Federal Financial Institutions Examination Council

FFIEC

Business Continuity Planning BCP

FEBRUARY 2015

IT Examination Handbook

Table of Contents

Introduction

This booklet is one in a series of booklets that comprise the Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook. This booklet provides guidance to assist examiners in evaluating financial institution [1] and service provider risk management processes to ensure the availability of critical financial services. This booklet was also designed to provide helpful guidance to financial institutions regarding the implementation of their business continuity planning processes.

This booklet rescinds and replaces the previous "Business Continuity Planning Booklet," which was issued in March 2003, and has been revised to reflect technological and regulatory changes with a focus on management's responsibilities regarding oversight of the continuity planning process for business operations. While significant revisions have been made, the focus of this booklet continues to be based on an enterprise-wide, process-oriented approach that considers technology, business operations, testing, and communication strategies that are critical to business continuity planning for the entire business, instead of just the information technology department.

This booklet is divided into two parts. The first part, or narrative, describes the business continuity planning process and addresses the responsibilities of the board of directors (board) and senior management. The second part includes examination procedures, a glossary, detailed appendices supporting the narrative, and a reference list of each agency's applicable laws, regulations, and guidance. Each section in the narrative begins with an "Action Summary" that highlights the major points in that section. While not a substitute for reading the entire booklet, the action summaries may be used to quickly assess the most important issues discussed in that section. It is also important to read the detailed appendices, which can serve as a comprehensive reference guide for the topics discussed in the narrative.

The overall goal of this booklet is to provide guidance to the financial services industry about the importance of business continuity planning, which establishes the basis for financial institutions to recover and resume business processes when operations have been disrupted unexpectedly. Because financial institutions play a crucial role in the overall economy, disruptions in service should be minimized in order to maintain public trust and confidence in the financial system. As such, financial institution management should incorporate business continuity considerations into the overall design of their business model to proactively mitigate the risk of service disruptions.

Financial institution management should develop a comprehensive business continuity plan (BCP) as part of the business continuity planning process. The BCP should be based on the size and complexity of the institution and should be consistent with the financial institution's overall business strategy. The goal of the BCP should be to minimize financial losses to the institution, serve customers and financial markets with minimal disruptions, and mitigate the negative effects of disruptions on business operations. Reviewing a financial institution's business continuity planning process, which includes an assessment of the BCP, is an established part of examinations performed by the FFIEC member agencies. [2]

Changes in business processes and technology increased terrorism concerns, recent catastrophic natural disasters, and the threat of a pandemic have focused even greater attention on the need for effective business continuity planning. Consequently, these issues should be given greater consideration in the business continuity planning

process. Financial institution management should consider the potential for area-wide disasters that could affect an entire region and result in significant losses to the institution. The business continuity planning process should address interdependencies, both market-based and geographic, among financial system participants and infrastructure service providers. In most cases, recovery time objectives (RTOs) are now much shorter than they were a few years ago, and for some institutions, RTOs are based on hours and even minutes. Ultimately, all institutions should anticipate and plan for the unexpected and ensure that their business continuity planning process appropriately addresses the lessons they have learned from past disasters.

Board and Senior Management Responsibilities

Action Summary

A financial institution's board and senior management are responsible for overseeing the business continuity planning process, which includes:

- Establishing policy by determining how the institution will manage and control identified risks;
- Allocating knowledgeable personnel and sufficient financial resources to properly implement the BCP;
- Ensuring that the BCP is independently reviewed and approved at least annually;
- Ensuring employees are trained and aware of their roles in the implementation of the BCP;
- Ensuring the BCP is regularly tested on an enterprise-wide basis;
- Reviewing the BCP testing program and test results on a regular basis; and
- Ensuring the BCP is continually updated to reflect the current operating environment.

It is the responsibility of an institution's board and senior management to ensure that the institution identifies, assesses, prioritizes, manages, and controls risks as part of the business continuity planning process. The board and senior management should establish policies that define how the institution will manage and control the risks that were identified. Once policy is established, it is also important for the board and senior management to understand the consequences of these identified risks and support continuity planning on a continuous basis.

As part of their support for continuity planning, the board and senior management should

assign knowledgeable personnel and allocate sufficient financial resources to properly implement an enterprise-wide BCP. A large, complex institution may need a business continuity planning department with a team of departmental liaisons throughout the institution. A smaller, less complex institution may only need an individual business continuity planning coordinator. Financial institutions may also choose to have a business continuity planning group or committee that meets regularly with the BCP coordinator to discuss various issues, such as policy changes, employee training, and test plans. Regardless of how personnel resources are allocated, financial institution management should establish roles, responsibilities, and succession plans for various operational disruptions, as they may affect business processes in different ways. The board and senior management should also allocate sufficient financial resources to cover the expenses associated with alternate processing arrangements, business recovery, and comprehensive insurance coverage..

The board and senior management are also responsible for ensuring that the BCP is independently reviewed by the internal or external auditor at least annually. The board and senior management should also review and approve the BCP, with the frequency based on significant policy revisions resulting from changes in the operating environment, lessons learned from BCP testing, and audit and examination recommendations. These review procedures will ensure a more complete validation of all aspects of the BCP planning and management processes.

Once the BCP has been approved, the board and senior management should ensure that a comprehensive business continuity training program has been established. As part of this process, they should ensure that employees understand their roles and responsibilities as defined by the BCP. Consequently, the board and senior management should oversee the development of the business continuity training program and ensure that existing and new employees are trained on a continuous basis. These training programs may include instructional classes, computer-based training, and hands-on experience using various testing methods.

To maintain the effectiveness of the BCP, the board and senior management should ensure that enterprise-wide BCP tests are conducted at least annually, or more frequently depending on changes in the operating environment. Formal procedures should be established for reporting the implementation of the testing program and test results to the board and senior management.

After the BCP is approved and tested, the board and senior management have an on-going responsibility to oversee critical business processes and ensure that the BCP is updated to reflect the current operating environment.

Business Continuity Planning Process

Action Summary

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

- The business continuity planning process should include the recovery, resumption, and maintenance of all aspects of the business, not just recovery of the technology components;
- Business continuity planning involves the development of an enterprise-wide BCP and the prioritization of business objectives and critical operations that are essential for recovery;
- Business continuity planning includes the integration of the institution's role in financial markets;
- Business continuity planning should include regular updates to the BCP based on changes in business processes, audit recommendations, and lessons learned from testing; and
- Business continuity planning represents a cyclical, process-oriented approach that includes a business impact analysis (BIA), a risk assessment, risk management, and risk monitoring and testing.

The business continuity planning process involves the recovery, resumption, and maintenance of the entire business, not just the technology component. While the restoration of IT systems and electronic data is important, recovery of these systems and data will not always be enough to restore business operations.

Business continuity planning involves the development of an enterprise-wide BCP and the prioritization of business objectives and critical operations that are essential for recovery. This enterprise-wide framework should consider how every critical process, business unit, department, and system will respond to disruptions and which recovery solutions should be implemented. This framework should include a plan for short-term and long-term recovery operations. Without an enterprise-wide BCP that considers all critical elements of the entire business, an institution may not be able to resume customer service at an acceptable level. Management should also prioritize business objectives and critical operations that are essential for survival of the institution since the restoration of all business units may not be feasible because of cost, logistics, and other unforeseen circumstances.

Business continuity planning includes the integration of the institution's role in financial markets. Financial industry participants that perform clearing and settlement activities for critical financial markets (core firms) and organizations that process a significant share of transactions in critical financial markets (significant firms) are required to follow interagency guidelines, [3] which are designed to ensure the continued functioning of settlement and clearing activities that support critical financial markets. 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. Based on these guidelines, key financial industry participants are expected to identify activities that support these critical markets, continually maintain their ability to recover and resume critical operations in a timely manner, and routinely use or test recovery and resumption arrangements. Since these organizations participate in one or more critical financial markets and their failure to perform critical activities by the end of the business day could present systemic risk to financial systems, their role in financial markets should be addressed as part of the business continuity planning process

Financial institutions that do not directly participate in critical financial markets, but support critical financial market activities for regional or national financial sectors, are also expected to establish business continuity planning processes commensurate with their importance in the financial industry. Similarly, smaller, less complex institutions are expected to fulfill their responsibilities by developing an appropriate business continuity planning process that incorporates comprehensive recovery guidelines based on the institution's size and risk profile.

The business continuity planning process should include regular updates to the BCP. The BCP should be updated based on changes in business processes, audit recommendations, and lessons learned from testing. Changes in business processes include technological advancements that allow 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 advances underscore the importance of maintaining a current, enterprise-wide BCP.

Additional industry practices that are commonly used to maintain a current BCP include:

- Integrating business continuity planning into every business decision;
- Incorporating BCP maintenance responsibilities in applicable employee job descriptions and personnel evaluations;
- Assigning the responsibility for periodic review of the BCP to a planning coordinator, department, group, or committee; and
- Performing regular audits and annual, or more frequent, tests of the BCP.

The FFIEC agencies encourage financial institutions to adopt a cyclical, process-oriented approach to business continuity planning. This process-oriented approach will be discussed in the first part of the booklet, with additional information included in the appendices. The four steps in this process include:

1. Business Impact Analysis; [4]
2. Risk assessment; [5]
3. Risk management; [6] and
4. Risk monitoring and testing. [7]

While this approach is reflected as four steps, the business continuity planning process actually represents a continuous cycle that should evolve over time based on changes in potential threats, business operations, audit recommendations, and test results. In addition, this process should include each critical business function and the technology

that supports it. [8] As such, other policies, standards, and processes should also be integrated into the overall business continuity planning process.

Business Impact Analysis

Action Summary

A business impact analysis (BIA) is the first step in the business continuity planning process and should include the:

- Assessment and prioritization of all business functions and processes, including their interdependencies, as part of a work flow analysis;
- Identification of the potential impact of business disruptions resulting from uncontrolled, non-specific events on the institution's business functions and processes;
- Identification of the legal and regulatory requirements for the institution's business functions and processes;
- Estimation of maximum allowable downtime, as well as the acceptable level of losses, associated with the institution's business functions and processes; and
- Estimation of recovery time objectives (RTOs), recovery point objectives (RPOs), and recovery of the critical path.

The institution's first step in the business continuity process is the development of a BIA. [9] The amount of time and resources needed to complete the BIA will depend on the size and complexity of the financial institution. The BIA should include a work flow analysis that involves an assessment and prioritization of those business functions and processes that must be recovered. The work flow analysis should be a dynamic process that identifies the interdependencies between critical operations, departments, personnel, and services. The identification of these interdependencies, as part of the BIA, should assist management in determining the priority of business functions and processes and the overall affect on recovery timelines.

Once business functions and processes have been assessed and prioritized, the BIA should identify the potential impact of uncontrolled, non-specific events on these business functions and processes. Non-specific events should be identified so that management can concentrate on the impact of various disruptions instead of specific threats that may never affect operations. At the same time, management should never ignore potential risks that are evident in the institution's particular area. For example, financial institutions may be located in flood-prone areas, near fault lines, or by areas subject to tornados or hurricanes.

In addition to identifying the impact of non-specific events on business functions and processes, the BIA should also consider the impact of legal and regulatory requirements.

For example, management should assess the impact of compromised customer data, which can result in regulatory concerns and a loss of public confidence. [10] By identifying the potential impact of this issue, management may have a better idea of the business functions and processes that could potentially be affected. Management should consider the regulatory requirement regarding notification to the institution's primary federal regulator when facilities are relocated. [11]

The BIA should also estimate the maximum allowable downtime for critical business functions and processes and the acceptable level of losses (data, operations, financial, reputation, and market share) associated with this estimated downtime. As part of this analysis, management should decide how long its systems can operate before the loss becomes too great and how much data the financial institution can afford to lose and still survive. The results of this step will assist institution management in establishing RTOs, RPOs, and recovery of the critical path, which represents those business processes or systems that must receive the highest priority during recovery. These recovery objectives should be considered simultaneously to determine more accurately the total downtime a financial institution could suffer due to a disaster. In addition, these recovery objectives require management to determine which essential personnel, technologies, facilities, communications systems, vital records, and data must be recovered and what processing sequence should be followed so that activities that fall directly on the critical path receive the highest priority. One of the advantages of analyzing allowable downtime and recovery objectives is the potential support it may provide for the funding needs of a specific recovery solution based on the losses identified and the importance of certain business functions and processes.

Personnel responsible for the BIA 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 the 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 comprehensive BCP can be developed.

When determining a financial institution's critical needs, all functions, processes, and personnel should be analyzed. In documenting the mission critical functions performed, each department should consider the following questions:

- What critical interdependencies exist between internal systems, applications, business processes, and departments?
- What specialized equipment is required and how is it used?
- How would the department function if the 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 are the required responsibilities of the institution and the third-party service provider as defined by the service level agreement?

- What critical operational or security controls require implementation prior to recovery?
- What is the minimum number of staff and amount of space that would be required at a recovery site?
- What special forms or supplies would be needed at a recovery site?
- What equipment would be needed at a recovery site to communicate with employees, vendors, and customers?
- What is the potential impact if common recovery sites serve multiple financial institutions?
- Have employees received cross training, and has the department defined back-up functions/roles that employees should perform if key personnel are not available?
- Are the personal needs of employees adequately considered?
- What are the critical cash management/liquidity issues?

Once the BIA is complete, it should be evaluated during the risk assessment process and incorporated into, and tested as part of, the BCP. The BIA should be reviewed by the board and senior management periodically and updated to reflect significant changes in business operations, audit recommendations, and lessons learned during the testing process. In addition, a copy of the BIA should be maintained at an offsite location so it is easily accessible when needed.

Risk Assessment

Action Summary

The risk assessment is the second step in the business continuity planning process. It should include:

- Evaluating the BIA assumptions using various threat scenarios;
- Analyzing threats based upon the impact to the institution, its customers, and the financial market it serves;
- Prioritizing potential business disruptions based upon their severity, which is determined by their impact on operations and the probability of occurrence; and
- Performing a "gap analysis" that compares the existing BCP to the policies and procedures that should be implemented based on prioritized disruptions identified and their resulting impact on the institution.

The risk assessment step is critical and has significant bearing on whether business continuity planning efforts will be successful. During the risk assessment step, business processes and the BIA assumptions are evaluated using various threat scenarios. [12] This will result in a range of outcomes that may require changes to the BCP.

Financial institutions should develop realistic threat scenarios that may potentially disrupt business processes and their ability to meet clients' expectations (internal, business partners, or customers). Threats can take many forms, including malicious activity, natural and technical disasters, and pandemic incidents. [13] Where possible, institutions should analyze a threat by using non-specific, all-risk planning that focuses on the impact of the threat instead of the nature of the threat. For example, the effects of certain threat scenarios can include business disruptions that affect only specific personnel, 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, the resulting BCP may be too basic and omit reasonable steps that are needed for a timely recovery after a disruption.

Threat scenarios should consider the severity of the disaster, which is based upon the impact and the probability of business disruptions resulting from identified threats. Threats may range from those with a high probability of occurrence and low impact to the institution, such as brief power interruptions, to those with a low probability of occurrence and high impact to the institution, such as hurricanes or terrorist attacks. The most difficult threats to address are those that have a high impact on the institution but a low probability of occurrence. However, through the use of non-specific, all-risk planning, the BCP may be more flexible and adaptable to all types of disruptions.

When assessing the probability of a disruption, financial institutions and technology service providers should consider the geographic location of all facilities, their susceptibility to threats (e.g., location in a flood plain), and the proximity to critical infrastructures (e.g., power sources, nuclear power plants, airports, major highways, railroads). Worst-case scenarios, such as destruction of the facilities and loss of life, should be considered. As part of this process, external factors should also be closely monitored to determine the probability of occurrence. External factors can be monitored through constant communication with community and government officials and regulatory authorities. For example, institutions should monitor alerts issued by such organizations as the Department of Homeland Security and the World Health Organization, which provide information regarding terrorist activity and environmental risks, respectively.

After analyzing the impact, probability, and the resulting severity of identified threats, the institution can prioritize business processes and estimate how they could be disrupted under various threat scenarios. The resulting probability of occurrence may be based on a rating system of high, medium, and low.

At this point in the business continuity planning process, the financial institution should perform a "gap analysis." In this context, a "gap analysis" is a methodical comparison of what types of policies and procedures the institution (or business line) should implement to recover, resume, and maintain normal business operations, versus what the existing BCP provides. The difference between the two highlights additional risk exposure that management should address when developing the BCP.

Risk Management

Business Continuity Plan Development

Action Summary

Risk management represents the third step in the business continuity planning process. It is defined as the process of identifying, assessing, and reducing risk to an acceptable level through the development, implementation, and maintenance of a written, enterprise-wide BCP. The BCP should be:

- Based on a comprehensive BIA and risk assessment;
- Documented in a written program;
- Reviewed and approved by the board and senior management at least annually;
- Disseminated to financial institution employees;
- Properly managed when the maintenance and development of the BCP is outsourced to a third-party;
- Specific regarding what conditions should prompt implementation of the plan and the process for invoking the BCP;
- Specific regarding what immediate steps should be taken during a disruption;
- Flexible to respond to unanticipated threat scenarios and changing internal conditions;
- Focused on the impact of various threats that could potentially disrupt operations rather than on specific events;
- Developed based on valid assumptions and an analysis of interdependencies; and
- Effective in minimizing service disruptions and financial loss through the implementation of mitigation strategies.

The BIA and risk assessment represent the foundation of the BCP. The BCP should be written on an enterprise-wide basis, reviewed and approved by the board and senior management at least annually, and disseminated to financial institution employees for timely implementation. [14] All financial institutions should develop a BCP that documents business continuity strategies and procedures to recover, resume, and maintain all critical business functions and processes.

Some financial institutions may choose to develop their BCP internally, while others may

choose to outsource the development and maintenance of their BCP. While outsourcing BCP development may be a viable option, the board and management are ultimately responsible for implementing and maintaining a comprehensive BCP. Therefore, financial institution management should understand the business impact of potential threats, have the ability to implement mitigating controls, and ensure that the BCP can be properly executed by financial institution personnel and validated through comprehensive testing. When outsourcing BCP development, management should ensure that the chosen service provider has the expertise required to analyze the financial institution's business needs. The service provider should also be able to design executable strategies that are relevant to the financial institution's risk environment, create education and training programs necessary to achieve successful deployment of the BCP, and integrate necessary changes so that the BCP is properly updated.

A well-written BCP should describe the various types of events that could prompt the formal declaration of a disaster and the process for invoking the BCP. It should also describe the responsibilities and procedures to be followed by each continuity team, have current contact lists of critical personnel, address communication processes for internal and external stakeholders, identify relocation strategies to alternate facilities, and include procedures for approving unanticipated expenses.

The BCP should specifically describe the immediate steps to be taken during a disruption in order to maintain the safety of personnel and minimize the damage incurred by the institution. The BCP should include procedures to execute the plan's priorities for critical versus non-critical functions, services, and processes. Specific procedures to follow for recovery of each critical business function should be developed so that employees understand their role in the recovery process and can implement the BCP in a timely manner.

The BIA and risk assessment should be integrated into the written BCP by incorporating identified changes in internal and external conditions and the impact of various threats that could potentially disrupt operations rather than on specific events that may never occur. Examples of the potential impact of various threats include the following:

- Critical personnel are unavailable and they cannot be contacted;
- Critical buildings, facilities, or geographic regions are not accessible;
- Equipment (hardware) has malfunctioned or is destroyed;
- Software and data are not accessible or are corrupted;
- Third-party services are not available;
- Utilities are not available (power, telecommunications, etc.);
- Liquidity needs cannot be met; and
- Vital records are not available.

Assumptions

When developing the BCP, 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. Additionally, institutions should not assume they will be able to gain access to facilities or that critical personnel (including senior management) will be available immediately after the disruption. Public transportation systems such as airlines, railroads, and subways also may not be operating, and telecommunication systems may be overburdened and unavailable.

