventional attacks could also include the use of chemical, biological, or nuclear material. Bio-terrorists may employ bacterial or viral agents with effects that are delayed, making prevention, response, and recovery problematic. While the probability of a full-scale nuclear attack is remote, it is necessary to address the readiness to deal with attacks on nuclear power plants and industries using nuclear materials and for attacks initiated by means of "dirty" nuclear devices, weapons combining traditional explosives with radioactive materials.

NATURAL DISASTERS

FIRE

A fire can result in loss of life, equipment, and data. Data center personnel must know what to do in the event of a fire to minimize these risks. Instructions and evacuation plans should be posted in prominent locations, and should include the designation of an outside meeting place so personnel can be accounted for in an emergency, and guidelines for securing or removing media, if time permits. Fire drills should be periodically conducted to ensure personnel understand their responsibilities. Fire alarm boxes and emergency power switches should be clearly visible and unobstructed.

All primary and back-up facilities should be equipped with heat or smoke detectors. Ideally, these detectors should be located in the ceiling, in exhaust ducts, and under raised

flooring. Detectors situated near air conditioning or intake ducts that hinder the build up of smoke may not trigger the alarm. The emergency power shutdown should deactivate the air conditioning system. Walls, doors, partitions, and floors should be fire-resistant. Also, the building and equipment should be grounded correctly to protect against electrical hazards. Lightning can cause building fires, so lightning rods should be installed as appropriate. Local fire inspections can help in preparation and training.

Given government regulations to control ozone depletion, halon fire suppression systems are being replaced with alternative fire suppressant systems. Current systems utilize clean agents and include Inergen, FM-200, FE-13, and carbon dioxide. Additionally, dry pipe sprinkler systems should be used, which activate upon detection of a fire and fill the pipe with water only when required, thereby minimizing the risk of water damage from burst pipes. These systems should be the staged type, where the action triggered by a fire detector permits time for operator intervention before it shuts down the power or releases fire suppressants. Personnel should know how to respond to these automatic suppression systems, as well as the location and operation of power and other shut-off valves. Waterproof covers should be located near sensitive equipment in the event that the sprinklers are activated. Hand extinguishers and floor tile pullers should be placed in easily accessible and clearly marked locations. The extent of fire protection required depends on the degree of risk an institution is willing to accept and local fire codes or regulations.

FLOODS AND OTHER WATER DAMAGE

A financial institution that locates an installation in or near a flood plain exposes itself to increased risk, and should take the necessary actions to manage that level of exposure. As water seeks the lowest level, critical records and equipment should be located on upper floors, if possible, to mitigate this risk. Raised flooring or elevating the wiring and servers several inches off the floor can prevent or limit the amount of water damage. In addition, institutions should be aware that water damage could occur from other sources such as broken water mains, windows, or sprinkler systems. If there is a floor above the computer or equipment room, the ceiling should be sealed to prevent water damage. Water detectors should be considered as a way to provide notification of a problem.

SEVERE WEATHER

A disaster resulting from an earthquake, hurricane, tornado, or other severe weather typically would have its probability of occurrence defined by geographic location. Given the random nature of these natural disasters, institutions located in an area that experiences any of these events should consider including appropriate scenarios in their business continuity planning process. In instances where early warning systems are available, management should provide procedures to be implemented prior to the disaster to minimize losses.

AIR CONTAMINANTS

Some disasters produce a secondary problem by polluting the air for a wide geographic area. Natural disasters such as flooding can also result in significant mold or other contamination after the water has receded. The severity of these contaminants can impact air quality at an institution and even result in evacuation for an extended period of time. Business continuity planning should consider the possibility of air contamination and provide for evacuation plans and the shut down of HVAC systems to minimize the risks caused by the contamination. Additionally, consideration should be given to the length of time the affected facility could be inoperable or inaccessible.

HAZARDOUS CHEMICAL SPILL

Some financial institutions maintain facilities close to chemical plants, railroad tracks, or major highways used to transport hazardous chemicals. A leak or spill can result in air contamination, as described above, chemical fires, as well as other health risks. Institutions should make reasonable efforts to determine the types of chemicals being produced or transported nearby, obtain information about the risks each may pose, and take steps to mitigate such risks.