Internal and External Components

A BCP consists of many components that are both internal and external to a financial institution. An effective BCP coordinates across its many components, identifies potential process or system dependencies, and mitigates the risks from interdependencies.Refer to Appendix C: "Internal and External Threats"; Appendix E: "Interdependencies"; and Appendix G: "Business Continuity Plan Components" for additional information. The activation of a continuity plan and restoration of business in the event of an emergency depends on the successful interaction of these various components. The overall strength and effectiveness of a BCP can be decreased by its weakest component. Internal components that should be addressed in the BCP to ensure adequate recovery of business operations may include interdependencies between various departments, business functions, and personnel within the institution. These interdependencies can also include single points of failure with internal telecommunications and computer systems. External components that can negatively affect the timely recovery of business operations and that should be addressed in the BCP may include interdependencies with telecommunications providers, service providers, customers, business partners, and suppliers.

Mitigation Strategies

Management should develop comprehensive mitigation strategies to resolve potential problems that may result from internal and external interdependencies. Mitigation strategies will depend upon the results of the BIA and risk assessment, but should always ensure that processing priorities can be adequately implemented and that business operations can be resumed in a timely manner. The following represent examples of appropriate mitigation strategies:

- Strengthening the physical facility using dependable construction materials;
- Establishing redundant vendor support;
- Establishing media protection safeguards and comprehensive data back-up procedures;
- Implementing redundant or alternative power sources, communication links, data back-up technologies, and data recovery methods;

- Increasing inventories of critical equipment;
- Installing fire detection and suppression systems; and
- Purchasing and maintaining adequate reserves of food, water, batteries, and medical supplies.

Once the BCP is complete, the viability of the plan must be assessed as part of the risk monitoring and testing step, which involves the development, execution, evaluation, and assessment of a testing program. The testing program is then used to update the BCP based on issues identified as part of the testing process.

Risk Monitoring and Testing

Principles of the Business Continuity Testing Program

Action Summary

Risk monitoring and testing is the final step in the cyclical business continuity planning process. Risk monitoring and testing ensures that the institution's business continuity planning process remains viable through the:

- Incorporation of the BIA and risk assessment into the BCP and testing program;
- Development of an enterprise-wide testing program;
- Assignment of roles and responsibilities for implementation of the testing program;
- Completion of annual, or more frequent, tests of the BCP;
- Evaluation of the testing program and the test results by senior management and the board;
- Assessment of the testing program and test results by an independent party; and
- Revision of the BCP and testing program based upon changes in business operations, audit and examination recommendations, and test results.

Risk monitoring and testing is necessary to ensure that the business continuity planning process remains viable through the incorporation of the BIA and risk assessment into an enterprise-wide BCP and testing program. The testing program has become a key focus of banking supervisors, in light of recent, catastrophic events, and has received heightened attention within the financial services industry because such a program can

be used to validate the viability of the BCP. As such, there are various principles that should be followed by financial institutions when developing a testing program.

The following principles should be addressed in the business continuity testing program of all institutions, regardless of whether they rely on service providers or process their work internally:

- Roles and responsibilities for implementation and evaluation of the testing program should be specifically defined;
- The BIA and risk assessment should serve as the foundation of the testing program, as well as the BCP that it validates;
- The breadth and depth of testing activities should be commensurate with the importance of the business process to the institution, as well as to critical financial markets;
- Enterprise-wide testing should be conducted at least annually, or more frequently, depending on changes in the operating environment;
- Testing should be viewed as a continuously evolving cycle, and institutions should work towards a more comprehensive and integrated program that incorporates the testing of various interdependencies; [15]
- Institutions should demonstrate, through testing, that their business continuity arrangements have the ability to sustain the business until permanent operations are reestablished;
- The testing program should be reviewed by an independent party; and
- Test results should be compared against the BCP to identify any gaps between the testing program and business continuity guidelines, with notable revisions incorporated into the testing program or the BCP, as deemed necessary.

A key challenge for management is to develop a testing program that provides a high degree of assurance for the continuity of critical business processes, including supporting infrastructure, systems, and applications, without compromising production environments. Therefore, a robust testing program should incorporate roles and responsibilities; a testing policy that includes testing strategies and test planning; the execution, evaluation, independent assessment, and reporting of test results; and updates to the BCP and testing program.

Roles and Responsibilities

The board and senior management are responsible for establishing and reviewing an enterprise-wide testing program. Once the program is established, they direct the

following groups to develop, implement, and evaluate the institution's business continuity testing program.A detailed discussion of roles and responsibilities can be found in Appendix H: "Testing Program - Governance and Attributes."

- Business line management, who has ownership and accountability for the testing of business operations;
- IT management, who has ownership and accountability for testing recovery of the institution's information technology systems, infrastructure, and telecommunications;
- Crisis management, who has ownership and accountability for testing the institution's event management processes;
- Facilities management, who has ownership and accountability for testing the operational readiness of the institution's physical plant and equipment, environmental controls, and physical security; and
- The internal auditor (or other qualified independent party), who has the responsibility for evaluating the overall quality of the testing program and the test results.

Testing Policy

An enterprise-wide business continuity testing policy should be established by the board and senior management and should set expectations for business lines and support functions to follow in implementing testing strategies and test plans. The policy should establish a testing cycle that increases in scope and complexity over time. As such, the testing policy should continuously improve by adapting to changes in business conditions and supporting expanded integration testing.

The testing policy should incorporate the use of a BIA and risk assessment for developing enterprise-wide and business line continuity testing strategies. The policy should identify key roles and responsibilities and establish minimum requirements for the institution's business continuity testing, including baseline requirements for frequency, scope, and reporting test results.

Testing policies will vary depending on the size and risk profile of the institution. While all institutions should develop testing policies on an enterprise-wide basis and involve essential employees in the testing process, some considerations differ depending on whether the institution relies on service providers (serviced institutions) or whether it processes its work internally (in-house).

A serviced institution's testing policy should include guidelines addressing tests between the financial institution and its service provider.Refer to the following guidance included in the FFIEC IT Examination Handbook for additional information: June 2004 "Outsourcing Technology Services Booklet" in the section entitled, Related Topics, and the June 2004 "Management Booklet" in the section entitled, Management Considerations for Technology Service Providers. Serviced institutions should test communication and connectivity procedures to be followed when either the financial institution's or service provider's systems, at their primary or alternate sites, are inoperable. Serviced institutions should participate in tests with their critical service providers to ensure that institution employees fully understand the recovery process.

The testing policy for in-house institutions should address the active involvement of personnel when systems and data files are tested. In-house institutions often send their back-up media to a recovery site to be processed by the back-up service provider's employees. This is not a sufficient test of an institution's BCP and is considered ineffective because financial institution employees are not directly involved in the testing process. As a result, the institution cannot verify that tests were conducted properly and institution personnel may not be familiar with recovery procedures and related logistics in the event of a true disaster.

Once an institution develops the testing policy, this policy is typically implemented through the development of testing strategies that include the testing scope and objectives and test planning using various scenarios and testing methods.

Testing Strategies

The testing policy should include enterprise-wide testing strategies that establish expectations for individual business linesBusiness lines include all internal and external supporting functions, such as IT and facilities management. across the testing life cycle of planning, execution, measurement, reporting, and test process improvement. The testing strategy should include the following:

- Expectations for business lines and support functions to demonstrate the achievement of business continuity test objectives consistent with the BIA and risk assessment;
- A description of the depth and breadth of testing to be accomplished;
- The involvement of staff, technology, and facilities;
- Expectations for testing internal and external interdependencies; and
- An evaluation of the reasonableness of assumptions used in developing the testing strategy.

Testing strategies should include the testing scope and objectives, which 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 business continuity planning process is accurate, relevant, and viable under adverse conditions. Therefore, the business continuity planning process should be tested at least annually, with more frequent testing required when significant changes have occurred in business operations. Testing should include applications and business functions that were identified during the BIA. The BIA determines the recovery point objectives and recovery time objectives, which then help determine the appropriate recovery strategy. Validation of the RPOs and RTOs is important to ensure that they are attainable

Testing objectives should start simply, and gradually increase in complexity and scope. The scope of individual tests can be continually expanded to eventually encompass enterprise-wide testing and testing with vendors and key market participants. Achieving the following objectives provides progressive levels of assurance and confidence in the plan. At a minimum, the testing scope and objectives 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 testing procedures can be revised;
- Consider deviating from the test script to interject unplanned events, such as the loss of key individuals or services; and
- Involve a sufficient volume of all types of transactions to ensure adequate capacity and functionality of the recovery facility.

Test Planning

The testing policy should also include test planning, which is based on the predefined testing scope and objectives established as part of management's testing strategies. Test planning includes test plan review procedures and the development of various testing scenarios and methods. Management should evaluate the risks and merits of various types of testing scenarios and develop test plans based on identified recovery needs. Test plans should identify quantifiable measurements of each test objective and should be reviewed prior to the test to ensure they can be implemented as designed. Test scenarios should include a variety of threats, event types, and crisis management situations and should vary from isolated system failures to wide-scale disruptions. Scenarios should also promote testing alternate facilities with the primary and alternate facilities of key counterparties and third-party service providers. Comprehensive test scenarios focus attention on dependencies, both internal and external, between critical business functions, information systems, and networks.Integrated testing moves beyond the testing of individual components, to include testing with internal and external parties and the supporting systems, processes, and resources. Refer to Appendix E: "Interdependencies" and Appendix H: "Testing Program - Governance and Attributes" for additional information. As such, test plans should include scenarios addressing local and wide-scale disruptions, as appropriate. Business line management should develop scenarios to effectively test internal and external interdependencies, with the assistance of IT staff members who are knowledgeable regarding application data flows and other areas of vulnerability. Institutions should periodically reassess and update their test scenarios to reflect changes in the institution's business and operating environment.

Test plans should clearly communicate the predefined test scope and objectives and provide participants with relevant information, including:

- A master test schedule that encompasses all test objectives;
- Specific description of test objectives and methods;
- Roles and responsibilities for all test participants, including support staff;
- Designation of test participants;

- Test decision makers and succession plans;
- Test locations; and
- Test escalation conditions and test contact information.

Test Plan Review

Management should prepare and review a scriptRefer to Appendix H: "Testing Program - Governance and Attributes" for additional information on test scripts. 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 affect a critical business function. In addition, as a preliminary step to the testing process, management should perform a thorough review of the BCP (checklist review). A checklist review involves distributing copies of the BCP to the managers of each critical business unit and requesting that they review portions of the plan applicable to their department to ensure that the procedures are comprehensive and complete.

Testing Methods

Testing methods can vary from simple to complex depending on the preparation and resources required. Each bears its own characteristics, objectives, and benefits. The type or combination of testing methods employed by a financial institution should be determined by, among other things, the institution's age and experience with business continuity planning, size, complexity, and the nature of its business.

Testing methods include both business recovery and disaster recovery exercises. Business recovery exercises primarily focus on testing business line operations, while disaster recovery exercises focus on testing the continuity of technology components, including systems, networks, applications, and data. To test split processing configurations, in which two or more sites support part of a business line's workload, tests should include the transfer of work among processing sites to demonstrate that alternate sites can effectively support customer-specific requirements and work volumes and site-specific business processes. A comprehensive test should involve processing a full day's work at peak volumes to ensure that equipment capacity is available and that RTOs and RPOs can be achieved.

More rigorous testing methods and greater frequency of testing provide greater confidence in the continuity of business functions. While comprehensive tests do require greater investments of time, resources, and coordination to implement, detailed testing will more accurately depict a true disaster and will assist management in assessing the actual responsiveness of the individuals involved in the recovery process. Furthermore, comprehensive testing of all critical functions and applications will allow management to identify potential problems; therefore, management should use one of the more thorough testing methods discussed in this section to ensure the viability of the BCP before a disaster occurs. Examples of testing methods in order of increasing complexity include:

Tabletop Exercise/Structured Walk-Through Test

A tabletop exercise/structured walk-through test is considered a preliminary step in the overall testing process and may be used as an effective training tool; however, it is not a

preferred testing method. Its primary objective is to ensure that critical personnel from all areas are familiar with the BCP and that the plan accurately reflects the financial institution's ability to recover from a disaster. It is characterized by:

- Attendance of business unit management representatives and employees who play a critical role in the BCP process;
- Discussion about each person's responsibilities as defined by the BCP;
- Individual and team training, which includes a walk-through of the step-by-step procedures outlined in the BCP; and
- Clarification and highlighting of critical plan elements, as well as problems noted during testing.

Walk-Through Drill/Simulation Test

A walk-through drill/simulation test is somewhat more involved than a tabletop exercise/ structured walk-through test because the participants choose a specific event scenario and apply the BCP to it. However, this test also represents a preliminary step in the overall testing process that may be used for training employees, but it is not a preferred testing methodology. It includes:

- Attendance by all operational and support personnel who are responsible for implementing the BCP procedures;
- Practice and validation of specific functional response capabilities;
- Focus on the demonstration of knowledge and skills, as well as team interaction and decision-making capabilities;
- 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 without performing actual recovery processing; and
- Varying degrees of actual, as opposed to simulated, notification and resource mobilization to reinforce the content and logic of the plan.

Functional Drill/Parallel Test

Functional drill/parallel testing is the first type of test that involves the actual mobilization of personnel to other sites in an attempt to establish communications and perform actual recovery processing as set forth in the BCP. The goal is to determine whether critical systems can be recovered at the alternate processing site and if employees can actually deploy the procedures defined in the BCP. It includes:

- A full test of the BCP, which involves all employees;
- Demonstration of emergency management capabilities of several groups practicing a series of interactive functions, such as direction, control, assessment, operations, and planning;
- Testing medical response and warning procedures;
- Actual or simulated response to alternate locations or facilities using actual communications capabilities;
- Mobilization of personnel and resources at varied geographical sites, including evacuation drills in which employees test the evacuation route and procedures for personnel accountability; and
- Varying degrees of actual, as opposed to simulated, notification and resource mobilization in which parallel processing is performed and transactions are compared to production results.

Full-Interruption/Full-Scale Test

Full-interruption/full-scale test is the most comprehensive type of test. In a full-scale test, a real-life emergency is simulated as closely as possible. Therefore, comprehensive planning should be a prerequisite to this type of test to ensure that business operations are not negatively affected. The institution implements all or portions of its BCP by processing data and transactions using back-up media at the recovery site. It involves:

- Enterprise-wide participation and interaction of internal and external management response teams with full involvement of external organizations;
- 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;
- Actual processing of data using 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 to allow realistic role-playing of all the involved groups.

Execution, Evaluation, Independent Assessment, and Reporting of Test Results

Once testing strategies and test plans are developed, the following procedures should be implemented as part of the overall testing policy:

Execution and Documentation

Testing requires centralized coordination by the BCP coordinator or team. The team or coordinator is responsible for overseeing the accomplishment of targeted objectives and ensuring the test results are appropriately documented.

Generally, it is advisable to have the maximum number of personnel involved in implementing the BCP to also participate in the test. Management should also rotate personnel periodically during the testing process to reduce dependence on specific individuals who may leave the organization or may not be available during a disaster. This participation increases awareness and ownership in achieving successful BCP implementation.

Once the tests are executed, test results should be properly documented and include the following, at a minimum:

- Test dates and locations;
- An executive summary detailing a comparison between the test objectives and test results;
- Material deviations from the test plans, including whether intended participation levels were achieved;
- Problems identified during testing; and
- An evaluation by a qualified independent party.

Evaluation

Once tests have been executed and documented, test results should be evaluated to ensure that test objectives are achieved and that business continuity successes, failures, and lessons learned are thoroughly analyzed. Business lines and support function management should review test results to validate whether test procedures were effectively completed and adequately documented. Finally, test results, including quantitative metrics, such as achieving RTOs and RPOs, should be used to determine the effectiveness of the institution's BCP. If test objectives were not achieved, business line and support function management should identify necessary corrective measures and determine whether a follow-up test should be conducted prior to the next regularly scheduled exercise. Exceptions to this process should be documented and approved by senior management.

Institutions are expected to evaluate testing across business lines and support functions in order to validate the BCP. An analysis of tests completed over a period of time should be conducted to determine whether the institution is capable of achieving its overall business continuity objectives.

Independent Assessment

Key tests should be observed, verified, and evaluated by independent parties. This provides assurance to the board and other stakeholders of the validity of the testing process and the accuracy of test results. This independent assessment is typically conducted by internal audit, although it can be performed by other qualified third parties. An effective practice is to include a review by both business line and IT auditors. This review should include an assessment of the testing scope and objectives, written test plans, testing methods and schedules, and communication of test results and recommendations to the board. The analysis of underlying assumptions and the results of modeling and simulation techniques should also be independently assessed to assure the board and other stakeholders of their reasonableness and validity. In addition, the board should receive and review audit reports addressing the effectiveness of the institution's process for identifying and correcting areas of weakness, and audit recommendations should be monitored to ensure that they are implemented in a timely manner.

Reporting Test Results

Test results, gaps between the BCP and the actual test results, and the resolution of any problems should be reported to several audiences, including the board and senior management, business line management, risk management, IT management, and other stakeholders. A management assessment of the institution's ability to meet its continuity objectives and testing program requirements should be provided to the board at least annually. The assessment should contain sufficient information so that the board can determine if the BCP meets the objectives established by the BIA. In addition, business lines and support functions should identify the validity of the test data processed, any untested aspects of production operations, and the need for additional tests. The board should receive reports more frequently when test results for critical business lines indicate an inability to meet continuity objectives.

Updating Business Continuity Plan and Test Program

After the test results are executed, evaluated by management, independently assessed, and reported to the board, it may be necessary to update the BCP and test program. As part of this process, the BCP and test program should be reviewed by senior management, the planning team or coordinator, team members, and the board at least annually. 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. If significant changes have occurred in the business environment, or if audit findings warrant changes to the BCP or test program, the business continuity policy guidelines and program requirements should be updated accordingly. In addition, an independent assessment of the revised BCP and test program should be performed by an auditor to ensure that both are comprehensive and updated based on the institution's risk profile and test results.

The process of updating the BCP and the test program requires management to document, track, and ultimately resolve any necessary changes by revising the BCP, the test program, or conducting additional tests, if deemed necessary.

Issue Tracking, Resolution and Continuity Update

Test owners, typically business line or support management, should assign responsibility

for resolution of material business continuity problems identified during testing and should track issues to ensure that they are effectively addressed in a timely manner. Issues requiring resolution may stem from a number of factors, including changes in internal or external dependencies involving staff, technology, facilities, and third parties. Test results and issues should be periodically analyzed to determine whether problems encountered during testing could be traced to a common source, such as inadequate change control procedures. Software applications are commercially available to assist the BCP coordinator in identifying and tracking changes so that the BCP can be appropriately updated. Once the BCP is updated, the financial institution should ensure that the revised BCP is distributed throughout the organization.

Updating Test Program and Re-Testing

Once tests have been completed, documented, and assessed, the test program should be updated to address any gaps identified during the tests. Suggestions for improving test scenarios, plans, or scripts provided by test participants should be incorporated into the testing cycle. In the event that tests do not succeed in meeting their required objectives, management should determine whether it is necessary to re-test prior to the next scheduled test. Failure to meet significant test objectives for critical business functions requires management to address re-testing based on the risk to the institution.

Other Policies, Standards and Processes

Action Summary

The following policies, standards, and processes should be integrated into the business continuity planning process:

- Security Standards;
- Project Management;
- Change Control Policies;
- Data Synchronization Procedures;
- Crises Management;
- Incident Response;
- Remote Access;
- Employee Training;
- Notification Standards;
- Insurance; and
- Government and Community.

Security Standards

Security standards should be an integral part of the entire business continuity planning process. During a disaster, security becomes very important due to potential changes in the working environment, personnel, and equipment. Consequently, different security risks will emerge that should be considered during the risk assessment process. Ultimately, mitigating strategies should incorporate the various risks identified to ensure that adequate security controls are in place if an event triggers the implementation of the BCP. Additionally, security standards should be incorporated into the BCP training and testing program.Refer to the "Information Security Booklet" included in the FFIEC IT Examination Handbook for additional information.

Project Management

Project management should incorporate business continuity considerations. Evaluating business continuity needs during the planning stages of a project will allow management to determine compliance with business continuity requirements prior to implementation and to make adjustments in acquisition or development plans accordingly. In addition, advance project planning facilitates the development of a more robust system that supports the institutions business strategy and business continuity objectives. During the project initiation stage, project plans should address the following issues at a minimum:For additional information refer to the "Development and Acquisition Booklet" included in the FFIEC IT Examination Handbook.

- Business unit requirements for resumption and recovery alternatives;
- Information on back-up and storage;
- Hardware and software requirements at recovery locations;
- Maintenance of documentation supporting project decisions;
- Disaster recovery testing; and
- Staffing and facilities.

Change Control Policies

To maintain the viability of the BCP, change control policies should address potential changes to the operating environment. When a change is made to an application, operating system, or utility in the production environment, a methodology should exist to ensure that all back-up copies of those systems are also updated. In addition, if a new or changed system is implemented and results in new hardware, new capacity requirements, or other technology changes, management should ensure that the BCP is updated and the recovery site can support the new production environment. Change control policies should also allow for changes to be implemented quickly in the event of an emergency; however, these changes should still be properly monitored and

documented.

Data Synchronization Procedures

Data synchronization processes should include business continuity considerations due to the potential challenges that emerge when dealing with an active environment. The larger or more complex an institution is (i.e., shorter acceptable operational outage period, greater volume of data, and greater distances between primary and back-up locations), 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. In some situations, the data latency may be seconds, minutes or even hours; therefore, reconciliation procedures should be established to ensure that post-disaster data is accurate. Additionally, testing of contingency arrangements is critical to ensure that data can be synchronized with the primary work environment within a reasonable amount of time.

Crisis Management

Business continuity planning should include the development of a crisis management team and crisis management process. The crisis management team is typically responsible for the actual declaration of an event, and its duties internally are to implement the BCP and externally to deal with outside agencies, government offices, and emergency communications. The team should include a cross section of individuals from various departments throughout the financial institution, including senior management (decision making), facilities management (locations and safety), human resources (personnel issues and travel), marketing (media contact), finance/accounting (funds disbursement and financial decisions), and any other area appropriate for the institution. The key to a good crisis management team is in the planning. Individuals should be able to make instantaneous decisions, possibly based on limited information, often without the support of others. Each recovery scenario requires a specific media plan and notification plan as well. The BCP allows the institution to recover critical business operations, and the crisis management team deals with the crisis at hand. A crisis management test can be used to validate the overall process, including disaster declaration and escalation procedures.

Incident Response

Every financial institution should develop an incident response policy that is properly integrated into the business continuity planning process. A security incident represents the attempted or successful unauthorized access, use, modification, or destruction of information systems or customer data. If unauthorized access occurs, the financial institution's computer systems could potentially fail and confidential information could be compromised. In the event of a security incident, management must decide how to properly protect information systems and confidential data while also maintaining business continuity. Management's ultimate goal should be to minimize damage to the institution and its customers through containment of the incident and proper restoration

of information systems. A key element of incident response involves assigning responsibility for evaluating, responding, and managing security incidents and developing guidelines for employees to follow regarding escalation and reporting procedures. Management should determine who will be responsible for declaring an incident and restoring affected computer systems once the incident is resolved. Individuals who are assigned this responsibility should have the expertise and training necessary to quickly respond in an appropriate manner. Financial institutions should assess the adequacy of their preparation by testing incident response guidelines to ensure that the procedures correspond with business continuity strategies.

Remote Access

Remote access policies and standards should be established as an important part of BCP implementation. In the event of a disaster, personnel may be able to work from a remote location and vendors may be allowed remote access to back-up facilities. As such, remote access guidelines should be developed addressing acceptable configuration and software requirements for certain remote devices that may introduce security risks. Remote access policies should address various security guidelines including prior management approval requirements, controls for third-party access, and virus controls. If employees are allowed to use personal computers for remote access during a disaster, management should ensure that only secure connections are used e.g., VPN. In addition, clear guidance should be established and disseminated to employees regarding appropriate procedures to follow when accessing or transmitting confidential information from a remote location.

Employee Training

Financial institutions should provide business continuity training for personnel to ensure that all parties are aware of their primary and back-up responsibilities should a disaster occur. Key employees should be involved in the business continuity development process as well as periodic tests and 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 the BCP 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 used to anticipate restoring operations in the absence of key employees. Employee training should be regularly scheduled and updated to address changes to the BCP.

Notification Standards

Formal notification standards should be developed and integrated into the business continuity planning process. Various communication methods, such as pagers, satellite phones, cell phones, e-mail, or two-way radios, can be used to promptly notify employees and applicable third parties of a disaster situation. Comprehensive notification standards should address the maintenance and distribution of contact lists that include primary phone numbers, emergency phone numbers, e-mail addresses, and physical addresses of institution personnel, vendors, emergency services, transportation

companies, and regulatory agencies. As part of this process, employee evacuation plans should be documented to ensure that financial institution management knows where employees plan to relocate and how to contact employees during an emergency. Reporting or calling locations should also be established to ensure that institution personnel are accounted for and that employees are trained to understand post-disaster communication procedures.

Various methods can be used to distribute this information, such as wallet cards, Intranet postings, e-mail messages, cell phone text messages, and calling trees. Many financial institutions work with their human resources departments to ensure that accurate contact records are properly updated and that personal information is securely maintained. Management should ensure that contact information is readily accessible during a disaster by maintaining copies at off-site locations.

Notification standards should also include an awareness program to ensure that customers, service providers, and regulators know how to contact the institution if normal communication channels are inoperable. Financial institution management should designate a media contact to communicate with these outside parties and employees should be properly trained to refer any inquiries to appropriate personnel.

Insurance

Insurance is an important component of the business continuity planning process. While insurance is not a substitute for an effective BCP, it may allow management to recover losses that cannot be completely prevented and expenses related to recovering from a disaster. Generally, insurance coverage is obtained for risks that cannot be entirely controlled, yet represent a potential for financial loss or other disastrous consequences. While the decision to obtain insurance is based on several factors, one consideration should be the probability and degree of loss identified during the BIA. Financial institutions should determine potential exposure based on various exclusions, deductibles, limits, and riders. Available insurance options should be reviewed to ensure that appropriate insurance coverage is provided given the risk profile of the institution. Institutions should perform an annual insurance review to ensure that the level and types of coverage are commercially reasonable and consistent with any legal, management, and board requirements.

Insurance can reimburse an institution for some or all of the financial losses incurred as the result of a disaster or other significant event. To facilitate the claims process, institutions should create and retain a comprehensive hardware and software inventory list in a secure off-site location and detailed expenses should be documented to support insurance claims.

Government and Community

An institution should establish an on-going relationship with community and government officials and the news media to ensure the successful implementation of the BCP. Since financial institutions must often compete with the restoration of other critical components in the area, some institutions and emergency staff located in close geographic proximity have formed coalitions to discuss business continuity planning issues and to facilitate critical infrastructure planning efforts. Ideally, these relationships should be initially

established during the planning or testing phases of business continuity planning so institution management understands the proper protocol required if a citywide or region-wide event affects 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 and the availability of power and telecommunications systems should be coordinated with various entities to ensure timely resumption of operations. Facilities access should be coordinated with the police and fire department, local and state government agencies, and, depending on the nature and extent of the disaster, possibly the Federal Emergency Management Agency (FEMA).

Summary

In summary, the following factors represent critical aspects of an effective business continuity planning process:

- The effectiveness of business continuity planning depends upon the involvement of the board and senior management;
- Business continuity planning involves a continuous, process-oriented approach that includes a BIA, a risk assessment, risk management, and risk monitoring and testing;
- A thorough BIA and risk assessment should form the foundation of a comprehensive BCP;
- The BCP and testing program should be developed on an enterprise-wide basis;
- The effectiveness of the BCP should be validated through annual, or more frequent, testing;
- The BCP and test program should be thoroughly documented, evaluated by institution management, independently reviewed by an internal and/or external audit function, and reported to the board;
- The BCP and test program should be updated to reflect and respond to changes in the institution and gaps identified during continuity testing; and
- In addition to the BCP, other financial institution policies, standards, and processes should be integrated into the business continuity planning process.

Endnotes

[1]	This booklet uses the terms "institution" and "financial institution" to describe insured banks, thrifts, and credit unions, as well as technology service providers 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 the Office of Thrift Supervision.
[3]	Refer to the "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System," issued by the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission.
[4]	Refer to Appendix F: "Business Impact Analysis Process" for additional information.
[5]	Refer to Appendix C: "Internal and External Threats," Appendix D: "Pandemic Planning," Appendix E: "Interdependencies" and Appendix F: "Business Impact Analysis Process" for additional information.
[6]	Refer to Appendix G: "Business Continuity Plan Components."
[7]	Refer to Appendix H: "Testing Program - Governance and Attributes" for additional information.
[8]	Refer to the "Interagency Guidelines Establishing Information Security Standards," Board of Governors of the Federal Reserve System, 12 CFR part 208, Appendix D-2, and 12 CFR part 225, Appendix F; Federal Deposit Insurance Corporation, 12 CFR part 364, Appendix B; National Credit Union Administration, 12 CFR part 748, Appendix A & B; Office of the Comptroller of the Currency, 12 CFR part 30, Appendix B; Office of Thrift Supervision, 12 CFR part 570, Appendix B, for additional information.
[9]	Refer to Appendix F: "Business Impact Analysis Process" for additional information.
[10]	Refer to the "Information Security Booklet" included in the Federal Financial Institutions Examination Council IT Examination Handbook for additional information.
[11]	Refer to the "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 Closing Notices and Policies," Volume 64 Federal Register, page 34844 (June 29, 1999); "Establishment and Relocation of Domestic Branches and Offices," Board of Governors of the Federal Reserve System, 12 CFR Part 208.6; Federal Deposit Insurance Corporation, 12 CFR Part 303.44; Office of the Comptroller of the Currency, 12 CFR Part 5.30; and Office of Thrift Supervision, 12 CFR Part 545.95.

[12]	Refer to Appendix F: "Business Impact Analysis Process" for additional information.
[13]	Refer to Appendix C: "Internal and External Threats" and Appendix D: "Pandemic Planning" for additional information
[14]	Refer to Appendix G: "Business Continuity Plan Components" for additional information.
[15]	Integrated testing includes testing with internal and external parties and the supporting systems, processes, and resources. A discussion of interdependencies can be found in Appendix E: "Interdependencies." Related testing guidance is included in Appendix H: "Testing Program - Governance and Attributes."
[16]	As evidenced by Hurricane Katrina, while the duration of a specific natural disaster may be relatively brief, the social and economic recovery from such events can be prolonged.
[17]	The World Health Organization (WHO) tracks the status of virus transmission using a six phase scale; the U.S. Government uses a six stage scale that has a geographic focus. Financial institutions should be familiar with and monitor both sources.
[18]	A planning assumption from The Implementation Plan for the National Strategy for Pandemic Influenza is that rates of absenteeism will depend on the severity of the pandemic. In a severe pandemic, absenteeism attributable to illness, the need to care for ill family members, and fear of infection may reach 40 percent during the peak weeks of a community outbreak, with lower rates of absenteeism during the weeks before and after the peak. Certain public health measures (closing schools, quarantining household contacts of infected individuals, "snow days") are likely to increase rates of absenteeism.
[19]	See References at the end of this Appendix for specific U.S. Government and industry association guides covering pandemic planning.
[20]	The Department of Homeland Security (DHS) Continuity of Operations - Essential (COP-E) planning process may be useful here. It is contained in the Pan-demic Influenza Preparedness, Response, and Recovery Guide and is available at: http://www.pandemicflu.gov.
[21]	See The National Implementation Plan at http://www.pandemicflu.gov/plan/community/commitigation.html.
[22]	See The National Implementation Plan at http://www.pandemicflu.gov/plan/community/commitigation.html.
[23]	FFIEC IT Examination Handbook's "Outsourcing Technology Services Booklet", /ITBooklets/FFIEC_ITBooklet_OutsourcingTechnologyServices.pdf.

[24]	Refer to "Introduction" and "Business Continuity Planning Process" sections of this booklet.
[25]	See the "Third-Party Capacity" section below.
[26]	See the FFIEC IT Examination Handbook's "Outsourcing Technology Services Booklet, " /ITBooklets/FFIEC_ITBooklet_OutsourcingTechnologyServices.pdfor comprehensive information on contract provisions.
[27]	See the "Risk Monitoring and Testing" section of this booklet.
[28]	Refer to the "Testing With Third-Party TSPs" section below.
[29]	This includes internal and outsourced audit reports, reports issued by regulatory agencies, and other independent assessments, such as consulting reports, penetration tests, and vulnerability assessments.
[30]	MIS reports include, for example, compliance with SLAs, TSP risk mitigation capabilities, or mediation timeframes.
[31]	This concept is equally applicable to a situation where operations are moved to an alternate data center owned by the same service provider.
[32]	See Appendix H, "Testing Program - Governance and Attributes."
[33]	Proxy testing is a term used to refer to testing that is conducted on like systems and with like interfaces for the purpose of not having to repeat similar tests that should provide similar results. Proxy tests are conducted using the same hardware and operating software and are sometimes used as a replacement for actual tests.
[34]	A zero-day threat exploits previously undiscovered vulnerabilities for which a software patch or other mitigating control is not yet available.
[35]	Hardening software and operating systems is intended to eliminate security risks and includes activities such as configuration management, security patch management, and the removal of all unnecessary programs and utilities.
[36]	FFIEC IT Examination Handbook's "Information Security Booklet," /ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf.
[37]	Cloud-based disaster recovery services employ virtualization, disk backup, and data replication technologies to provide financial institutions and their service providers with low-latency, diversified, and cost-effective offsite backup, recovery, and restoration services. The term "cloud" refers to the fact that the internal architecture of these services is abstracted from the customer.

[38]	Virtualization technology involves one physical computer running virtualization software that may contain two or more "virtual machines" that process data independently. These virtual machines may be backed up on offline media or replicated between physical processing environments.
[39]	FFIEC IT Examination Handbook's "Information Security Booklet," /ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf

Appendix A: Examination Procedures

EXAMINATION OBJECTIVE: Determine the quality and effectiveness of the organization's business continuity planning process, and determine whether the continuity testing program is sufficient to demonstrate the financial institution's ability to meet its continuity objectives. These procedures will disclose the adequacy of the planning and testing process for the organization to recover, resume, and maintain 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 or testing processes work on a micro level or for a particular business function or process.

This workprogram is not intended to be an audit guide; however, it was developed to be comprehensive and assist examiners in determining the effectiveness of a financial institution's business continuity planning and testing program. Examiners may choose to use only certain components of the workprogram based upon the size, complexity, and nature of the institution's business.

The objectives and procedures are divided into Tier I and Tier II:

- Tier I assesses an institution's process for identifying and managing risks.
- Tier II provides additional verification where risk is eviden

Tier I and Tier II objectives and procedures are intended to be a tool set examiners may use when selecting examination procedures for their particular examination. Examiners should use these procedures as necessary to support examination objectives.

TIER I OBJECTIVES AND PROCEDURES

Examination Scope

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

1. Review examination documents and financial institution reports for outstanding issues or problems. Consider the following:

- Pre-examination planning memos;
- Prior regulatory reports of examination;
- Prior examination workpapers;
- Internal and external audit reports, including third-party reports;

- Business continuity test results; and
- The financial institution's overall risk assessment and profile.

2. Review management's response to audit recommendations noted since the last examination. Consider the following:

- Adequacy and timing of corrective action;
- Resolution of root causes rather than just specific audit deficiencies;
- Existence of any outstanding issues; and
- Monitoring systems used to track the implementation of recommendations on an on-going basis

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

- Any significant changes in management, business strategies or internal business processes that could affect the business recovery process;
- Any material changes in the audit program, scope, or schedule related to business continuity activities;
- IT environments and changes to configuration or components;
- Changes in key service providers (technology, communication, back-up/recovery, etc.) and software vendors; 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 the following:

- Technological and security vulnerabilities;
- Internally identified threats; and
- Externally identified threats (including security alerts, pandemic alerts, or emergency warnings published by information sharing organizations or local, state, and federal agencies).

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.

Board and Senior Management Oversight

Objective 2: Determine the quality of business continuity plan oversight and support provided by the board and senior management.

1. Determine whether the board has established an on-going, process-oriented approach to business continuity planning that is appropriate for the size and complexity of the organization. This process should include a business impact analysis (BIA), a risk assessment, risk management, and risk monitoring and testing. Overall, this planning process should encompass the organization's business continuity strategy, which is the ability to recover, resume, and maintain all critical business functions.

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

3. Determine whether the board and senior management has ensured that integral groups are involved in the business continuity process (e.g. business line management, risk management, IT, facilities management, and audit).

4. Determine whether the board and senior management have established an enterprise-wide BCP and testing program that addresses and validates the continuity of the institution's mission critical operations.

5. Determine whether the board and senior management review and approve the BIA, risk assessment, written BCP, testing program, and testing results at least annually and document these reviews in the board minutes.

6. Determine whether the board and senior management oversee the timely revision of the BCP and testing program based on problems noted during testing and changes in business operations.

Business Impact Analysis (BIA) and Risk Assessment

Objective 3: Determine whether an adequate BIA and risk assessment have been completed.

1. Determine whether the work flow analysis was performed to ensure that all departments and business processes, as well as their related interdependencies, were included in the BIA and risk assessment.

2. Review the BIA and risk assessment to determine whether the prioritization of business functions is adequate.

3. Determine whether the BIA identifies maximum allowable downtime for critical business functions, acceptable levels of data loss and backlogged transactions, recovery time objectives (RTOs), recovery point objectives (RPOs), recovery of the critical path (business processes or systems that should receive the highest priority), and the costs associated with downtime.

4. Review the risk assessment and determine whether the includes the impact and probability of disruptions of information services, technology, personnel, facilities, and

services provided by third-parties, including:

- Natural events such as fires, floods, severe weather, air contaminants, and hazardous spills;
- Technical events such as communication failure, power failure, equipment and software failure, transportation system disruptions, and water system disruptions;
- Malicious activity including fraud, theft or blackmail; sabotage; vandalism and looting; and terrorism; and
- Pandemics.

5. Verify that reputation, operational, compliance, and other risks that are relevant to the institution are considered in the BIA and risk assessment.

Risk Management

Objective 4: Determine whether appropriate risk management over the business continuity process is in place and if the financial institution's and TSP's risk management strategies consider wide-scale recovery scenarios designed to achieve industry-wide resilience.

1. Determine whether management has engaged other firms in the discussion of scenarios, performed continuity planning using wide-scale or severely disruptive scenarios, and assessed capacity and feasibility of resuming normal operations.

2. Determine whether 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 and remote computing.
- Back-up of:
  - Data;
  - Operating systems;
  - Applications;
  - Utility programs; and
  - Telecommunications;
- Secure and up-to-date off-site storage of:

- Back-up media;
- Supplies;
- BCP; and
- System documentation (e.g. topologies; inventory listing; firewall, router, and network configurations; operating procedures).

- Alternate power supplies (e.g. uninterruptible power source, back-up generators);
- Recovery of data (e.g. backlogged transactions, reconciliation procedures); and
- Preparation for return to normal operations once the permanent facilities are available.

3. Determine whether satisfactory consideration has been given to geographic diversity for:

- Alternate facilities;
- Alternate processing locations;
- Alternate telecommunications;
- Alternate staff; and
- Off-site storage.

4. Determine whether management has considered the possibility of transferring critical aspects of the institution's operation to alternate backup providers or other industry participants to ensure continuity of operations in extreme situations.