TECHNICAL DISASTERS

COMMUNICATIONS FAILURE

The distributed processing environment has resulted in an increased reliance on telecommunications networks for both voice and data communications to customers, third parties, and back-up sites. Financial institutions lacking diversity in their telecommunications infrastructures may be susceptible to single points of failure in the event a disaster affects one or more of these critical systems.

Institutions should make efforts to identify and document potential single points of failure within their internal and external communications systems. If arrangements are made with multiple telecommunications providers for diverse routing to achieve redundant systems in an attempt to mitigate this risk, management should, to the extent possible, identify common points of failure within these systems. One technique is to perform an end-to-end trace of all critical or sensitive circuits to search for single points of failure such as a common switch, router, PBX, or telephone central office.

In addition to restoring data communication lines with affiliates and vendors, restoration of communications with employees will be critical to any BCP. As an alternative to voice landlines, institutions should consider cell phones, two-way radios, text-based pagers, corporate and public e-mail systems, and Internet-based instant messaging. Another alternative would be to register and establish a standby World Wide Web home page that is activated during a disaster and is used to communicate information and

instructions to employees, customers, and/or affiliates. Finally, depending upon individual requirements, satellite phones may be useful for communicating with key personnel.

POWER FAILURE

The loss of power can occur for a variety of reasons, including storms, fires, malicious acts, brownouts, and blackouts. A power failure could result in the loss of computer systems, lighting, heating and cooling systems, and security and protection systems. Additionally, power surges can occur as power is restored, and without proper planning, can cause damage to equipment. As a means to control this risk, voltage entering the computer room should be monitored by a recording voltmeter and regulated to prevent power fluctuations. In the event of power failure, institutions should use an alternative power source, such as uninterruptible power supplies (UPS), or gasoline, kerosene, natural gas, or diesel generators. A UPS is essentially a collection of standby batteries that provide power for a short period of time. When selecting a UPS, an institution should make sure that it has sufficient capacity to provide ample time to shut down the system in an orderly fashion to ensure no data is lost or corrupted. Some UPS equipment can initiate the automated shut down of systems without human intervention.

If processing time is more critical, an organization may arrange for a generator, which will provide power to at least the mission critical equipment during extended power outages. Management should maintain an ample supply of fuel on hand and have arrangements for replenishment. One potential advantage of natural gas is that it is supplied by pipeline, avoiding the need to truck it in and maintain it onsite. It is important to note that if a disruption is significant enough it may result in the inability to obtain additional fuel. Further, fuel pumps and delivery systems may not be operable.

It is also important to ensure alternative power supplies receive periodic maintenance and testing to maintain operability. Moreover, management should discuss with local authorities the ordinances relative to location of generators, and the storage and delivery of fuel.

EQUIPMENT AND SOFTWARE FAILURE

Equipment and software failures may result in extended processing delays and/or implementation of BCPs for various business units depending on the severity of the failure. The performance of preventive maintenance enhances system reliability and should be extended to all supporting equipment, such as temperature and humidity control systems and alarm or detecting devices.

TRANSPORTATION SYSTEM DISRUPTIONS

Financial institutions should not assume regional or national transportation systems will continue to operate normally during a disruption. Air traffic and/or trains may be halted by natural or technical disasters, malicious activity, work stoppages, or accidents. This can adversely impact cash distribution, check clearing, and relocation of staff to back-up sites. Institutions should investigate the option of using private, ground-based carriers (e.g., messenger services, trucking companies, bus companies) to ensure the continuation of these vital functions.

APPENDIX D: INTERDEPENDENCIES

TELECOMMUNICATIONS INFRASTRUCTURE

Voice and data communications are essential for conducting business and connecting critical elements of an institution such as business areas, customers and service providers/vendors. The advancement in network technologies allows greater geographic separation between people and system resources and/or primary and alternate processing locations. Network technologies have played a key role in enabling distributed processing environments, which reflect an increased reliance on telecommunications networks for both voice and data communications. Given their critical nature and importance, it is necessary for institutions to design high levels of redundancy and resiliency into their voice and data communication infrastructures. In addition, as critical as it is to have effective business continuity arrangements for a data center, it is equally important to have effective back-up arrangements for voice and data telecommunications links. Since voice and data infrastructures are typically a shared resource across the different business areas of an institution, the dependency and criticality of these resources are further heightened.