5. Verify that appropriate policies, standards, and processes address business continuity planning issues including:

- Security;
- Project management;
- Change control process;
- Data synchronization, back-up, and recovery;
- Crisis management (responsibility for disaster declaration and dealing with outside parties);
- Incident response;

- Remote access;
- Employee training;
- Notification standards (employees, customers, regulators, vendors, service providers);
- Insurance; and
- Government and community coordination.

6. Determine whether personnel are regularly trained in their specific responsibilities under the plan(s) and whether current emergency procedures are posted in prominent locations throughout the facility.

7. Determine whether the continuity strategy addresses interdependent components, including:

- Utilities;
- Telecommunications;
- Third-party technology providers;
- Key suppliers/business partners; and
- Internal systems and business processes.

8. Determine whether management has reviewed all interrelated components of each mission critical application and the underlying continuity strategy to determine "single point of failure" exposure.

9. Determine whether there are adequate processes in place to ensure that a current BCP is maintained and disseminated appropriately. Consider the following:

- Designation of personnel who are responsible for maintaining changes in processes, personnel, and environment(s); and
- Timely distribution of revised plans to personnel.

10. Determine management's process for determining the scope of disaster recovery test scenarios, including whether management augments the tests with multiple concurrent or widespread interruptions to simulate the impact of "worst case" scenarios.

11. Determine whether 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 as an observer and as a reviewer of test plans and results; and
- Documentation of audit findings

Business Continuity Planning (BCP) - General

Objective 5: Determine the existence of an appropriate enterprise-wide BCP.

1. Review and verify that the written BCP:

- Addresses the recovery of each business unit/department/function/application:
  - According to its priority ranking in the risk assessment;
  - Considering interdependencies among systems; and
  - Considering long-term recovery arrangements.
- Addresses the recovery of vendors and outsourcing arrangements.
- Take(s) into account:
  - Personnel;
  - Communication with employees, emergency personnel, regulators, vendors/ suppliers, customers, and the media;
  - Technology issues (hardware, software, network, data processing equipment, telecommunications, remote computing, vital records, electronic banking systems, telephone banking systems, utilities);
  - Vendor(s) ability to service contracted customer base in the event of a major disaster or regional event;
  - Facilities;
  - Liquidity;
  - Security;
  - Financial disbursement (purchase authorities and expense reimbursement for senior management during a disaster); and
  - Manual operating procedures.
- Include(s) emergency preparedness and crisis management plans that:
  - Include an accurate contact tree, as well as primary and emergency contact

information, for communicating with employees, service providers, vendors, regulators, municipal authorities, and emergency response personnel;

- Define responsibilities and decision-making authorities for designated teams or staff members;
- Explain actions to be taken in specific emergencies;
- Define the conditions under which the back-up site would be used;
- Include procedures for notifying the back-up site;
- Identify a current inventory of items needed for off-site processing;
- Designate a knowledgeable public relations spokesperson; and
- Identify sources of needed office space and equipment and a list of key vendors (hardware/software/telecommunications, etc.).

BCP - Hardware, Back-up and Recovery Issues

Objective 6: Determine whether the BCP includes appropriate hardware back-up and recovery.

1. Determine whether there is a comprehensive, written agreement or contract for alternative processing or facility recovery.

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

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

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

4. 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.

5. 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.

6. 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).

BCP - Security Issues

Objective 7: Determine that the BCP includes 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, stored, retrieved, loaded, and destroyed.

2. Determine whether 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 whether the intrusion detection and incident response plan considers facility and systems changes that may exist when alternate facilities are used.

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

5. 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 systems, data, and facilities access.

6. Review the assignment of authentication and authorization credentials to determine whether they are based upon primary job responsibilities and if they also include business continuity planning responsibilities.

BCP - Pandemic Issues

Objective 8: Determine whether the BCP effectively addresses pandemic issues.

1. Determine whether the Board or a committee thereof and senior management provide appropriate oversight of the institution's pandemic preparedness program.

2. Determine whether the BCP addresses the assignment of responsibility for pandemic planning, preparing, testing, responding, and recovering.

3. Determine whether the BCP includes the following elements, appropriately scaled for the size, activities and complexities of the organization:

- A preventive program to reduce the likelihood that an institution's operations will be significantly affected by a pandemic event, including: monitoring of potential outbreaks, educating employees, communicating and coordinating with critical service providers and suppliers, and providing appropriate hygiene training and tools to employees.
- A documented strategy that provides for scaling the institution's pandemic efforts so they are consistent with the effects of a particular stage of a pandemic outbreak, such as first cases of humans contracting the disease overseas, first cases within the United States, and first cases within the organization itself.
- A comprehensive framework of facilities, systems, or procedures that provide the

organization the capability to continue its critical operations in the event that a large number of the institution's staff are unavailable for prolonged periods. Such procedures could include social distancing to minimize staff contact, telecommuting, or conducting operations from alternative sites.

- A testing program to better ensure that the institution's pandemic planning practices and capabilities are effective and will allow critical operations to continue.
- An oversight program to ensure ongoing reviews and updates to the pandemic plan, so that policies, standards, and procedures include up-to-date, relevant information provided by governmental sources or by the institution's monitoring program.

4. Determine whether pandemic risks have been incorporated into the business impact analysis and whether continuity plans and strategies reflect the results of the analysis.

5. Determine whether the BCP addresses management monitoring of alert systems that provide information regarding the threat and progression of a pandemic. Further, determine if the plan provides for escalating responses to the progress or particular stages of an outbreak.

6. Determine whether the BCP addresses communication and coordination with financial institution employees and the following outside parties regarding pandemic issues:

- Critical service providers;
- Key financial correspondents;
- Customers;
- Media representatives;
- Local, state, and federal agencies; and
- Regulators.

7. Determine whether the BCP incorporates management's analysis of the impact on operations if essential functions or services provided by outside parties are disrupted during a pandemic.

8. Determine whether the BCP includes continuity plans and other mitigating controls (e.g. social distancing, teleworking, functional cross-training, and conducting operations from alternative sites) to sustain critical internal and outsourced operations in the event large numbers of staff are unavailable for long periods.

9. Determine whether the BCP addresses modifications to normal compensation and absenteeism polices to be enacted during a pandemic.

10. Determine whether management has analyzed remote access requirements, including the infrastructure capabilities and capacity that may be necessary during a pandemic.

11. Determine whether the BCP provides for an appropriate testing program to ensure that continuity plans will be effective and allow the organization to continue its critical operations. Such a testing program may include:

- Stress testing online banking, telephone banking, ATMs, and call centers capacities to handle increased customer volumes;
- Telecommuting to simulate and test remote access;
- Internal and external communications processes and links;
- Table top operations exercises; and
- Local, regional, or national testing/exercises.

BCP - Third-Party Management and Outsourced Activities

Objective 9: Determine whether management and the BCP addresses critical third parties and outsourced activities and whether there is appropriate oversight in place.

1. Determine if management has taken sufficient steps to ensure third-party technology service providers (TSPs) employ the most recent techniques and technologies (or identify where gaps exist) to mitigate against:

- Large scale disruptive events that could affect the ability to service clients;
- Cyber events that could impact the ability to service clients; and
- Significant downtime that would threaten the financial institution's business resiliency.

2. Determine if the financial institution's due diligence processes considered its service provider's business continuity program. Consider whether management assessed:

- Recovery capabilities and capacity of the service provider;
- Cyber resilience and preparedness;
- Significant downtime that would threaten the financial institution's business resilience; and
- Service provider's oversight of subcontractors.

3. Assess whether the third-party TSP's contract provides for the following elements to ensure business resiliency:

- DR/BCP test results for RTOs that provide evidence the TSP can recover from large scale disruptions and cyber events;
- Independent audit reports that support the RTOs;
- Inclusion of reasonable performance standards (e.g., SLAs, RTOs);
- Right to terminate language (if the TSP defaults on SLAs and RTOs);
- TSP accountability for actions/inactions of subcontractors should the subcontractor fail to provide necessary service(s) for business recovery capabilities;
- Adherence to U.S. data confidentiality and security standards at a minimum by foreign-based service providers/subcontractors;
- Testing requirements with the TSP; and
- Data governance expectations.

4. Evaluate the financial institution's third-party ongoing monitoring program, including the adequacy of information reviewed to determine that the service provider can continue to meet its obligations to provide financial services and support the institution's business resilience. Consider:

- Full-scope, end-to-end testing with a frequency commensurate with complexity and risk;
- Review of independent third-party assessments and regulatory reports;
- Regular review of MIS reporting (e.g., adherence to RTOs);
- Participation in third-party testing;
- Third-party testing results;
- Periodic reporting to an appropriate oversight committee; and
- Awareness and oversight of service provider's use of subcontractors.

5. Evaluate data governance standards and expectations with third-party providers. Consider:

- Data protection, classification, accuracy, availability and back-up; and
- Data volume and growth.

6. Determine whether the BCP addresses communications and connectivity with TSPs in

the event of a disruption at the institution.

7. Determine whether the BCP addresses communications and connectivity with TSPs in the event of a disruption at any of the TSP's facilities.

8. Determine whether 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.

9. Determine whether the institution has a copy of the TSPs' BCP and incorporates it, as appropriate, into their plans.

10. Determine whether management has received and reviewed testing results of their TSPs.

11. Determine whether institution management has assessed the adequacy of the TSPs' business continuity program through their vendor management program (e.g. contract requirements, third-party reviews).

12. For foreign-based third-party service providers determine if management has adequately addressed production and back-up data that remains offshore. Consider:

- Evidence of management's evaluation of whether storage of data offshore (production or back-up) meets the financial institution's risk appetite and profile; and
- Management's assessment of the foreign-based provider's resilience architecture and strategy.

Cyber Resilience

Objective 10: Determine whether the financial institution's and TSP's risk management strategies are designed to achieve resilience, such as the ability to effectively respond to wide-scale disruptions, including cyber attacks and attacks on multiple critical infrastructure sectors.

1. Determine whether the financial institution and service provider have developed specific procedures for the investigation and resolution of data corruption in response and recovery strategies, including data integrity controls.

2. Determine whether the use of cloud-based disaster recovery services integrate with and protect against data destruction with the same level of assurance as existing (internal) disaster recovery solutions.

3. Determine whether the financial institution and service provider manage the underlying virtualization platform upon which cloud disaster recovery services are based to minimize the impact of attacks designed to cause data destruction and corruption.

4. Determine whether the financial institution and service provider are considering alternate data communications infrastructure to achieve resilience. Consider the efficacy of managing the following risks:

- Reliance upon a single communications provider;
- Disruption of telephony and electronic messaging due to the convergence of voice and data services on the same network; and
- Disruption of data and voice communications between facilities and service providers.

5. Determine whether the financial institution and service provider use a layered anti-malware strategy, including integrity checks, anomaly detection, system behavior monitoring and employee security awareness training, in addition to traditional signature-based anti-malware systems.

6. Determine whether the financial institution and service provider consider their susceptibility to simultaneous attacks in their business resilience planning, testing, and recovery strategies.

7. Determine whether the financial institution and service provider consider their susceptibility to an insider threat and what impact this may have on business continuity and broader resilience.

8. Determine whether the financial institution and service provider have made advance arrangements for both third-party computer forensics and incident management services in advance of a wide-scale cyber security event.

9. Determine whether the incident response program includes a cyber component and assess whether it is appropriate for the size and complexity of the financial institution or service provider. Review the incident response plan to ensure that it addresses the following:

- Teams and responsibilities;
- Procedures for determining the nature and scope of the incident;
- Steps to be taken to contain the problem;
- Details about what is required for contacting affected customers;
- Details about contacting the appropriate regulator;
- Details about filing Suspicious Activity Reports (SARs);
- Details about addressing zero-day attacks;
- A requirement for periodic testing of the incident response plan in the real-world threat landscape; and
- Data destruction and corruption.

Risk Monitoring and Testing

Objective 11: Determine whether the BCP testing program is sufficient to demonstrate the financial institution's ability to meet its continuity objectives.

Testing Policy

1. Determine whether the institution has a business continuity testing policy that sets testing expectations for the enterprise-wide continuity functions, business lines, support functions, and crisis management.

2. Determine whether the testing policy identifies key roles and responsibilities of the participants in the testing program.

3. Determine whether the testing policy establishes a testing cycle with increasing levels of test scope and complexity.

Testing Strategy

1. Determine whether the institution has a business continuity testing strategy that includes documented test plans and related testing scenarios, testing methods, and testing schedules and also addresses expectations for mission critical business lines and support functions, including:

- The scope and level of detail of the testing program;
- The involvement of staff, technology, and facilities;
- Expectations for testing internal and external interdependencies; and
- An evaluation of the reasonableness of assumptions used in developing the testing strategy.

2. Determine whether the testing strategy articulates management's assumptions and whether the assumptions (e.g. available resources and services, length of disruption, testing methods, capacity and scalability issues, and data integrity) appear reasonable based on a cost/benefit analysis and recovery and resumption objectives.

3. Determine whether the testing strategy addresses the need for enterprise-wide testing and testing with significant third-parties.

4. Determine whether the testing strategy includes guidelines for the frequency of testing that are consistent with the criticality of business functions, RTOs, RPOs, and recovery of the critical path, as defined in the BIA and risk assessment, corporate policy, and regulatory guidelines.

5. Determine whether the testing strategy addresses the documentation requirements for all facets of the continuity testing program, including test scenarios, plans, scripts, results, and reporting.

6. Determine whether the testing strategy includes testing the effectiveness of an institution's crisis management process for responding to emergencies, including:

- Roles and responsibilities of crisis management group members;
- Risk assumptions;
- Crisis management decision process;
- Coordination with business lines, IT, internal audit, and facilities management;
- Communication with internal and external parties through the use of diverse methods and devices (e.g., calling trees, toll-free telephone numbers, instant messaging, websites); and
- Notification procedures to follow for internal and external contacts.

7. Determine whether the testing strategy addresses physical and logical security considerations for the facility, vital records and data, telecommunications, and personnel.

Execution, Evaluation, and Re-Testing

1. Determine whether the institution has coordinated the execution of its testing program to fully exercise its business continuity planning process, and whether the test results demonstrate the readiness of employees to achieve the institution's recovery and resumption objectives (e.g. sustainability of operations and staffing levels, full production recovery, achievement of operational priorities, timely recovery of data).

2. Determine whether test results are analyzed and compared against stated objectives; test issues are assigned ownership; a mechanism is developed to prioritize test issues; test problems are tracked until resolution; and recommendations for future tests are documented.

3. Determine whether the test processes and results have been subject to independent observation and assessment by a qualified third party (e.g., internal or external auditor).

4. Determine whether an appropriate level of re-testing is conducted in a timely fashion to address test problems or failures.

Testing With Third-Party Service Providers

Objective 12: Determine whether the financial institution's testing program enhances resilience through demonstrated ability to recover, resume, and maintain operations after disruptions, ranging from minor outages to wide-scale disasters consistent with the BIA and risk assessment.

1. Determine whether testing with third-party providers is included in the institution's enterprise BCP testing program. 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.

2. Determine whether a process exists to rank third parties based on criticality, risk, and testing scope.

3. Determine whether the financial institution has a process to ensure they are included in their critical third-party providers' testing program(s) at reasonable intervals. Consider whether:

- Testing is full-scale and end-to-end;
- Testing includes network connectivity and identifies interdependencies; and
- Testing includes critical subcontractors.

4. Evaluate how the financial institution ensures timeliness, thoroughness, and completeness of periodic testing with their critical providers.

5. Determine whether testing scenarios with critical third-parties considers:

- An outage or disruption of the service provider;
- An outage or disruption at the financial institution;
- An incident response plan;
- Crisis management;
- Cyber events; and
- Return to normal operations.

6. Assess documented process/transaction flow charts to evaluate the thoroughness of the testing scope, plans and strategy.

7. Determine whether the client institution has received assurance, via testing documentation, that the third party can restore services to client institution and support typical volumes during a recovery event.

8. Determine whether the institution relies on proxy testing.

9. Determine whether the institution receives adequate testing information which validates and demonstrates the recovery capability and capacity of their critical service providers.

Testing Expectations for Core Firms and Significant Firms

Note: The following testing expectations only apply to core and significant firms as defined by interagency guidelines.

Core firms are defined as organizations that perform core clearing and settlement

activities in critical financial markets. Significant firms are defined as organizations that process a significant share of transactions in critical financial markets.

For core and significant firms:

1. Determine whether core and significant firms have established a testing program that addresses their critical market activities and assesses the progress and status of the implementation of the testing program to address BCP guidelines and applicable industry standards.

2. Determine the extent to which core and significant firms have demonstrated through testing or routine use that they have the ability to recover and, if relevant, resume operations within the specified time frames addressed in the BCP guidelines and applicable industry standards.

3. Determine whether core and significant firm's strategies and plans address wide-scale disruption scenarios for critical clearance and settlement activities in support of critical financial markets. Determine whether test plans demonstrate their ability to recover and resume operations, based on guidelines defined by the BCP and applicable industry standards, from geographically dispersed data centers and operations facilities.

4. Determine that back-up sites are able to support typical payment and settlement volumes for an extended period.

5. Determine that back-up sites are fully independent of the critical infrastructure components that support the primary sites.

6. Determine whether the tests validate the core and significant firm's back-up arrangements to ensure that: :

- Trained employees are located at the back-up site at the time of disruption;
- Back-up site employees are independent of the staff located at the primary site, at the time of disruption; and
- Back-up site employees are able to recover clearing and settlement of open transactions within the timeframes addressed in the BCP and applicable industry guidance.

7. Determine that the test assumptions are appropriate for core and significant firms and consider:

- Primary data centers and operations facilities that are completely inoperable without notice;
- Staff members at primary sites, who are located at both data centers and operations facilities, are unavailable for an extended period;
- Other organizations in the immediate area that are also affected;
- Infrastructure (power, telecommunications, transportation) that is disrupted;

- Whether data recovery or reconstruction necessary to restart payment and settlement functions can be completed within the timeframes defined by the BCP and applicable industry standards; and
- Whether continuity arrangements continue to operate until all pending transactions are closed.

For core firms:

8. Determine whether the core firm's testing strategy includes plans to test the ability of significant firms, which clear or settle transactions, to recover critical clearing and settlement activities from geographically dispersed back-up sites within a reasonable time frame.

For significant firms:

9. Determine whether the significant firm has an external testing strategy that addresses key interdependencies, such as testing with third-party market providers and key customers.

10. Determine whether the significant firm's external testing strategy includes testing from the significant firm's back-up sites to the core firms' back-up sites.

11. Determine whether the significant firm meets the testing requirements of applicable core firms.

12. Determine whether the significant firm participates in "street" or market-wide tests sponsored by core firms, markets, or trade associations that tests the connectivity from alternate sites and includes transaction, settlement, and payment processes, to the extent practical.

Conclusions

Objective 13: Discuss corrective action and communicate findings.

1. From the procedures performed:

- Determine the need to proceed to Tier II objectives and procedures for additional validation to support conclusions related to any of the Tier I objectives and procedures.
- 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.
- Document conclusions regarding the testing program and whether it is appropriate for the size, complexity, and risk profile of the institution.
- Document whether the institution has demonstrated, through an effective testing

program, that it can meet its testing objectives, including those defined by management, the FFIEC, and applicable regulatory authorities.

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
- The 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 report of examination.

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

Tier II Objectives and Procedures

Tier II objectives and examination procedures may be used to provide additional verification of the effectiveness of business continuity planning or identify potential root causes for weaknesses in the business continuity program. These procedures may be used in their entirety or selectively, depending on the scope of the examination and the need for additional verification. Examiners should coordinate this coverage with other examiners to avoid duplication of effort while reviewing various issues found in other work programs.

The procedures provided in this section should not be construed as requirements for control implementation. The selection of controls and control implementation should be guided by the risk profile of the institution. Therefore, the controls necessary for any single institution or any given area may differ from those noted in the following procedures.

Testing Strategy

Objective 1: Determine whether the testing strategy addresses various event scenarios, including potential issues encountered during a wide-scale disruption:

Event Scenarios

1. Determine whether the strategy addresses staffing considerations, including:

- The ability to perform transaction processing and settlement;
- The ability to communicate with key internal and external stakeholders;

- The ability to reconcile transaction data;
- The accessibility, rotation, and cross training of staff necessary to support critical business operations;
- The ability to relocate or engage staff from alternate sites;
- Staff and management succession plans;
- Staff access to key documentation (plans, procedures, and forms); and
- The ability to handle increased workloads supporting critical operations for extended periods.

2. Determine whether the strategy addresses technology considerations, including:

- Testing the data, systems, applications, and telecommunications links necessary for supporting critical financial markets;
- Testing critical applications, recovery of data, failover of the network, and resilience of telecommunications links;
- Incorporating the results of telecommunications diversity assessments and confirming telecommunications circuit diversity;
- Testing disruption events affecting connectivity, capacity, and integrity of data transmission; and
- Testing recovery of data lost when switching to out-of-region, asynchronous back-up facilities.

3. Determine whether the business line testing strategy addresses the facilities supporting the critical business functions and technology infrastructure, including:

- Environmental controls - the adequacy of back-up power generators; heating, ventilation, and air conditioning (HVAC) systems; mechanical systems; and electrical systems;
- Workspace recovery - the adequacy of floor space, desk top computers, network connectivity, e-mail access, and telephone service; and
- Physical security facilities - the adequacy of physical perimeter security, physical access controls, protection services, and video monitoring.

Test Planning

Objective 2: Determine if test plans adequately complement testing strategies.

Scenarios - Test Content

1. Determine whether the test scenarios include a variety of threats and event types, a range of scenarios that reflect the full scope of the institution's testing strategy, an increase in the complexity and scope of the tests, and tests of wide-scale disruptions over time.

2. Determine whether the scenarios include detailed steps that demonstrate the viability of continuity plans, including:

- Deviation from established test scripts to include unplanned events, such as the loss of key individuals or services; and
- Tests of the ability to support peak transaction volumes from back-up facilities for extended periods.

3. Determine that test scenarios reflect key interdependencies. Consider the following:

- Whether plans include clients and counterparties that pose significant risks to the institution, and periodic connectivity tests are performed from their primary and contingency sites to the institution's primary and contingency sites;
- Whether plans test capacity and data integrity capabilities through the use of simulated transaction data; and
- Whether plans include testing or modeling of back-up telecommunications facilities and devices to ensure availability to key internal and external parties.

Plans: How the institution conducts Testing

1. Determine that the test plans and test scripts are documented and clearly reflect the testing strategy, that they encompass all critical business and supporting systems, and that they provide test participants with the information necessary to conduct tests of the institution's continuity plans, including:

- Participants' roles and responsibilities, defined decision makers, and rotation of test participants;
- Assigned command center and assembly locations;
- Test event dates and time stamps;
- Test scope and objectives, including RTOs, RPOs, recovery of the critical path,

duration of tests, and extent of testing (e.g. connectivity, interoperability, transaction, capacity);

- Sequential, step-by-step procedures for staff and external parties, including instructions regarding transaction data and references to manual work-around processes, as needed;
- Detailed information regarding the critical platforms, applications and business processes to be recovered;
- Detailed schedules to complete each test; and
- A summary of test results (e.g. based on goals and objectives, successes and failures, and deviations from test plans or test scripts) using quantifiable measurement criteria.

Appendix B: Glossary

Access - The ability to physically or logically enter or make use of an IT system or area (secured or unsecured); the process of interacting with a system.

Agency - A legal relationship between two parties who agree that one (the agent) is to act on behalf of another (the principal), subject to the latter's general control. The principal generally is held liable for the agent's actions.

Availability - Whether or how often a system is available for use by its intended users. Because downtime is usually costly, availability is an integral component of security.

Business Continuity - The ability to maintain operations and services, both technology and business, in the event of a disruption to normal operations and services. Assures that any impact or disruption of services is within a documented and acceptable recovery time period and that system or operations are resumed at a documented and acceptable point in the processing cycle.

Business Resilience - The capacity to maintain functions and organizational structure in the face of an internal or external change or threat, recover from a significant disruption, and continue critical operations with minimal impact.

Capacity Planning - The process used to determine whether a service, application, or process is sufficient to handle volumes at peak times and meet growth projections for a specific period of time. Analysis should consider hardware (networks, servers, routers, etc.), software (operating system and application software), and personnel.

Classification - Categorization (e.g., "confidential," "sensitive," or "public") of the information processed by the service provider on behalf of the receiver company.

Computer Security - Technological and managerial procedures applied to computer systems to ensure the availability, integrity, and confidentiality of information managed by the computer system.

Confidentiality - Assuring information will be kept secret, with access limited to appropriate persons.

Configuration Management - The management of security features and assurances through control of changes made to a system's hardware, software, firmware, documentation, testing, test fixtures, and test documentation throughout the development and operational life of the system.

Contingency Plan - A plan for emergency response, backup operations, and post-disaster recovery maintained by an institution as a part of its security program. The plan ensures the availability of critical resources and facilitates the continuity of operations in an emergency situation.

Control Requirements - Process used to document and/or track internal processes to determine that those established procedures and/or physical security policies are being followed.

Conversion Plan - A plan that details transition planning and implementation issues in the period between the execution of an outsourcing agreement and the full production

use of the outsourced services.

Cyber Attack - An attempt to damage, disrupt, or gain unauthorized access to a computer, computer system, or electronic communications network; An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Cyber Resilience - The ability of a system or domain to withstand cyber attacks or failures, and in such events, to reestablish itself quickly.

Data Corruption - Errors in computer data that occur during writing, reading, storage, transmission, or processing, which introduce unintended changes to the original data.

Data Integrity - The property that data has not been destroyed or corrupted in an unauthorized manner; Maintaining and assuring the accuracy and consistency of data over its entire life-cycle.

Data Synchronization - The comparison and reconciliation of interdependent data files at the same time so that they contain the same information.

Database - A database represents the collection of data that is stored on any type of computer storage medium and may be used for more than one purpose.

Dedicated Synchronous Optical NETwork (SONET) - SONET is a standard for telecommunications transmissions over fiber optic cables. SONET is self-healing so that if a break occurs in the lines, it can use a back-up redundant ring to ensure that the transmission continues. SONET networks can transmit voice and data over optical networks.

Digital Subscriber Line (DSL) - DSL provides the ability to transmit high-speed digital signals over existing telephone lines.

Disaster Recovery Exercise - A test of an institution's disaster recovery or BCP.

Disaster Recovery Plan - A plan that describes the process to recover from major processing interruptions.

Disk Shadowing - A back-up process that involves writing images to two physical disks or servers simultaneously.

Distributed Denial of Service (DDoS) - A type of attack that makes a computer resource or resources unavailable to its intended users. Although the means to carry out, motives for, and targets of a DDoS attack may vary, it generally consists of the concerted efforts of a group that intends to affect an institution's reputation by preventing an Internet site, service, or application from functioning efficiently.

Diversity - A description of financial services sectors in which primary and back-up telecommunications capabilities do not share a single point of failure.

Dual Control - Dividing the responsibility of a task into separate, accountable actions to ensure the integrity of the process.

Due Diligence - Technical, functional, and financial review to verify a service provider's ability to deliver the requirements specified in its proposal. The intent is to verify that the service provider has a well-developed plan and adequate resources and experience to

ensure acceptable service, controls, systems backup, availability, and continuity of service to its clients.

Electronic Vaulting - A back-up procedure that copies changed files and transmits them to an off-site location using a batch process.

Emergency Plan - The steps to be followed during and immediately after an emergency such as a fire, tornado, bomb threat, etc.

Encryption - A data security technique used to protect information from unauthorized inspection or alteration. Information is encoded so that data appears as a meaningless string of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using an encryption key.

End-to-End Process Flow - Document that details the flow of the processes, considering automated and manual control points, hardware, databases, network protocols, and real-time versus periodic processing characteristics.

End-to-End Recoverability - The ability of an institution to recover a business process from initiation, such as customer contact, through process finalization, such as transaction closure.

Enterprise-Wide - Encompassing an entire organization, rather than a single business department or function.

FEMA - FEMA is an acronym for Federal Emergency Management Agency.

Financial Industry Participants - Financial institutions and other companies that are involved in the banking, securities, and/or insurance industry and are regulated by supervisory authorities.

Frame Relay - A high-performance WAN protocol that operates at the physical and data link layers of the Open Systems Interconnect (OSI) reference model. Frame Relay is an example of a packet-switched technology. Packet-switched networks enable end stations to dynamically share the network medium and the available bandwidth. Frame relay uses existing T-1 and T-3 lines and provides connection speeds from 56 Kbps to T-1.

Functional Drill/Parallel Test - This test involves the actual mobilization of personnel at other sites in an attempt to establish communications and coordination as set forth in the BCP.

Functionality Testing - A test designed to validate that a business process or activity accomplishes expected results.

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.

Grandfather-Father-Son - Retaining multiple versions of the back-up files off-site on a “grandfather-father-son” rotating basis is recommended. This tape methodology creates three sets of back-up tapes: daily incremental sets or “sons,” weekly full sets or “fathers,” and end-of-month tapes or “grandfathers.”

Hardware - The physical elements of a computer system; the computer equipment as opposed to the programs or information stored in a machine.

Hierarchical Storage Management (HSM) - HSM is used to dynamically manage the back-up and retrieval of files based on how often they are accessed using storage media and devices that vary in speed and cost.

HVAC - Heating, ventilation, and air conditioning.

Implementation Plan - A plan that details project management requirements and issues to be addressed during the period between the execution of an outsourcing agreement and the full production use of the outsourced services.

Incident Response Plan - A plan that defines the action steps, involved resources, and communication strategy upon identification of a threat or potential threat event, such as a breach in security protocol, power or telecommunications outage, severe weather, or workplace violence.

Industry Testing - A test designed to validate that business processes, integrated across firms and within the financial industry, which supports the business continuity objectives of the firms, both individually and collectively.

Information Security - The result of any system of policies and/or procedures for identifying, controlling, and protecting information from unauthorized disclosure; The process by which an organization protects and secures its systems, media, and facilities that process and maintain information vital to its operations.

Information Technology - Systems technologies, including operations such as central computer processing, distributed processing, end-user computing, local area networking, and telecommunications. These operations often represent critical services to financial institutions and their customers.

Integrated Services Digital Network (ISDN) -

Integrated Test / Exercise - This integrated test/exercise incorporates more than one component or module, as well as external dependencies, to test the effectiveness of the continuity plans for a business line or major function.

Integrity - Assurance that information is trustworthy and accurate; Ensuring that information will not be accidentally or maliciously altered or destroyed (see “Data Integrity”).

Interdependencies - Where two or more departments, processes, functions, and/or third parties support one another in some fashion.

Internet Protocol (IP) - IP is a standard format for routing data packets between computers. IP is efficient, flexible, routable, and widely used with many applications, and is gaining acceptance as the preferred communication protocol.

Intrusion Detection - Techniques that attempt to detect unauthorized entry or access into a computer or network by observation of actions, security logs, or audit data; detection of break-ins or attempts, either manually or via software expert systems that operate on logs or other information available on the network.

Magnetic Ink Character Recognition (MICR) - Magnetic codes found on the bottom of

checks, deposit slips, and general ledger debit and credit tickets that allow a machine to scan (capture) the information. MICR encoding on a check includes the account number, the routing number, the serial number of the check, and the amount of the check. The amount of the check is encoded when the proof department processes the check.

Malware - Short for malicious software, malware is designed to secretly access a computer system without the owner's informed consent. The expression is a general term used to mean a variety of forms of hostile, intrusive, or annoying software or program code. Malware includes computer viruses, worms, trojan horses, spyware, dishonest adware, ransomware, crimeware, most rootkits, and other malicious and unwanted software or programs.

Media - Physical objects that store data, such as paper, hard disk drives, tapes, and compact disks (CDs).

Microwave Technology - Narrowband technology that requires a direct line-of-sight to transmit voice and data communications and is used to integrate a broad range of fixed and mobile communication networks.

Modeling - The process of abstracting information from tangible processes, systems and/or components to create a paper or computer-based representation of an enterprise-wide or business line activity.

Module - A combination of various components of a business process or supporting system.

Module Test / Exercise - A test designed to verify the functionality of multiple components of a business line or supporting function at the same time.

Multiplexers - A device that encodes or multiplexes information from two or more data sources into a single channel. They are used in situations where the cost of implementing separate channels for each data source is more expensive than the cost and inconvenience of providing the multiplexing/de-multiplexing functions.

Network Attached Storage (NAS) - NAS systems usually contain one or more hard disks that are arranged into logical, redundant storage containers much like traditional file servers. NAS provides readily available storage resources and helps alleviate the bottlenecks associated with access to storage devices.

Network Security - The protection of computer networks and their services from unauthorized entry, modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and that there are no harmful side effects. Network security includes providing for data integrity.

Object Program - A program that has been translated into machine language and is ready to be run (i.e., executed) by the computer.

Offsite Rotation - Used for backup and/or disaster recovery; moving a copy of the most current database, information, file, or tape to an offsite storage facility to be used only in an emergency.

Pandemic - An epidemic or infectious disease that can have a worldwide impact.

PBX - Private branch exchange. A telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines.

Permanent Virtual Circuit (PVC) - PVC is a pathway through a network that is predefined and maintained by the end systems and nodes along the circuit, but the actual pathway through the network may change due to routing problems. The PVC is a fixed circuit that is defined in advance by the public network carrier. Refer to switched virtual circuit for an additional virtual circuit option.

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; therefore, reciprocal agreements are not usually acceptable as a primary recovery option.

Recovery Point Objective (RPO) - The amount of data that can be lost without severely impacting the recovery of operations or the point in time in which systems and data must be recovered (e.g., the date and time of a business disruption).

Recovery Point Objectives (RPOs) - RPOs represent the amount of data that can be lost without severely impacting the recovery of operations or the point in time in which systems and data must be recovered (e.g., the date and time of a business disruption).

Recovery Service Levels - Collectively, terms that define the speed, quality, and quantity of recovery capability in response to a disaster, including recovery time objective, recovery point objective, timely notification, percentage of normal production service level agreements (SLAs) that will be delivered during recovery mode, etc.

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 Objective (RTO) - The maximum allowable downtime that can occur without severely impacting the recovery of operations or the time in which systems, applications, or business functions must be recovered after an outage (e.g. the point in time that a process can no longer be inoperable).

Recovery Time Objectives (RTOs) - RTOs represent the maximum allowable downtime that can occur without severely impacting the recovery of operations or the time in which systems, applications, or business functions must be recovered after an outage (e.g. the point in time that a process can no longer be inoperable).

Recovery Vendors - Organizations that provide recovery sites and support services for a fee.

Remote Access Capabilities - The ability to obtain access to a computer or network from a remote distance.

Remote Capture - Process that is used to scan and transmit check images and data electronically.

Remote Control Software - Software that is used to obtain access to a computer or network from a remote distance.

Remote Journaling - Process used to transmit journal or transaction logs in real time to a back-up location.

Resiliency - The ability of an organization to recover from a significant disruption and resume critical operations.

Resiliency Testing - Testing of an institution's business continuity and disaster recovery resumption plans.

Retention Requirement - Requirement established by a company or by regulation for the length of time and/or for the amount of information that should be retained.

Risk Analysis - The process of identifying risks, determining their probability and impact, and identifying areas needing safeguards; Risk analysis is an integral part of risk management.

Risk Assessment - A prioritization of potential business disruptions based on severity and likelihood of occurrence. The risk assessment includes an analysis of threats based on the impact to the institution, its customers, and financial markets, rather than the nature of the threat.

SAS 70 Report - An audit report of a servicing institution prepared in accordance with guidance provided in the American Institute of Certified Public Accountant's Statement of Auditing Standards Number 70.

Satellite Technology - These links efficiently extend the reach of typical communication systems to distant areas and provide alternative traffic routing in an emergency.

Security Architecture - A detailed description of all aspects of the system that relate to security, along with a set of principles to guide the design. A security architecture describes how the system is put together to satisfy the security requirements.

Security Audit - An independent review and examination of system records and activities to test for adequacy of system controls, ensure compliance with established policy and operational procedures, and recommend any indicated changes in control, policy, and procedures.

Security Violation - An instance in which a user or other person circumvents or defeats the controls of a system to obtain unauthorized access to information or system resources.

Server - A computer or other device that manages a network service. An example is a print server, which is a device that manages network printing.

Service Level Agreement (SLA) - Formal documents that outline the institution's predetermined requirements for the service and establish incentives to meet, or penalties for failure to meet, the requirements. They should specify and clarify performance expectations, establish accountability, and detail remedies or consequences if performance or service quality standards are not met.

Service Provider - Also referred to as a technology service provider (TSP). Among a broad range of entities, including affiliated entities, non-affiliated entities, and alliances of companies providing products and services. Other terms used to describe service providers include vendors, subcontractors, external service providers, application service providers, and outsourcers.

Significant Firms - Firms that process a significant share of transactions in critical financial markets.

Simulated Loss of Data Center Site(s) Test / Exercise - A type of disaster recovery test that involves the simulation of the loss of the primary, alternate, and/or tertiary data processing sites to verify that the institution can continue its data processing activities.

Simulation - The process of operating a model of an enterprise-wide or business line activity in order to test the functionality of the model. Computer systems may support the simulation of business models to aid in evaluating the BCP.

Sound Practices - Defined in the "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System," which was issued by the Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and Securities and Exchange Commission.

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.

Split Processing - The ongoing operational practice of dividing production processing between two or more geographically dispersed facilities.

Storage Area Network (SAN) - SAN represents several storage systems that are interconnected to form one back-up network, which allows various systems to be connected to any storage device and prevents dependence on a single line of communication.

Stovepipe Application - Stand-alone programs that may not easily integrate with other applications or systems.

Street Tests - Street tests are also called cross-market tests or market-wide tests that are sponsored by the Securities Industry Association, Bond Market Association, and Futures Industry Association. These tests validate the connectivity from alternate sites and include transaction, settlement, and payment processes, to the extent practical.

Sustainability - The period of time for which operations can continue at an alternate processing facility.

Synchronous Data Replication - A process for copying data from one source to another in which an acknowledgement of the receipt of data at the copy location is required for application processing to continue. Consequently, the content of databases stored in alternate facilities is identical to those at the original storage site, and copies of data contain current information at the time of a disruption in processing.

T-1 Line - A special type of telephone line for digital communication and transmission. T-1 lines provide for digital transmission with signaling speed of 1.544Mbps (1,544,000 bits per second). This is the standard for digital transmissions in North America. Usually delivered on fiber optic lines.

Table Top Exercise/ Structured Walk- Through Test -

Terminal Services - A component of Microsoft Windows operating systems (both client and server versions) that allows a user to access applications or data stored on a remote computer over a network connection.

Test Assumptions - The concepts underlying an institution's test strategies and plans.

Test Plan - A document that is based on the institution's test scope and objectives and includes various testing methods.

Test Scenario - A potential event, identified as the operating environment for a business continuity or disaster recovery test, which the institution's recovery and resumption plan must address.

Test Scripts - Documents that define the specific activities, tasks, and steps that test participants will conduct during the testing process.

Test Strategy - Testing strategies establish expectations for individual business lines across the testing life cycle of planning, execution, measurement, reporting, and test process improvement. Testing strategies include the testing scope and objectives, which clearly define what functions, systems, or processes are going to be tested and what will constitute a successful test.

Transaction Testing - A testing activity designed to validate the continuity of business transactions and the replication of associated data.

Two-way Polling - An emergency notification system that allows management to ensure that all employees are contacted and have confirmed delivery of pertinent messages.