The telecommunications infrastructure contains single points of failure that represent vulnerabilities and risks for financial institutions. Elements of risk reside within the public telecommunications network infrastructure and are outside the control of a single institution. This necessitates the need for financial institutions to be proactive in establishing robust processes to ensure telecommunication resiliency and diversity. Institutions need to develop risk management practices to identify and eliminate single points of failure across their network infrastructures. Risk management strategies need to be incorporated into the design, acquisition, implementation, and maintenance processes related to communication networks and should address single points of failure or points of commonality relating to:

- Primary and back-up network infrastructures;
- Telecommunication carriers;
- Points of entry into facilities;
- Telecommunication routing through central offices; and
- PBXs within an institution.

Financial institutions are encouraged to actively manage their service relationship with their telecommunication providers in order to manage risk more effectively. In

coordination with vendors, management should ensure that, at a minimum, risk management strategies:

- Establish service level agreements that address contingency measures and change management for services provided;
- Establish processes to inventory and validate telecommunication circuits and routing paths; and
- Include a framework to periodically verify telecommunication routing paths.

In addition to robust risk management practices, financial institutions should have viable business continuity arrangements for voice and data services. At a minimum, telecommunications plans should address skilled human resources, internal and external connectivity, communications media, network equipment and telecommunication management systems. The BCP should establish priorities and identify critical network components. Original plan components such as reliability, flexibility, and compatibility must also be considered in formulating the back-up plan. For example, a modem used for back-up may not provide the level of service required, or a line may satisfactorily transmit voice, but be insufficient in quality and speed for data transmission. The costs of various back-up alternatives should be weighed against the level of risk protection provided by the alternatives. This assessment also should address costs associated with testing, since all components of a plan should be tested periodically, including the communications media.

The BCP should address the practicality of each component. Selected alternatives should be able to accommodate the anticipated volumes or capacities at the necessary speeds to meet the established priorities. For example, several dial-up lines may not be a practical replacement for a T-1 line. Also, the back-up plan should recognize availability and lead times required to employ certain components, such as installing additional lines or modems and multiplexers/concentrators at a recovery site.

Financial institutions that play a key role in the maintenance of financial systems should be aware of certain government programs and offices that work to coordinate and expedite the restoration or procurement of telecommunication services during an emergency. The Office of Priority Telecommunications (OPT) under the National Communications System (NCS) administers the Telecommunications Service Priority System (TSP) which ensures priority treatment of the nation's most important telecommunication services supporting national security and emergency preparedness missions.[8] This means that TSP designated circuits will be the first to be repaired in an emergency. All non-federal users requesting TSP provisioning or restoration are required

[8] See http://tsp.ncs.gov.

to have a federal agency sponsor. Institutions are encouraged to contact their primary federal regulator for information on the TSP program and whether they qualify for a TSP designation.

Similarly, some financial institutions may qualify for sponsorship in the Government Emergency Telecommunications Service (GETS) card program. This program is also administered by NCS and provides emergency access and priority processing for voice communications services in emergency situations. Financial institutions that perform national security or emergency preparedness functions essential to the maintenance of the nation's economic posture during any national or regional emergency will qualify for program sponsorship.[9]

The BCP should consider the security of alternative components to ensure data integrity. Switching from fiber optics to wire pairs, dedicated to switched, or digital to analog may make the line more susceptible to a wiretap or to line noise, which can result in errors. Using dial-up lines could facilitate access by the public. Additionally, where warranted, alternate equipment selected should be checked to determine if it permits encryption.

The relative importance of the applications processed and the extent to which an institution depends on its telecommunications system will determine the degree of back up required. Management should make a careful appraisal of its back-up telecommunications requirements, decide on an effective plan, detail the procedures, and test its effectiveness periodically.

THIRD-PARTY PROVIDERS, KEY SUPPLIERS, AND BUSINESS PARTNERS

Reliance on third-party providers, key suppliers, or business partners may expose financial institutions to points of failure that may prevent resumption of operations in a timely manner. The risks in outsourcing information, transaction processing, and settlement activities include threats to the security, availability and integrity of systems and resources, to the confidentiality of information, and to regulatory compliance. In addition, when a third party performs services on behalf of the institution, increased levels of credit, liquidity, transaction, and reputation risk can result. Institutions should review and understand service providers' BCPs and ensure critical services can be restored within acceptable timeframes based upon the needs of the institution. The contract should address the service provider’s responsibility for maintenance and testing

[9] See *Interim Sponsorship Policy for Government Emergency Telecommunications Service (GETS) Cards*, Federal Deposit Insurance Corporation FIL-84-2002 (August 6, 2002); Office of the Comptroller of the Currency, Bulletin 2002-33 (July 23, 2002); Office of Thrift Supervision, CEO Ltr 165 (July 26, 2002).

of disaster recovery and contingency plans. The financial institution should be provided testing results and review audits to determine the adequacy of plans and the effectiveness of the testing process. If possible, the institution should consider participating in their service provider's testing process.