Ultra Forward Service - This service allows control over the re-routing of incoming phone calls to pre-determined alternate locations in the event of a telecommunications outage.

UPS - Uninterruptible power supply. A device that allows your computer to keep running for at least a short time when the primary power source is lost. A UPS may also provide protection from power surges. A UPS contains a battery that "kicks in" when the device senses a loss of power from the primary source allowing the user time to save any data they are working on and to exit before the secondary power source (the battery) runs out. When power surges occur, a UPS intercepts the surge so that it doesn't damage your computer.

Utility programs - A program used to configure or maintain systems, or to make changes to stored or transmitted data.

Virtual Private Network (VPN) - A computer network that uses public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

Voice over Internet Protocol (VoIP) - The transmission of voice telephone conversations using the Internet or Internet Protocol networks.

Vulnerability - Hardware, firmware, or software flaw that leaves an information system open to potential exploitation; a weakness in automated system security procedures, administrative controls, physical layout, internal controls, etc., that could be exploited to gain unauthorized access to information or to disrupt critical processing.

Vulnerability Analysis - Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Vulnerability Scanning - Systematic examination of systems to determine the adequacy of security measures, identify security deficiencies, and provide data from which to

predict the effectiveness of proposed security measures.

Walk-Through Drill/Simulation Test - This test represents a preliminary step in the overall testing process that may be used for training employees but not as a preferred testing methodology. During this test, participants choose a specific scenario and apply the BCP to it.

Wallet Card - Portable information cards that provide emergency communications information for customers and employees.

Wide-Scale Disruption - An event that disrupts business operations in a broad geographic area.

Wireless Communication - The transfer of signals from place to place without cables, usually using infrared light or radio waves.

Work-Transfer - Work-transfer is a process whereby the staff located at a recovery site accepts the workload of staff located at a primary production site, and a data center located at a recovery site accepts the workload of the primary data processing site.

Worm - A self-replicating malware computer program. It uses a computer network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. This is primarily because of security vulnerabilities on the target computers.

Appendix C: Internal And External Threats

While a business continuity plan (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 operations. Many types of disasters affect not only the financial institution but also the surrounding community. The human element can be unpredictable in a crisis situation, and it should not be overlooked when developing a BCP since employees and their families could be affected as significantly as, or more significantly than, the institution. Therefore, institution management should consider various internal and external threats and determine the impact they may have on the entire institution, including employees. While the type and severity of internal and external threats may be different for each financial institution, this section discusses four primary categories of threats that should be considered when developing the BCP. These threats include malicious activity, natural disasters, technical disasters, and pandemics.

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.

Vandalism and Looting

Vandalism and looting represent a threat because individuals often seek financial gain by exploiting security weaknesses exposed during an emergency or disaster situation. In the event of an area-wide disaster, the financial institution's security staff may be unable to reach the damaged facility and it may be difficult to obtain services from outside security personnel without prior notification. Therefore, management should address these potential threats before a disaster occurs by implementing alternate security measures to protect both the physical and logical assets of the financial institution.

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 those of FEMA and the Centers for Disease Control (CDC), should be considered.

Terrorism is not new, but the likelihood 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 by the attack.

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, which are 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, should include the designation of an outside meeting place so personnel can be accounted for in an emergency, and should provide guidelines for securing or removing media, if time permits. Fire drills should be periodically conducted to ensure that 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 are being used that activate upon detection of a fire and fill the pipe with water only when required. Consequently, the risk of water damage from burst pipes may be minimized. 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 implement procedures 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 affect 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 Spill

Some financial institutions maintain facilities close to chemical plants, railroad tracks, or major highways used to transport hazardous materials. 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 materials 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 with customers, employees, electronic payment system providers, affiliates, vendors, and service providers. Financial institutions lacking diversity in their telecommunications infrastructures may be susceptible to single points of failure in the event a disaster

disrupts their critical systems.

Customers

Customer reliance on institutions for account information creates a critical need for timely recovery of communications systems. Institutions should establish alternate forms of communication in the event local phone systems become inoperable including a plan for how customers will be advised of alternate means to contact the institution. One alternative form of voice communication involves the use of voice over Internet protocol (VoIP), which is the transmission of phone conversations through the Internet or Internet protocol networks. VoIP technologies also operate on both wireless Internet and cellular networks. While VoIP may become a viable solution when local phone systems are inoperable and the Internet is accessible and functioning, management should realize that preplanning may be required to ensure timely implementation of this technology.

Employees

In addition to restoring data communication lines with customers, restoration of communications with employees is also critical to any BCP. To make it easier for employees to contact the institution during a disaster, management could distribute pre-established toll-free phone numbers to employees. This method of communication would enable employees to report their status using a centralized location and obtain current information about operational restoration.

Calling trees may prove useless during an area-wide disaster since employees may have evacuated to unknown locations and standard telecommunications systems may be inoperable. Therefore, as an alternative to voice landlines, institutions should consider text messaging via cell phones, wireless personal digital assistants, two-way radios or satellite phones, text-based pagers, corporate and public e-mail systems, and Internet based instant messaging systems. In addition, secure connections may be established through a virtual private network (VPN) using a standard Internet connection and a laptop computer. Management should also ensure they have an adequate supply of batteries to operate the wireless devices and laptop computers.

Electronic Payment System Providers

Communications failures with electronic payment system providers may prevent the use of electronic forms of payment, such as debit and credit cards and electronic funds transfers. Therefore, cash needs become critical when customers and employees do not have access to funds electronically, and cash is in short supply during an area-wide disaster. It may be difficult to obtain additional supplies of cash and take delivery of sensitive documents when transportation and telecommunications services are limited. As such, management should carefully analyze funding needs if they anticipate, or when they become aware of, a pending disaster to ensure that liquidity needs are met in a timely manner.

Affiliates, Vendors, and Service Providers

The restoration of communication with affiliates, vendors, and service providers is also paramount to the timely recovery of an institution. Alternate methods of communication and procedures for accessing, downloading, and uploading information should be pre-established with the institution's technology service providers, correspondents, affiliates, and third-party vendors to ensure continuity of service.

Power Failure

The loss of power can occur for a variety of reasons, including storms, fires, malicious acts, brownouts, and blackouts and may result in widespread failure of the power grid and inoperable power distribution centers. 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 regulated to prevent power fluctuations. In the event of power failure, institutions should use an alternative power source, such as an uninterruptible power supply (UPS), 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 and ensure that 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, such as propane, natural gas, or diesel fuel, and arrange for replenishment. One potential advantage of natural gas is that it is supplied by a pipeline, avoiding the need to ship 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. Therefore, proper planning involves careful consideration of which equipment and facilities should be powered up and whether certain operations should be scaled back.

It is also important to ensure that alternative power supplies receive periodic maintenance and testing to maintain operability. Moreover, management should discuss with local authorities the ordinances relative to the 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 the inability to implement the BCP. 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 or trains may be halted by natural or technical disasters, malicious activity, or accidents. In instances of area-wide disasters, delivery of essential services may be diverted for humanitarian and other emergency efforts. This can adversely affect cash distribution, fuel delivery, 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.

Water System Disruptions

Essential necessities, such as water, could be limited or non-existent during a disaster. HVAC systems may be dependent upon water to operate, and initial supplies of drinking water for employees may be quickly exhausted or difficult to find since new shipments

may be delayed due to transportation problems. Institutions should plan for potential disruptions in water services by determining the impact of such a disruption on business operations and maintaining adequate reserves on hand.

Appendix D: Pandemic Planning

Pandemics are defined as epidemics or outbreaks in humans of infectious diseases that have the ability to spread rapidly over large areas, possibly worldwide. Several pandemics have occurred throughout history, and experts predict that we will experience at least one pandemic outbreak in this century.

The current threat originates from an outbreak of avian flu in Asia. It is unknown if an avian virus will result in a human pandemic. The widespread nature of this virus in birds and the possibility that it may mutate over time raise concerns that it will become transmissible among humans, with potentially devastating consequences. The united Sates Government has issued a National Strategy that discusses the threat and potential impact of a pandemic influenza event. The implementation Plan for the National Strategy identifies roles and responsibilities for the federal government, the private sector, and others.

The adverse economic effects of a pandemic could be significant, both nationally and internationally. Due to their crucial financial and economic role, **financial institutions should have plans in place that describe how they will manage through a pandemic event.** Sound planning should minimize the disruptions to the local and national economy and should help the institution maintain the trust and confidence of its customers.

DIFFERENCES BETWEEN TRADITIONAL BUSINESS CONTINUITY PLANNING AND PANDEMIC PLANNING

There are distinct differences between pandemic planning and traditional business continuity planning. When developing business continuity plans, financial institution management typically considers the effect of various natural or man-made disasters that differ in their severity. These disasters may or may not be predictable, but they are usually short in duration or limited in scope. [16] In most cases, malicious activity, technical disruptions, and natural/man-made disasters typically will only affect a specific geographic area, facility, or system. These threats can usually be mitigated by focusing on resiliency and recovery considerations.

Pandemic planning presents unique challenges to financial institution management when developing their continuity plans. Unlike natural disasters, technical disasters, malicious acts, or terrorist events, the impact of a pandemic is much more difficult to determine because of the anticipated difference in scale and duration. The nature of the global economy virtually ensures that the effects of a pandemic event will be widespread and threaten not just a limited geographical region or area, but potentially every continent. In addition, while traditional disasters and disruptions normally have limited time durations, pandemics generally occur in multiple waves, each lasting two to three months. Consequently, no individual or organization is safe from the adverse effects that might result from a pandemic event will be staffing shortages due to absenteeism. These differences and challenges highlight the need for all financial institutions, no matter their size, to plan for a pandemic event when developing their BCP.

Pandemic plans should be sufficiently flexible to effectively address a wide range of possible effects that could result from a pandemic. Pandemic plans need to reflect the institution's size, complexity, and business activities. The potential impact of a pandemic on the delivery of a financial institution's critical financial services should be incorporated into the ongoing business impact analysis and risk assessment processes. The

institution's BCP should then be revised, if needed, to reflect the conclusions of its business impact analysis and risk assessment.

To address the unique challenges posed by a pandemic. The financial institution's BCP should provide for:

- **A preventive program** to reduce the likelihood that an institution's operations will be significantly affected by a pandemic event, including: monitoring of potential outbreaks, educating employees, communicating and coordinating with critical service providers and suppliers, in addition to providing appropriate hygiene training and tools to employees.
- **A documented strategy** that provides for scaling the institution's pandemic efforts so they are consistent with the effects of a particular stage of a pandemic outbreak, such as first cases of humans contracting the disease overseas, first cases within the United States, and first cases within the organization itself. [17] The strategy will also need to outline plans that state how to recover from a pandemic wave and proper preparations for any following wave(s).
- **Comprehensive framework of facilities, systems, or procedures** that provide the organization the capability to continue its critical operations in the event that large numbers [18] of the institution's staff are unavailable for prolonged periods. Such procedure could include social distancing to minimize staff contact, telecommuting, redirecting customers to electronic banking services, or conducting operations from alternative sites. The framework should consider the impact of customer reactions and the potential demand for, and increased reliance on, online banking, telephone banking, ATMs, and call support services. In addition, consideration should be given to possible actions by public health and other government authorities that may affect critical business functions of a financial institution.
- **A testing program** to ensure that the institution's pandemic planning practices and capacities are effective and will allow critical operations to continue.
- **An oversight program to ensure ongoing review and updates** to the pandemic plan so that policies, standards, and procedures include up-to-date, relevant information provided by government sources [19] or by the institution's monitoring program.

The traditional BCP methodologies detailed in the FFIEC's Business Continuity Planning booklet provide a sound framework for institutions of all types in developing plans for pandemic events. Institutions should review the following:

- The **National Strategy for Pandemic Influenza** (National Strategy) and the Implementation Plan for the National Strategy for Pandemic Influenza (National Implementation Plan) issued by the federal government provide a complete guide to pandemic planning. The documents can be found at: http://www.pandemicflu.gov/.
- The financial Services Sector Coordinating Committee issued a **Statement on Preparations for Avian Flu,** which provides industry-developed guidance for financial

institutions preparing for the potential of a serious influenza epidemic. The document can be found at: https://www.fsscc.org/influenza/financial panning.jsp.

- The Departments of Homeland Security (DHS) published **The Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources**. This document is one of the tools DHS developed to enhance pandemic planning. It provides a source listing of primary government and pandemic influenza-specific background material, references, and contacts. Institutions may find the Continuity of Operations-Essential (COP-E) planning process especially useful. The document can be found at: http://www.pandemicflu.gov/plan/pdf/cikrpandemicinfluenzaguide.pdf.

- The Department of Health and Human Services Center for Disease Control published **Interim Pre-pandemic Planning Guidance: Community Strategy for Pandemic Influenza Mitigation in the United States - Early, Targeted, Layered Use of Nonpharmaceutical Interventions**. This document provides information about community actions that may be taken to limit the impact from pandemic influenza when vaccine and antiviral medications are in short supply or unavailable. Financial institutions may be asked to plan for the use of the identified interventions to help limit the spread of a pandemic, prevent disease and death, lessen the impact on the economy, and keep society functioning. The document can be found at: http://www.pandemicflu.gov/plan/community/commitigation.html.

- The Department of Health and Human Services (DHHS) has published a series of checklists that are intended to aid preparation for a pandemic in a coordinated and consistent manner across all segments of society. Included are checklists for state and local governments, for U.S. businesses with overseas operations, for the Workplace, for Individuals and Families, for Schools, for Health Care and for Community Organizations. They can also be found at: http://www.pandemicflu.gov/.

PHASES: PLANNING, PREPARING, RESPONDING, AND RECOVERING

Traditional business continuity and pandemic planning require management to follow a cyclical process of planning, preparing, responding, and recovering. However, pandemic planning requires additional actions to identify and prioritize essential functions, employees, and resources within the institution and across other business sectors. The issues discussed below highlight the specific challenges faced by management and the mitigating controls that should be considered when developing a pandemic plan.

BOARD AND SENIOR MANAGEMENT RESPONSIBILITIES

As with other BCP activities, pandemic planning should not be viewed as solely an Information Technology (IT) issue, but rather as a significant risk to the entire business. As such, an institution's pandemic planning activities should involve senior business management from all functional, business and product areas, including administrative, human resources, legal, IT support functions, and key product lines.

An institution's board of directors is responsible for overseeing the development of the

pandemic plan. The board or a committee thereof should also approve the institution's written plan and ensure that senior management is investing sufficient resources into planning, monitoring, and testing the final plan. Senior management is responsible for developing the pandemic plan and translating the plan into specific policies, processes, and procedures.

Senior management is also responsible for communicating the plan throughout the institutions to ensure consistent understanding of the key elements of the plan and to ensure that employees understand their role and responsibilities in responding to a pandemic event. Finally, senior management is responsible for ensuring that the plan is regularly tested and remains relevant to the scope and complexity of the institution's operations.

INCORPORATING PANDEMIC RISK INTO THE BUSINESS IMPACT ANALYSIS (BIA)

The potential effects of a pandemic should be a part of the financial institution's overall BCP business impact analysis (BIA). The BIA should:

- Assess and prioritize essential business functions and processes that may be affected by a pandemic;
- Identify the potential impact of a pandemic on the institution's essential business functions [20] and processes, and supporting resources;
- Identify the potential impact of an pandemic on customers: those that could be most affected and those that could have the greatest impact on the (local) economy;
- Identify the legal and regulatory requirements for the institution's business functions and processes;
- Estimate the maximum downtime associated with the institution's business functions and processes that may occur during a pandemic;
- Assess cross training conducted for key business positions and processes; and
- Evaluate the plans of critical service providers for operating during a pandemic. Financial institutions should evaluate the plans and monitor the servicers to ensure critical services are available. Financial institutions may wish to have back-up arrangements to mitigate any risk. Special attention should be directed at the institution's ability to access leased premises and whether sufficient internet access capacity is available if telecommuting is a key risk mitigation strategy.

Incorporating the impact of pandemic risk into the institution's BCP involves additional complexity since typical disaster or emergency response mechanisms and methods may not be feasible. For example, moving employees to an alternate facility that is typically used during a natural disaster or other emergency, may not be an appropriate or feasible way to continue operations in a pandemic. There may be a shortage of available staff to relocate and it is possible that the alternate site might be affected by the pandemic. DHS provides a list of twelve planning assumptions that institutions should consider when developing the impact analysis. [21]

The pandemic issues considered in the impact analysis also should involve forecasting

employee absenteeism and considering family care issues that may affect business operations. [22] DHS believes rates of absenteeism will depend on the severity of the pandemic. In a severe pandemic, absenteeism attributable to illness, the need to care for ill family members and fear of infection may reach 40 percent during the peak weeks of a community outbreak, with lower rates of absenteeism during the weeks before and after the peak. Certain public health measures (e.g. closing schools, quarantining household contacts of infected individuals, or altering or ceasing public transportation schedules) are likely to increase the rate of absenteeism.

A key part of an institution's BIA that addresses pandemics is to examine external factors. For example, assessing the impact of critical interdependencies will involve making planning assumptions regarding the availability of external services and prioritizing the effect of possible disruptions. In addition, potential travel restrictions imposed by health and emergency management officials may limit access to those services, even if they are still operating.

RISK ASSESSMENT/RISK MANAGEMENT

As noted in the main body of this booklet, the institution's risk assessment process is critical and has a significant bearing on whether BCP efforts will be successful. Important risk assessment and risk management steps that are important for pandemic planning include;

- Prioritizing the severity of potential business disruptions resulting from a pandemic, based on the institution's estimate of impact and probability of occurrence on operations.
- Performing a "gap analysis" that compares existing business processes and procedures with that is needed to mitigate the severity of potential business disruptions resulting from a pandemic;
- Developing a written pandemic plan to follow during a possible pandemic event;
- Reviewing and approving the pandemic plan by the board or a committee thereof and senior management at least annually; and
- Communicating and disseminating the plan and the current status of pandemic phases to employees. Specific risk assessment and risk management actions arising from a pandemic include the following:

Coordination with Outside Parties

Open communication and coordination with outside groups, including critical service providers is an important aspect of pandemic planning. Financial institutions should coordinate information sharing efforts through participation in business and community working groups and develop coalitions with outside parties to provide support and maintenance for vital services during a pandemic. Efforts could include consideration of cooperative arrangements with other financial institutions within the institution's geographical trade area. In addition, management should coordinate its pandemic planning efforts with local public health and emergency management teams, identify authorities that can take specific actions (e.g., who has the ability to close a building or alter transportation), and plan to alert local and state agencies regarding significant

employee absenteeism that may be caused by a sudden pandemic outbreak. Communication with customers and the media is also critical to ensure that accurate information is disseminated about business operations.

Critical interdependency challenges require management to ensure an adequate reserve of essential supplies and to proactively manage maintenance of equipment to ensure sustainability during potential weakness in the service and supply chains, and develop potential alternatives for obtaining critical service and supplies.

Triggering Events

Identification of A triggering event occurs when an environmental change takes place that requires management to implement its response plans based on the pandemic alert status. Alerts may be issued by various organizations that have developed surveillance systems to monitor the progression of viral outbreaks. Depending on the severity of the alert, management may need to act quickly to implement elements of its pandemic response plans. Therefore, it is important for financial institution management to monitor national and international pandemic news sources in order to be aware of potential outbreaks. Management should monitor websites devoted to national health care issues, identify key points of contact for emergency and health care organizations, and assess potential implications for the financial institution if a pandemic occurs. Management also should communicate to employees and key service providers the actions it plans to take at specific triggering points.

Employee Protection Strategies

Employee protection strategies are crucial to sustain an adequate workforce during a pandemic. Institutions should promote employee awareness by communicating the risks of a pandemic outbreak and discussing the steps employees can take to reduce the likelihood of contracting a pandemic virus. The following risk management strategies should also be considered:

- Publicize the Centers for Disease control and Prevention "Cover Your Cough" and "Clean Your Hands" programs or other general hygiene programs;
- Encourage employees to avoid crowded places and public transportation systems;
- Implement "social distancing"_ techniques to minimize typical face-to-face contact through the use of teleconference calls, video conferencing, flexible work hours, telecommuting, encouraging customers to use online or telephone banking services, ATMs and drive-up windows; and
- Review and consider the use of other non-pharmaceutical interventions developed by the Centers for Disease control and Prevention (more information is available at: http://www.pandemicflu.gov/plan/community/ commitigation.html.

Mitigating Controls

Despite the unique challenges posed by a pandemic, there are control processes that management can implement to mitigate risk and the effects of a pandemic. For example, to overcome some of the personnel challenges, management should ensure that employees are cross-trained and that succession plans have been developed. The

institution may be able to leverage plans already established as part of traditional business continuity planning.

Remote Access

During a pandemic there may be a high-reliance on employees telecommuting, which could put a strain on remote access capabilities such as capacity, bandwidth, and authentication mechanisms. Moreover, employees who typically work onsite may not have remote access authority or the necessary technology infrastructure to work at home. Analysis of remote access capabilities, mapping of related technology infrastructure to employee needs during a pandemic, assessing the infrastructure at the neighborhood level, and considering internal and external capacity are necessary to help ensure telecommuting strategies will work during a pandemic.

RISK MONITORING AND TESTING

As information from medical and governmental experts about the causes and effects of a pandemic continues to evolve, and institution's pandemic plan must be sufficiently flexible to incorporate new information and risk mitigation approaches. As a result, risk monitoring and testing of the pandemic plan is important to the overall planning process. A key challenge for management is developing a testing program that provides a high degree of assurance that critical business processes, including, supporting infrastructure, systems, and applications, will function even during a severe pandemic.

A robust program should incorporate testing:

- Roles and responsibilities of management, employees, key suppliers, and customers;
- Key pandemic planning assumptions;
- Increased reliance on online banking, telephone banking, and call center services; and
- Remote access and telecommuting capabilities

Test results should be reported to management, with appropriate updates made to the pandemics plan and testing program.

Testing for a pandemic may require variations to the scope of traditional disaster recovery and business continuity testing, as potential test scenarios will most likely be different. Alternatives for pandemic testing can include: well orchestrated "work at home" days for critical and essential employees to test remote access capabilities and infrastructure; crisis management team communication exercises; table top exercises that test various scenarios related to escalated absenteeism rates; additional or modified call-tree exercises; and community, regional or industry-wide exercises with members of the financial services sector to test the financial sector's ability to respond to a pandemic-like crisis.

REFERENCES

In addition to references included above, institutions may find these web sites helpful in

their pandemic planning activities:

- The official Federal web site, http://www.pandemicflu.gov, contains the complete text of the National Strategy for Pandemic Influenza and other important, related details.

- Department of Health and human Services (DHHS) http://www.dhhs.gov/nvpo/pandemics/index.html

- Business Pandemic Influenza Planning Checklist (DHSS) http://www.pandemicflu.gov/plan/pdf/businesschecklist.pdf

- Avian Flu Website (DOD) http://fhp.osd.mil/factsheetDetail.jsp?fact=3

- Centers for Disease Control (CDC) http://www.cdc.gov/flu/avian/index. htm

- World Health Organization (WHO) http://www.who.int/csr/disease/ avaian_influenza/en/

- U.S. Department of Veterans Affairs (VA) http://www.publichealth.vc. gov/flu/pandemicflu.htm

- Department of Agriculture (USDA) http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB/.cmd/ad/.ar/sa.retrievecontent/

  .c/6_2_1UH/.ce/7_2_5JM/.p/5_2_4TQ/.d/0/_th/J_2_9D/_s.7_0_A/7_0_1OB?PC_7_2_5JM_contentid=AI05.xml#7_2_5JM

- Department of Labor Occupational Safety and Health Administration (OSHA) http://www.osha.gov/dsg/wuidance/avian-flu.html

- Department of State http://travel.state.gov/travel/tips/health/health_1181.htm

- U.S. Agency for International Development (USAID) http://www. usaid.gov/our_work/global_health/home/News/news_items/avian_influenza.html

- Security and Prosperity Partnership of North America (The North America Plan for Avian & Pandemic Influenza) http://www.spp.gov/pdf/nap_flu07.pdf

Appendix E: Interdependencies

Financial institutions can be very complex, with numerous interdependencies between internal and external systems and processes. Analyzing interdependencies represents a critical step in the business continuity process and is an integral part of a business impact analysis. The analysis of interdependencies allows financial institution management to evaluate the critical resources and services that are shared, identify the potential consequences in the event an interdependent system or process is disrupted, and develop business continuity plans that include mitigating controls and recovery strategies. While each financial institution has a unique business environment and may be dependent on different internal and external systems and processes, this section discusses three common interdependencies, including telecommunications infrastructure; third-party providers, key suppliers, and business partners; and internal systems and business processes. These interdependencies should be considered as part of the business continuity planning process.

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. Advancements in network technologies allow greater geographic separation between people and system resources 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 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 importance of these resources are further heightened.

Single Points of Failure

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. As a result, financial institutions should establish robust processes to ensure that telecommunications are diverse and can be quickly recovered. Institutions should develop risk management practices to identify and eliminate single points of failure across their network infrastructures. Risk management strategies should 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;
- Telecommunications carriers;
- Telecommunications routing through central offices;

- Payment, clearing, and settlement processes, such as electronic funds transfer (EFT) and automated teller machine (ATM) services;
- Core processing providers;
- Points of entry into facilities; and
- Private branch exchanges within an institution.

Telecommunications Diversity Guidelines

A financial institution's BCP should address diversity guidelines for its telecommunications capabilities. This is particularly important for the financial services sector that provides critical payment, clearing, and settlement processes; however, diversity guidelines should be considered by all financial institutions and should be commensurate with the institution's size, complexity, and overall risk profile.

Diversity guidelines may include arrangements with multiple telecommunications providers. However, diverse routing may be difficult to achieve since primary telecommunications carriers may have an agreement with the same sub-carriers to provide local access service, and these sub-carriers may also have a contract with the same local access service providers. Financial institutions do not have any control over the number of circuit segments that will be needed, and they typically do not have a business relationship with any of the sub-carriers. Consequently, it is important for financial institutions to understand the relationship between their primary telecommunications carrier and these various sub-carriers and how this complex network connects to their primary and back-up facilities. To determine whether telecommunications providers use the same sub-carrier or local access service provider, management should consider performing 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 central telephone office..

Management should also consider the following telecommunications diversity components to enhance the BCP:

- Alternative media, such as secure wireless systems;
- Internet protocol networking equipment that provides easily configurable re-routing and traffic load balancing capabilities;
- Local service to more than one telecommunications carrier's central office, or diverse physical paths to independent central offices;
- Multiple, geographically diverse cables and separate points of entry;
- Dedicated Synchronous Optical NETwork (SONET) technology using fiber-optic rings over two diverse routes for connections to telecommunications carrier central offices;
- Frame relay circuits that do not require network interconnections, which often causes delays due to concentration points between frame relay providers;

- Separate power sources for equipment with generator and/or uninterrupted power supply back-up;
- Separate connections to back-up locations;
- Regular use of multiple, active facilities in which traffic is continually split between the connections; and
- Separate suppliers for hardware and software infrastructure needs.

Monitoring Telecommunications Providers

Financial institutions are encouraged to actively monitor their service relationship with telecommunications providers in order to manage the inherent risks more effectively.

In coordination with vendors, management should ensure that risk management strategies include the following, at a minimum:

- Establish service level agreements that address contingency measures and change management for services provided;
- Ensure that primary and back-up telecommunications paths do not share a single point of failure; and
- Establish processes to periodically inventory and validate telecommunications circuits and routing paths through comprehensive testing.

Business Continuity Arrangements

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 telecommunications 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 security and practicality of alternative telecommunications solutions. Switching from fiber optic to wire pairs, dedicated to switched lines, or digital to analog services may make the line more susceptible to a wiretap or to line noise, which could affect data security. Practicality issues should also be addressed, such as selecting alternatives that will accommodate the anticipated volumes 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.

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 periodically test its effectiveness.

Telecommunications Service Priority System (TSPS)

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 telecommunications services during an emergency. The Office of Priority Telecommunications (OPT) under the National Communications System (NCS) administers the TSPS, which ensures priority treatment of the nation's most important telecommunications services supporting national security and emergency preparedness missions.**This means that TSPS designated circuits will be the first to be repaired in an emergency. All non-federal users requesting TSPS provisioning or restoration are required to have a federal agency sponsor. Institutions are encouraged to contact their primary federal regulator for information on the TSPS program and whether they qualify for a TSPS designation. If they do qualify, the financial institution's restoration and recovery plan should include the TSPS program as a key component.**

Government Emergency Telecommunications Service (GETS) and Wireless Priority Service Program (WPS)

Some financial institutions may qualify for sponsorship in the GETS card program and the WPS program, which is the wireless complement to GETS. GETS and WPS are both administered by NCS and provide emergency access and priority processing for voice communications services in emergencies. Financial institutions that perform national security or emergency preparedness functions that are essential to the maintenance of the nation's economic posture during any national or regional emergency will qualify for program sponsorship.**WPS users are encouraged to use GETS to enhance telecommunications services, and both of these programs may prove helpful when heavy usage of the public switched network or the wireless network creates congestion and decreases the probability of completing a call.**

Additionally, in the event state and federal emergency response authorities commandeer cell phone circuits to manage disaster relief efforts, these programs may provide voice communications for financial institutions that have made prior arrangements for these services. Private sector financial institutions may request GETS Cards by submitting an application to their primary federal regulator. Institutions should limit GETS Cards requests to key personnel with crisis management responsibilities or other senior management personnel responsible for carrying out communications during times of emergency.

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 (core, ATM, and EFT), and cash 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.

Telecommunications

During widespread telecommunications outages, considerable challenges emerge regarding real-time communications and cross-industry interdependencies with core processors and other third-party service providers, including ATM and EFT business partners. For financial institutions and their branch offices, timely connectivity with significant vendors, suppliers, service providers, and business partners is critical in order to conduct routine banking transactions. Therefore, redundant systems and manual operating procedures should be an integral part of financial institutions' and service providers' BCP. For example, alternate methods for processing EFT through Internet based systems, proprietary software, or correspondent bank relationships should be established to ensure timely transmission of customer transactions. To ensure that employees understand cross-industry interdependencies and manual operating procedures, comprehensive, enterprise-wide testing should be performed.

Redundant telecommunications links can also be established with the service provider through the development of a contractual arrangement that allows either party to switch its connection to an alternate communication path. For example, either party could use permanent virtual circuit or switched virtual circuit technology, which re-routes the communication path around a problem location either permanently or temporarily, as deemed necessary, and assists in re-establishing timely connectivity between the service provider and the institution.

Liquidity Needs

Reliance on correspondent financial institutions or other third parties for liquidity needs also represents a critical aspect of the BCP process. In the event of an area-wide disaster, existing arrangements with cash providers and delivery services may not be feasible. Therefore, management should establish procedures for securing, storing, delivering, and distributing cash despite having limited power, telecommunications, staff, and security available.

Vendor Due Diligence

To ensure timely recovery of operations, management should routinely perform vendor due diligence.**As part of this due diligence process, management should inquire about the physical paths used by the service provider to ensure that system redundancies have been properly implemented. Institutions should also review the service provider's BCP and ensure that critical services can be restored within acceptable timeframes based upon the needs of the institution. The contract with the service provider should address the service provider's responsibility for maintenance and testing of disaster recovery and contingency plans. Financial institution management should request a copy of the service provider's BCP test results and audit reports to determine the adequacy of business continuity plans and the effectiveness of the testing program. If possible, the institution should consider participating in the service provider's testing process. If the service provider fails to perform satisfactorily during a service disruption, management should determine whether the institution has sufficient resources and capacity to perform these processes internally or if alternate vendor arrangements should be considered.**

Transaction Processing and Report Distribution

Alternate methods of transaction processing and report distribution represent another important element of recovery for serviced institutions. During area-wide disasters, remote image capture systems, using a VPN connection, may allow financial institutions to scan daily items and electronically deliver the imaged information to their service provider for processing without having to physically transport the daily work. In addition, the financial institution may use remote capture software and a secure Internet connection to retrieve various reports needed for operations.

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 that 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? When the back-up site is oversubscribed, is there a limit on the amount of time each client can use the facility?
- 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 financial institution that addresses the requirements of the "Interagency Guidelines Establishing Information Security Standards"?
- Telecommunications-Has the service provider taken appropriate steps to ensure that 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 has a reciprocal agreement with another financial institution, does the other institution have sufficient excess computer capacity to ensure that the affected institution's work will be 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? Will the site be available in the event of an area-wide disaster?
- Space-Does the recovery site have adequate resources to accommodate the institution's employees by providing basic necessities and enabling them to conduct business?
- Paper Files and Forms-Does the recovery site maintain a sufficient inventory of paper-based files and forms that are necessary to perform business functions?
- Printing Capacity/Capability-Does the recovery site maintain adequate printing capacity to meet the demand of the affected institution?
- Contacts-Who is authorized to initiate use of the back-up site? Who does the institution contact at the back-up site, and how much lead time is needed prior to the financial institution's arrival at the back-up site? How much will it cost to activate the back-up site?

Internal Systems and Business Processes

The failure of critical systems or the interruption of vital business processes could prevent timely recovery of operations. Therefore, financial institution management must fully understand the vulnerabilities associated with interrelationships between various systems, departments, and business processes. These vulnerabilities should be incorporated into the BIA, which analyzes the correlation between system components and the services they provide.

Various tools can be used to analyze these critical interdependencies, such as a work flow analysis, an organizational chart, a network topology, and inventory records. A work flow analysis can be performed by observing daily operations and interviewing employees to determine what resources and services are shared among various departments. This analysis, in conjunction with the other tools, will allow management to understand various processing priorities, documentation requirements, and the interrelationships between various systems.

The analysis of internal interdependencies will become even more important during a disruption, particularly if the financial institution is required to relocate to another facility and comparable systems are not available. For example, financial institutions sometimes develop stand-alone programs, called stovepipe applications, in attempt to solve an immediate problem without regard to interoperability issues. While these applications may work well within the institution's environment, they may not easily integrate with other applications or systems. Therefore, when performing business continuity planning, management should be aware of the processes that are dependent upon these stand-alone programs and consider their impact on recovery strategies.

While every financial institution is unique and has its own risk profile, management

should consider the following issues when determining critical interdependencies within the organization:

- Key personnel;
- Vital records;
- Shared equipment, hardware, software, data files, and workspace;
- Production processes;
- Customer services;
- Network connectivity; and
- Management information systems.

Appendix F: Business Impact Analysis Process

Business Impact Analysis Goals

The purpose of a business impact analysis is to determine what impact a disruptive event would have on a financial institution. As such, a BIA has three primary goals:

- Determine Criticality-Every critical business function must be identified, and the impact of a disruption must be determined. While non-critical business functions and processes may likely warrant a lower priority rating, consideration should be given to the impact of interdependencies between various departments and functions before ultimately determining their criticality and priority.
- Estimate Maximum Downtime-Management should estimate the maximum downtime that the financial institution can tolerate while still maintaining viability. Management should determine the longest period of time that a critical process can be disrupted before recovery becomes impossible. In some instances, the BIA process may provide evidence that a business interruption can be tolerated for a shorter period of time than originally anticipated.
- Evaluate Resource Requirements-Realistic recovery efforts require a thorough evaluation of the resources required to resume critical operations and related interdependencies as quickly as possible. Examples of resources include facilities, personnel, equipment, software, data files, vital records, and third-party relationships.

There are generally four cyclical steps included in the BIA process:

1. Gathering information;
2. Performing a vulnerability assessment;
3. Analyzing the information; and
4. Documenting the results and presenting the recommendations.

Gathering Information

The first step of the BIA is to identify which departments and business processes are critical to the recovery of the financial institution. The Business Continuity Planning Committee and/or Coordinator should review organizational charts, observe daily work flow, and interview department managers and employees to identify critical functions and significant interrelationships on an enterprise-wide basis. Information can also be gathered using surveys, questionnaires, and team meetings.

As information is gathered and critical operations are identified, business operations and

related interdependencies should be reviewed to establish processing priorities between departments and alternate operating procedures that can be utilized during recovery.

Performing a Vulnerability Assessment

A vulnerability assessment is similar to a risk assessment; however, it focuses solely on providing information that will be used in the business continuity planning process. The goal of the vulnerability assessment is to determine the potential impact of disruptive events on the financial institution's business processes. Financial industry participants should consider the impact of a major disruption since they play a critical role in the financial system. As part of the vulnerability assessment, a loss impact analysis should be conducted that defines loss criteria as either quantitative (financial) or qualitative (operational). For example, quantitative losses may consist of declining revenues, increasing capital expenditures, or personal liability issues. Conversely, qualitative losses may consist of declining market share or loss of public confidence. While performing a vulnerability assessment, critical support areas and related interdependencies, which are defined as a department or process that must be properly functioning to sustain operations, should be identified to determine the overall impact of a disruptive event. In addition, required personnel, resources, and services used to maintain these support areas must also be identified. Critical support areas and interdependencies should include the following, at a minimum:

- Telecommunications;
- IT departments;
- Transportation and delivery services;
- Shared physical facilities, equipment, hardware, and software;
- Third-party vendors; and
- Back-office operations, including accounting, payroll, transaction processing, customer service, and purchasing.

The steps needed to perform a vulnerability assessment include the following:

1. List applicable threats that may occur internally and externally;
2. Estimate the likelihood that each threat might occur;
3. Assess the potential impact of the threat on employees and customers, property, and business operations; and
4. Assess the internal and external resources available to deal with the identified threats.

Analyzing the Information

During the analysis phase of the BIA, results of the vulnerability assessment should be analyzed and interpreted to determine the overall impact of various threats on the financial institution. This analysis process should include an estimation of maximum allowable downtime (MAD) that can be tolerated by the financial institution as a result of a disruptive event. MAD estimates that may be used include the following:

- Nonessential- 30 days
- Normal- 7 days
- Important- 72 hours
- Urgent- 24 hours
- Critical- minutes to hours

Each business function and process should be placed in one of these categories so that management can determine applicable solutions to ensure timely recovery of operations. Management should then determine which business functions represent the highest priority for recovery and establish recovery objectives for these critical operations. The Business Continuity Planning Committee or Coordinator should discuss the impact of all possible disruptive events, instead of focusing on specific events that may never occur. For example, the impact of a disruptive event could result in equipment failure, destruction of facilities, data corruption, and the lack of available personnel, supplies, vendors, or service providers. Once the impact of a disruption is determined, management should estimate MADs.

After completing the data analysis, the results should be reviewed by knowledgeable employees to ensure that the findings are representative of the true risks and ultimate impact faced by the financial institution. If notable gaps are identified, they should be recognized and incorporated into the overall analysis.

Documenting the Results and Presenting the Recommendations

The final step of the BIA involves documenting all of the processes, procedures, analyses, and results. Once the BIA is complete, a report should be presented to the board and senior management identifying critical departments and processes, significant interdependencies, a summary of the vulnerability assessment, and recommended recovery priorities generated from the analysis.

Appendix G: Business Continuity Plan Components

An enterprise-wide business continuity plan (BCP) should be developed to prevent the interruption of normal operations and to allow for the resumption of business processes in a timely manner. In addition, a comprehensive BCP should provide guidelines for emergency responses, extended back-up operations, and post-disaster recovery. All financial institutions are required to establish a comprehensive BCP regardless of whether they process their work internally or outsource their processing to a service provider. If a financial institution uses a service provider to process its daily transactions, management should ensure that it has incorporated applicable guidelines from the vendor's BCP into the financial institution's plan. The guidelines in this appendix will address the components that should be implemented as part of the business continuity planning process to ensure an effective BCP.