Contracts should include detailed business recovery timeframes that meet the business continuity planning needs of the institution. A financial institution's business continuity planning process should include developing call lists necessary for contacting key individuals at the service provider's primary and recovery locations. The institution's BCP should also address how it will be exchanging information with its service providers should the institution be operating from an alternative location, e.g., transmission via a branch facility that has redundant telecommunications links with the service provider.

CONTRACTS

Many financial institutions contract with third-party service providers and other vendors for disaster recovery assistance. These arrangements can be cost-effective for smaller institutions since the cost of maintaining a dedicated recovery site can be substantial. When contracting with third-party providers for recovery services, institutions should consider:

- *Staffing*—What kinds of technical support personnel is the service provider obligated to make available onsite to assist institution employees in getting the recovery site operating?
- *Processing Time Availability*—Assuming other clients are also using the same recovery site, how much processing time is the institution entitled to on a particular computer system? Is the institution guaranteed a sufficient amount of processing time to handle the volume of work that will need to be done at the site?
- *Access Rights*—Since most back-up sites can be used by numerous clients, does the institution have a guaranteed right to use the site in case of an emergency? Alternatively, does the service provider accept clients on a first-come, first-serve basis until the recovery site is at full capacity?
- *Hardware and Software*—Is the recovery site equipped with the precise computer hardware and software that the institution needs to continue operations? Will the institution be notified of changes in the equipment at the recovery site?
- *Security Controls*—Does the recovery site have sufficient physical and logical security to adequately protect the institution's information assets?
- *Testing*—Does the contract with the service provider permit the institution to perform at least one full-scale test of the recovery site annually? Does the service provider perform tests of its own BCP and submit test reports to customer financial institutions?

- *Confidentiality of Data*—In the event other businesses are also using the recovery site, what steps will the service provider take to ensure the security and confidentiality of institution data? Has the service provider entered into an appropriate contract with the customer financial institution that addresses the requirements of the Interagency Guidelines Establishing Standards for Safeguarding Customer Information?
- *Telecommunications*—Has the service provider taken appropriate steps to ensure the recovery site will have adequate telecommunications services (both voice and data) for the number of personnel that will be working at that site and the volume of data transmissions that are anticipated?
- *Reciprocal Agreements*—In the event the institution's recovery site is another financial institution with whom it has a reciprocal agreement, does the other institution have sufficient excess computer capacity to ensure the affected institution's work will get done? Are the hardware and software at the recovery site compatible with the affected institution's systems? Will the institution be notified of changes in equipment at the recovery site?
- *Space*—Does the recovery site have adequate space and related services to accommodate the affected institution's staff and enable them to conduct business? This may also include consideration of the space at the service provider or in the local community to provide food, toilets, medical supplies, family care, counseling, news, housing, and diversions to personnel.
- *Paper Files and Forms*—Does the recovery site maintain a sufficient inventory of paper-based files and forms that are necessary to the conduct of the affected institution's business?
- *Printing Capacity/Capability*—Does the recovery site maintain adequate printing capacity to meet the demand of the affected institution?
- *Contacts*—Who at the institution is authorized to initiate use of the back-up site? Who does the institution contact at the back-up site?

APPENDIX E: BCP COMPONENTS

PERSONNEL

Based on the BIA, the BCP should assign responsibilities to management, specific personnel, teams, and service providers. The plan should identify integral personnel that are needed for successful implementation of the plan and develop contingencies to be implemented should those employees not be available. Additionally, vendor support needs should be identified. The BCP should address:

- How will decision making succession be determined in the event of the loss of management personnel?
- Who will be responsible for leading the various BCP Teams (e.g., Crisis/Emergency, Recovery, Technology, Communications, Facilities, Human Resources, Business Units and Processes, Customer Service)?
- Who will be the primary contact with critical vendors, suppliers, and service providers?
- Who will be responsible for security (information and physical)?

Planning should also consider personnel resources necessary for decision making and staffing at alternate facilities under various scenarios. Key personnel should be identified to make decisions regarding efforts to provide for renovating or rebuilding the primary facility. This could require personnel beyond what is necessary for ongoing business continuity efforts.

Finally, the business continuity planning coordinator and/or planning committee should be given responsibility for regularly updating the BCP on at least an annual basis, and after significant changes to the operations and environment.

TECHNOLOGY COMPONENTS

The technology components that should be addressed in an effective BCP include:

- Hardware – mainframe, network, end-user;
- Software – applications, operating systems, utilities;
- Communications (network and telecommunications);
- Data files and vital records;

- Operations processing equipment; and
- Office equipment.

Comprehensive inventories will assist with the business resumption and recovery efforts, and ensure all components are considered during plan development. Planning should include identifying critical business unit data that may only reside on individual workstations, which may or may not adhere to proper back-up schedules. Additionally, the plan should address vital records, necessary back-up methods, and appropriate back-up schedules for these records.

Institutions should exercise caution when identifying non-critical assets. An institution's telephone banking, Internet banking, or ATM systems may not seem mission critical when systems are operating normally. However, these systems may play a critical role in the BCP and be a primary delivery channel to service customers during a disruption. Similarly, an institution's electronic mail system may not appear to be mission critical, but may be the only system available for employee or external communication in the event of a disruption.

DATA CENTER RECOVERY ALTERNATIVES

Financial institutions should make formal arrangements for alternate processing capability in the event their data processing site becomes inoperable or inaccessible. The type of recovery alternative selected will vary depending on the criticality of the processes being recovered and the recovery time objectives. Recovery plan alternatives may take several forms and involve the use of another data center, or installation, such as a third-party service provider. A legal contract or agreement should evidence recovery arrangements with a third-party vendor. The following are acceptable alternatives for data center recovery. However, institutions will be expected to describe their reasons for choosing a particular alternative and why it is adequate based on their size and complexity.

- *Hot Site (traditional "active/backup" model)*—A hot site is fully configured with compatible computer equipment and typically can be operational within several hours. Financial institutions may rely on the services of a third party to provide back-up facilities. The traditional active/back-up model requires relocating, at a minimum, core employees to the alternative site. This model also requires back-up media to be transferred off-site on at least a daily basis. Large institutions that operate critical real-time processing operations or critical high-volume processing activities should consider mirroring or vaulting. If an institution is relying on a third party to provide the hot site, there remains a risk that the capacity at the service provider may not be able to support their operations in the event of a regional or large-scale event. Smaller, less complex institutions may contract for a "mobile hot site," i.e., a trailer

outfitted with the necessary computer hardware that is towed to a predetermined location in the event of a disruption and connected to a power source.

- *Duplicate Facilities/Split Operations ("active/active" model)*—Under this scenario, two or more separate, active sites provide inherent back up to one another. Each site has the capacity to absorb some or all of the work of the other site for an extended period of time. This strategy can provide almost immediate resumption capacity, depending on the systems used to support the operations and the operating capacity at each site. The maintenance of excess capacity at each site and added operating complexity can have significant costs. Even using the active/active model, current technological limitations preclude wide geographic diversity of data centers that use real-time, synchronous data mirroring back-up technologies. However, other alternatives beyond synchronous mirroring may be available to allow for greater distance separation.

- *Cold Site*—Cold sites are locations that are part of a longer-term recovery strategy. A cold site provides a back-up location without equipment, but with power, air conditioning, heat, electrical, network and telephone wiring, and raised flooring. An example of a situation when a cold site can be a viable alternative is when a financial institution has recovered at another location, such as a hot site, but needs a longer-term location while their data center is being rebuilt. Cold sites typically can take up to several weeks to activate. Institutions may rely on the services of a third party to provide cold site facilities or may house such a facility at another location, such as a branch or other operations center.

- *Tertiary Location*—Some financial institutions have identified the need to have a third location or a "back-up to the back-up." These tertiary locations provide an extra level of protection in the event neither the primary location nor the secondary location is available. Moreover a tertiary location becomes the primary back up location in the event the institution has declared a disaster and is operating out of its contingency or secondary site.

Some financial institutions enter into agreements, commonly referred to as "Reciprocal Agreements," with other institutions to provide equipment back up. This arrangement is usually made on a best effort basis, whereby institution "A" promises to back up institution "B" as long as institution "A" has time available, and vice versa. In the vast majority of cases, reciprocal agreements are unacceptable because the institution agreeing to provide back-up has insufficient excess capacity to enable the affected institution to process its transactions in a timely manner. If an institution chooses to enter into a reciprocal agreement and can establish that such an arrangement will provide an acceptable level of back-up, the agencies expect such an agreement to be in writing and to obligate institution "A" to make available sufficient processing capacity and time. The agreement should also specify that each institution will be notified of equipment and software changes at the other institution.

BACK-UP RECOVERY FACILITIES

The recovery site should be tested at least annually and when equipment or application software is changed to ensure continued compatibility. Additionally, the recovery facility should exhibit a greater level of security protection than the primary operations site since the people and systems controlling access to the recovery site will not be as familiar with the relocated personnel using it. This security should include physical and logical access controls to the site as well as the computer systems. Further, the BCP and recovery procedures should be maintained at the alternative and off-site storage locations.

Regardless of which recovery strategy is utilized, the recovery plan should address how any backlog of activity and/or lost transactions will be recovered. The plan should identify how transaction records will be brought current from the time of the disaster and the expected recovery timeframes.

Alternative workspace capacity is just as important as alternative data processing capabilities. Management should arrange for workspace facilities and equipment for employees to conduct ongoing business functions.

GEOGRAPHIC DIVERSITY

When determining the physical location of an alternate-processing site, management should consider geographic diversity. Financial institutions should consider the geographic scope of disruptions and the implications of a citywide disruption or even a regional disruption. The distance between primary and back-up locations should consider recovery time objectives and business unit requirements. Locating a back-up site too close to the primary site may not insulate it sufficiently from a regional disaster. Alternatively, locating the back-up site too far away may make it difficult to relocate the staff necessary to operate the site. If relocation of staff is necessary to resume business operations at the alternate site, consideration should be given to their willingness to travel due to the events, the modes of transportation available, and if applicable, lodging and living expenses for employees that relocate. When evaluating the locations of alternate-processing sites, it is also important to subject the secondary sites to a threat scenario analysis.

BACK-UP AND STORAGE STRATEGIES

Institution management should base decisions on software and data file back up on the criticality of the software and data files to the financial institution's operations. In establishing back-up priorities, management should consider all types of information and the potential impact from loss of such files. This includes financial, regulatory, and administrative information, and operating, application, and security software. In assigning back-up priority, management should perform a risk assessment that addresses whether:

- The loss of these files would significantly impair the institution's operations;
- The files are being used to manage corporate assets or to make decisions regarding their use;
- The files contain updated security and operating system configurations that would be necessary to resume operations in a secure manner;
- The loss of the files would result in lost revenue; and
- Any inaccuracy or data loss would result in significant impact on the institution (including reputation) or its customers.

The frequency of file back up also depends on the criticality of the application and data. Critical data should be backed up using the multiple generation (i.e., "grandfather-father-son," etc.) method and rotated to an off-site location at least daily. Online/real-time or high volume systems may necessitate more aggressive back-up methods such as mirroring or electronic vaulting at a separate processing facility to ensure appropriate back up of operations, as an alternative to back-up tape storage.

Back-up tape storage remains a viable solution for many financial institutions. However, when an institution's primary back-up media is tape storage, back-up tapes should be sent to the off-site storage as soon as possible, and should not reside at their originating location overnight. Back-up media, especially tapes, should be periodically tested to ensure they are still readable. Tapes repeatedly used or subjected to extreme variations in temperature or humidity may become unreadable, in whole or part, over time.

Remote journaling is the process of recording transaction logs or journals at a remote location. These logs and journals are used to recover transaction and database changes since the most recent back up.

Back-up of operating system software and application programs must be performed whenever they are modified, updated, or changed.

DATA FILE BACK UP

One of the most critical components of the back-up process involves the financial institution's data files, regardless of the platform on which the data is located. Institutions must be able to generate a current master file that reflects transactions up to the point in time of the disruption. Data files should be backed up both onsite and off-site to provide recovery capability. Retention of current data files, or older master files and the transaction files necessary to bring them current, is important so that processing can continue in the event of a disaster or other disruption. The creation and rotation of core processing data file back up should occur at least daily, more frequently if the volume of processing or online transaction activity warrants. Less critical data files may not need to

be backed up as frequently. In either case, back-up data files should be transported off-site in a timely manner and not be returned until new back-up files are off-site.

SOFTWARE BACK UP

Software back up for all hardware platforms consists of three basic areas: operating system software, application software, and utility software. All software and related documentation should have adequate off-premises storage. Even when using a standard software package from one vendor, the software can vary from one location to another. Differences may include parameter settings and modifications, security profiles, reporting options, account information, or other options chosen by the institution during or subsequent to system implementation. Therefore, comprehensive back up of all critical software is essential.

The operating system software should be backed up with at least two copies of the current version. One copy should be stored in the tape and disk library for immediate availability in the event the original is impaired; the other copy should be stored in a secure, off-premises location. Duplicate copies should be tested periodically and recreated whenever there is a change to the operating system.

Application software, which includes both source (if the institution has it in its possession) and object versions of all application programs, should be maintained in the same manner as the operating system software. Back-up copies of the programs should be updated as program changes are made.

Given the increased reliance on the distributed processing environment, the importance of adequate back-up resources and procedures for local area networks and wide area networks is important. Management should ensure that all appropriate programs and information are backed up.

Depending on the size of the financial institution and the nature of anticipated risks and exposures, the time spent backing up data is minimal compared with the time and effort necessary for restoration. Files that can be backed up within a short period of time may require days, weeks, or months to recreate from hardcopy records, assuming hardcopy records are available. Comprehensive and clear procedures are necessary to recover critical networks and systems. Procedures should, at a minimum, include:

- Frequency of update and retention cycles for back-up software and data;
- Periodic review of software and hardware for compatibility with back-up resources;
- Periodic testing of back-up procedures for effectiveness in restoring normal operations;
- Guidelines for the labeling, listing, transportation and storage of media;

- Maintenance of data file listings, their contents, and locations;
- Hardware, software, and network configuration documentation;
- Controls to minimize the risks involved in the transfer of back-up data, whether by electronic link or through the physical transportation of diskettes and tapes to and from the storage site; and
- Controls to ensure data integrity, client confidentiality, and the physical security of hardcopy output, media, and hardware.

OFF-SITE STORAGE

The off-site storage location should be environmentally controlled and secure, with procedures for restricting physical access to authorized personnel. Moreover, the off-site premises should be an adequate distance from the computer operations location so that both locations will not be impacted by the same event. Beyond a copy of the BCP, duplicate copies of all necessary procedures, including end of day, end of month, end of quarter, and procedures covering relatively rare and unique issues should be stored at the offsite locations. Another alternative to consider would be to place the critical information on a secure shared network drive, with the data backed up during regularly scheduled network back-up. However, this shared drive should be in a different physical location that would not be affected by the same disruption. Management needs to maintain a certain level of non-networked (e.g., hardcopy) material in the event that the network environment is not available for a period of time.

Reserve supplies, such as forms, manuals, letterhead, etc., should also be maintained in appropriate quantities at an off-site location and management should maintain a current inventory of what is held in the reserve supply.

FACILITIES

The BCP should address site relocation for short-, medium- and long-term disaster and disruption scenarios. Continuity planning for recovery facilities should consider location, size, capacity (computer and telecommunications), and required amenities necessary to recover the level of service required by the critical business functions. This includes planning for workspace, telephones, workstations, network connectivity, etc. When determining an alternate processing site, management should consider scalability, in the event a long-term disaster becomes a reality. Additionally, during the recovery period, the BCP should be reassessed to determine if tertiary plans are warranted. Procedures to utilize at the recovery location should be developed. In addition, any files, input work, or specific forms, etc., needed at the back-up site should be specified in the written plan.

The plan should include logistical procedures for moving personnel to the recovery location, in addition to steps to obtain the materials (media, documentation, supplies, etc.)

from the off-site storage location. Plans for lodging, meals, and family considerations may be necessary.

COMMUNICATION

Communication is a critical aspect of a BCP and should include communication with emergency personnel, employees, directors, regulators, vendors/suppliers (detailed contact information), customers (notification procedures), and the media (designated media spokesperson). Alternate communication channels should be considered such as cellular telephones, pagers, satellite telephones, and Internet based communications such as e-mail or instant messaging.

OTHER CONSIDERATIONS

Each financial institution is different and processes will vary. However, management should consider how to accomplish the following:

- Prevention and preparedness;
- Reconciling recovery times with business unit requirements;
- Disaster declaration and plan implementation processes;
- Recovery progress reporting; and
- Testing of the plans.