Defining the Business continuity Strategy

The business continuity strategy represents a critical aspect of the BCP and is derived from the information collected during the business impact analysis (BIA) process. The following components should be considered when defining the business continuity strategy and developing the BCP:

- Personnel;
- Communication;
- Technology issues;
- Facilities;
- Electronic payment systems;
- Liquidity concerns;
- Financial disbursement;
- Manual operations; and
- Other considerations.

When developing the continuity strategy, consideration should be given to both short-term and long-term goals and objectives.

Short-term goals and objectives may include:

- Critical personnel, facilities, computer systems, operations, and equipment;
- Priorities for processing, recovery, and mitigation;

- Maximum downtime before recovery of operations; and
- Minimum resources required for recovery.

Long-term goals and objectives may include:

- Management's enterprise-wide strategic plan;
- Coordination of personnel and activities;
- Budgetary considerations; and
- Supervision of third-party resources.

Personnel

Human resources represent one of most critical BCP components, and often, personnel issues are not fully integrated into the enterprise-wide plan. Based on the BIA, the BCP should assign responsibilities to management, specific personnel, teams, and service providers. The planning group should comprise representatives from all departments or organizational units, and the BCP should be prepared by the individuals responsible for carrying out the assigned tasks. In addition, the plan should specifically identify the integral personnel that are needed for successful implementation of the BCP, and succession plans should assign responsibilities to back-up personnel in the event integral employees are not available. Additionally, vendor support needs should be identified. The BCP should address:

- How will management prepare employees for a disaster, reduce the overall risks, and shorten the recovery window?
- How will decision-making succession be determined in the event management personnel are unavailable?
- How will management continue operations if employees are unable or unwilling to return to work due to personal losses, closed roads, or unavailable transportation?
- How will management contact employees in the event personnel are required to evacuate to another area during non-business hours?
- Will the financial institution have the resources necessary to transport personnel to an offsite facility that is located a significant distance from their residence?
- Who will be responsible for contacting employees and directing them to their alternate locations?
- 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)?

Personnel Needs

One of the first things that many financial institutions realize during a disaster is that recovery cannot take place without adequate personnel. Recovery efforts are typically more successful when management attempts to solicit and meet the immediate needs of their employees. Ideally, advance plans should be established regarding living arrangements for displaced employees and their families, such as securing blocks of hotel rooms or maintaining rental contracts for small homes, within and outside the local area. If an emergency lodging program is offered by the financial institution, management should be aware of the business needs of each employee to ensure that proper communication channels and alternative telecommunications options are available, particularly if employees are required to work at their hotel or at an alternate location.

Management should plan for basic necessities and services for its staff members who have been displaced during a disaster. If possible, management should establish plans to obtain water, food, clothing, child care, medical supplies, and transportation prior to the disruptive event. On-site medical support, mobile command centers, and access to company vehicles and other modes of transportation should also be provided, if available. Management's efforts to maintain good employee relations will likely contribute to the commitment and loyalty of financial institution personnel and their desire to assist with the timely recovery of operations.

Emergency Training

Since personnel are critical to the recovery of the financial institution, business continuity training should be an integral part of the BCP. During a disaster, a well-trained staff will more likely remain calm during an emergency, realize the potential threats that may affect the financial institution, and be able to safely implement required procedures without endangering their lives or the lives of others. A comprehensive training program should be developed for all employees, conducted at least annually, and kept up-to-date to ensure that everyone understands their current role in the overall recovery process. In addition, an audit trail should be maintained to document management's training efforts.

Cross Training and Succession Planning

Cross-training of personnel and succession planning is also an important element of the business continuity planning process. Management should cross train employees throughout the organization and assign back-up personnel for key operational positions. The financial institution should also plan to shift employees to other corporate sites, branches, back-up locations, or service provider facilities outside of the disaster area and prior to the development of transportation problems, if possible.

To ensure adequate staffing at the alternate site, financial institutions may decide to locate staff at the back-up facility on a permanent basis or hire employees who live outside the primary business area and closer to the alternate facility. If employees are unable to return to work, management may use formal agreements with temporary

agencies and headhunting services to provide temporary staffing solutions.

BCP Team Assignments

Planning should also consider human resources necessary for decision making and staffing at alternate facilities under various scenarios. Typically, a recovery team is established to perform this function, and their primary responsibility is to recover predefined critical business functions at the alternate back-up site. They will be responsible for retrieving materials from the off-site storage location, such as data files, supplies, equipment, and software. Once these materials have been obtained, the recovery team will install the necessary hardware, software, telecommunications equipment, and data files required for recovery.

Key personnel should also be identified to make decisions regarding the renovation or rebuilding of the primary facility after the immediate disaster has ended. These tasks usually require personnel beyond what is necessary for ongoing business continuity efforts. Personnel responsible for returning the primary facility to normal operations are usually designated to a salvage team, which should be separate from the recovery team. The salvage team must be certain that all pending danger is over, and employees can safely return to the primary facility. Once personal security is ascertained, the salvage team will be responsible for supervising the retrieval and cleaning of equipment, the removal of debris, and the recovery of spoiled media and reports. The salvage team is also given the authority to resume normal operations at the primary facility, which is a significant task since numerous areas must be closely reviewed to ensure that operations will function properly.

Once the salvage team approves the resumption of normal operations, the recovery team is assigned the responsibility of returning production to the primary facility. However, before restoration tasks can be performed and employees return to the primary facility, the salvage team should perform an inventory of all property and ensure that the on-site investigation is complete. The BCP should address guidelines for transferring operations from the back-up site to the primary facility with minimum disruption. In addition, records should be maintained detailing associated costs and property valuations for documenting budgetary changes, general ledger records, and insurance claims.

Finally, the business continuity planning coordinator or planning committee should be given responsibility for regularly conducting employee awareness training and performing annual tests of the BCP. In addition, the BCP should be updated at least annually, or more frequently, after significant changes to business operations, or if training and testing reveal gaps in the policy guidelines.

Communication

Communication is a critical aspect of a BCP and should include communication with employees, emergency personnel, regulators, vendors/suppliers (detailed contact information), customers (notification procedures), and the media (designated media spokesperson). **Alternate telecommunications capabilities should be implemented to prevent any single point of failure that could disrupt operations. Policy guidelines should also address alternate methods of telecommunications in the event primary providers are unable to supply necessary services, and regular audits should confirm the adequacy of these diverse systems.**

Communicating With Employees

One of the most important activities of business continuity planning involves communicating with employees. Employees should be promptly notified of a pending disaster, and specific evacuation instructions should be provided and included in the BCP. Management must be able to communicate with personnel located in isolated areas or dispersed across multiple locations, and management should be aware of each employee's evacuation plans to ensure that they can be contacted in a timely manner during a disaster. While manually dialed telephone call trees may be a viable communication tool in some instances, emergency notification systems should be evaluated to determine their cost effectiveness. With either method, management should ensure that contact information is current and easily accessible. Synchronization with human resource departments and company mail systems may prove helpful in maintaining the currency of contact information. Employee notification solutions may also include the following:

- An in-bound hotline number for employees to retrieve up-to-date voice messages from any location or a website accessible only by employees that provides important information regarding the operational status of the financial institution and contact numbers for financial institution personnel;
- A two-way polling phone system that confirms all employees have been contacted, with confirmed delivery of messages;
- Remote access provided to employees through the use of laptops, software, and Internet based solutions by utilizing dial-up connections, cable modems, virtual private networks (VPNs), integrated services digital networks (ISDNs), digital subscriber lines (DSLs), or wireless capabilities;
- Ultra forward service, which allows incoming calls to be rerouted to a pre-determined alternate location;
- Custom redirect service, which allows management to determine where incoming calls are answered and redirect calls to various locations or pre-established phone numbers;
- Provisioning local phone services to one office from two different telecommunications provider locations to provide phone system redundancy; and
- Adding a back-up Internet Service Provider (ISP) and balancing the traffic between the two ISPs over separate communication paths.

Interfacing With External Groups

Financial institutions often forget about the need to include BCP guidelines regarding their interaction with external groups such as local and state municipal employees and city officials. Management should implement BCP guidelines addressing escalation procedures and include contact information for communicating with these various groups. Consideration should be given to the proximity of the financial institution to police, fire, and medical facilities, and the timeliness of their response should be factored into BCP recovery strategies.

Given the importance of the on-going operation of the financial system, financial

institutions should be able to communicate with their industry counterparts. Current contact information should be maintained and should be easily accessible to facilitate conference calls and meetings between financial sector trade associations, financial authority working groups, emergency response groups, and international exchange organizations. These groups should assess the potential impact of major operational disruptions, coordinate recovery efforts, and promptly respond to failures in critical communication systems.

Media Relations

A significant part of any BCP and related test plan should involve dealing with the media. When a disruptive event occurs that could affect the financial institution's ability to continue operations, the public must be informed. Before a disaster strikes, management should prepare a response that has been approved by the board and the shareholders. In addition, employees should be instructed to refer any questions to the financial institution's media contact. The chosen spokesperson should be adequately informed, credible, have strong communication skills, and be accessible to the media so that inaccurate information is not broadcast to the public, which could potentially harm the reputation of the financial institution. Only confirmed information should be provided, and the spokesperson should discuss what the financial institution is doing to mitigate any potential threats. In order to ease customer's concerns regarding the security of their deposit funds, it is a good idea to conduct regular media briefings until the emergency has ended.

Technology Issues

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

- Hardware - mainframe, mid-range, servers, network, end-user;
- Software - applications, operating systems, utilities;
- Communications (network and telecommunications);
- Data files and vital records;
- Operations processing equipment; and
- Office equipment.

These technology issues play a critical role in the recovery process; therefore, comprehensive inventories should be maintained to ensure that all applicable 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.

The BCP team or coordinator should also identify and document end-user requirements. For example, employees may be able to work on a stand-alone personal computer (PC) to complete most of their daily tasks, but they may require a network connection to fulfill other critical duties. Consequently, management should consider providing employees

with laptops and remote access capabilities using software or a VPN connection.

When developing the BCP, institutions should exercise caution when identifying non-critical assets. An institution's telephone banking, Internet banking, or automated teller machine (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 (RTOs). For example, financial industry participants whose operations are critical to the functioning of the overall financial system and other financial industry participants should establish high recovery objectives, such as same-day business resumption. Conversely, less stringent recovery objectives may be acceptable for other entities. Considerations such as the increased risk of failed transactions, liquidity concerns, solvency, and reputation risks should be factored into the decision making process. The scope of the recovery plan should address alternate measures for core operations, facilities, infrastructure systems, suppliers, utilities, interdependent business partners, and key personnel. Recovery plan alternatives may take several forms and involve the use of another data center or 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/back-up" model)-A hot site is fully configured with compatible computer equipment and typically can be operational within several hours. Financial institutions may rely on a service provider for back-up facilities. The traditional active/back-up model requires relocating at least core employees to the alternative site. This model also requires data files 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 their data to the alternate site on a continuous basis using either synchronous or asynchronous data replication. 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. In addition, there are also security concerns when using a hot site since the applications may contain production data. Consequently, management should ensure that the same security controls that are required at the primary site are also replicated at the hot site. 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. Other alternatives beyond synchronous mirroring are available to allow for greater distance separation; however, there is a risk that a small amount of transaction data may be lost in transit between the primary and alternate centers at the moment of the business disruption. Depending on the type of lost data and the cost of identifying and reprocessing it, the risk of losing a small amount of data in transit may be overshadowed by the ability to restore the institution to full business service in a short amount of time. This trade-off is not a technology decision; it is a business decision.

- Warm Site-Warm sites provide resumption capacity somewhere between that of a hot and cold site. The facility will be equipped with electricity; heating, ventilation, and air conditioning systems; computers; and external communication links. However, applications may not be installed, and there may be a limited number of available workstations. Therefore, management will need to deliver workstations for remote processing, and production data will need to be restored from back-up media. This recovery option is less costly, more flexible, and requires fewer resources to maintain than a hot site. Conversely, it will take longer to begin processing at the warm site and recover operations. However, if critical transaction processing is not required, this alternative may be acceptable.

- 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. 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. A variation of this recovery option is the rolling/mobile back-up site, which provides the same facility arrangements, but with mobility advantages. While cold sites represent a low cost solution, they typically can take up to several weeks to activate. Therefore, this type of facility is usually not considered an adequate primary recovery option because of the time it takes to start production and resume operations. In addition, it is difficult to perform a recovery test using this type of facility since parallel processing would take a great deal of time and effort to complete.

- 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.

- Multiple Centers or Dual Sites-Multiple centers distribute processing among various facilities for redundancy. These facilities could be owned by one entity or represent a reciprocal agreement with other financial institutions or businesses. The cost of this recovery option is predictable and allows for resource sharing among the various facilities; however, if the facilities are not geographically distributed in different locations, an area-wide disaster could render all of the sites useless. In addition, this

type of facility could be more difficult to manage and administer. Management should also understand that implementing a reciprocal agreement might not always provide an optimal back-up solution due to limited excess capacity.

- Service Bureaus-Financial institutions may contract with a service bureau to provide full processing capabilities. This recovery option will provide immediate availability, testing opportunities, and the possibility of additional services provided. Conversely, the disadvantage of this option is the associated costs and the likelihood of strained resources during an area-wide disaster.

- In-house or Vendor Supplied Hardware-This recovery option provides the supply of needed hardware to replace damaged equipment either through internal means or by contracting with an outside supplier to provide critical components using overnight delivery services. Depending on the amount of damaged equipment and the complexity of the damaged systems, this recovery option may be similar to a cold site and take several days or weeks to implement.

- Prefabricated Building-Financial institutions may contract for the construction of a prefabricated building at a predefined location to house back-up processing functions. While this alternative is not considered an adequate recovery option by itself, it may be considered an acceptable solution when used as a redundant or dual site recovery option or in combination with subscription services that provide immediate availability.

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 serve as a back-up for institution "B" as long as institution "A" has time available, and vice versa. In most 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 would be notified if the other institution implements equipment and software changes, and provisions should be included addressing each institution's right to conduct annual tests at the reciprocal site.

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 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.

The back-up site should mirror operational functionality. Consequently, duplicate check processing, imaging services, ATMs, telephone banking platforms, call centers, commercial cash management services, and electronic funds transfer systems should be duplicated for immediate activation at the back-up site.

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. In addition, alternate sites should not rely on the same critical infrastructure system that provides utility services such as electricity, telecommunications, transportation, and water. While geographic diversity is important for all financial institutions, this is a particularly important factor for financial industry participants whose rapid recovery is critical to the financial industry. Financial institutions should consider the geographic scope of disruptions and the implications of a citywide or regional disruption. The distance between primary and back-up locations should consider RTOs 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, 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 software and data file back-up decisions 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 the 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") 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 electronic vaulting, remote journaling, disk shadowing or data mirroring, hierarchical storage management (HSM), storage area network (SAN), or network-attached storage (NAS) to ensure appropriate back-up of operations.

Electronic vaulting represents a batch process that periodically transfers copies of modified files to an offsite back-up location. Conversely, remote journaling refers to the real time transfer of transaction logs or journals to a remote location. These logs and journals are used to recover transaction and database changes since the most recent back- up. As a result, this back-up process allows the alternate site to be fully operational at all times. Disk shadowing or data mirroring uses two separate disks or multiple servers, on which either data images or identical information is written to simultaneously. These back-up processes ensure data redundancy and the availability of duplicate disks or hardware.

Additional back-up options include HSM, SAN, and NAS. HSM uses optical disks, magnetic disks, or tapes to dynamically manage the back-up and retrieval of files to devices that vary in speed and cost. For example, the faster devices or media are used to hold the information that will be accessed more frequently, and the files that are not needed as often are stored on the slower devices or media. SAN represents several storage systems that are connected to form a single back-up network. This back-up option provides the ability for several devices to communicate with each other and with the various storage devices, which prevents dependence on a single connection. NAS systems usually contain one or more hard disks that are arranged into logical, redundant storage containers, much like traditional file servers. NAS provides readily available storage resources and helps alleviate the bottlenecks associated with access to storage devices. NAS environments are designed to facilitate the movement of data and allow any application or client to use any operating system to send data to or receive data from a NAS device.

Back-up tape storage remains an effective solution for many financial institutions. However, when an institution uses this type of media for its primary back-up storage, back-up tapes should be sent to the off-site storage facility as soon as possible, should not reside at their originating location overnight, should not be returned to the originating location until the are replaced with the current day's back-up tapes, and should be properly secured to prevent damage or unauthorized access. Back-up media, especially tapes, should be periodically tested to ensure that 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.

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 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 should not be returned to the originating location until new back-up files are off-site. Retaining multiple versions of the back-up files off-site on a "grandfather-father-son" rotating basis is recommended so that if the newest daily incremental files ("sons") are not readable, the weekly full sets ("fathers") are there as the next best alternative, and if the "fathers" are not readable, the end-of-month back-up files ("grandfathers") are available to restore business processes.

Software Back-up

Software back-up for all hardware platforms consists of four basic areas: operating system software, application software, utility programs, and databases. An inventory of 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. It is also common for financial institutions to request customized software programs from their software vendor. Therefore, a 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. In the event management does not have the source code in its possession, a software escrow agreement is established whereby a third-party maintains the source code, back-up copies of the compiled code, manuals, and other supporting materials in a secure location. A formal agreement is established between the financial institution, the software vendor, and the escrow agent, which allows the financial institution access to the source code if the software vendor goes out of business or is unable to fulfill their contact obligations. The BCP should identify this issue and applicable audit controls that protect the bank's interest in the source code.

Utility programs are used to assist in the operation of a computer by configuring or maintaining systems, making changes to stored or transmitted data, or compressing data. Utility programs should be maintained in the same manner as operating system software and application software to ensure that back-up copies are readily available when needed.

Databases represent the collection of data that may be stored on any type of computer storage medium. For example, a financial institution may maintain a database on their network file server that contains employee information used for processing payroll. Back-up copies of the database should be maintained off-site, and management should assess the criticality of the database to determine how frequently the database should be backed up.

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. As such, management should ensure that all critical networks and related software and data files are backed up appropriately to ensure timely recovery of operations.

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, fire-resistant, and secure, with procedures for restricting physical access to authorized personnel. Management should keep in mind that using a timed vault for off-site storage may present a problem if an unexpected emergency requires immediate retrieval during non-business hours. Consequently, a secure method for storing vault combinations and keys should be established to ensure that off-site storage items are accessible when needed. Financial institutions are discouraged from allowing employees to store back-up data files at their residence due to potential security concerns. Moreover, the off-site premises should be an adequate distance from the computer operations location so that both locations will not be affected by the same event.

In addition to 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. For example, most networks change over time as software, service packs, and patches are installed and configurations are altered. Therefore, documentation supporting the current network

environment is crucial. Another back-up 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 the financial institution's or service provider's computer systems are not available for a period of time. For example, a hard copy of current customer information should be maintained at the main facility and at an off-site location to ensure that employees have the information they need to perform manual operations and serve the financial institution's customers.

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.

As a service industry, one of the most critical components of the BCP involves the physical presence where customers can go to conduct business. Based on past experience during disaster situations, successful sharing of banking facilities with other financial institutions has benefited each bank by having an operational facility to service customer's needs, establish basic operations during the recovery process, and instill confidence in the financial institution's business continuity efforts. Therefore, management may consider establishing formal agreements with local and out-of-area businesses and financial institutions to use their facilities in the event of a disaster. Alternatively, management may also plan to enlist the assistance of state and local agencies to expedite building permits and inspections for temporary facilities. Close communication with regulatory authorities is imperative to ensure that approval requirements for additional branch facilities are properly followed. In addition, prior notification may expedite the recovery process.

If possible, the plan should include logistical procedures for moving personnel to the recovery location prior to a pending emergency. It is particularly important that recovery team members inspect the site before a disaster strikes to determine what items they will need to transport to the facility to ensure timely recovery of operations. Once the institution returns to their original facility, the BCP should be reassessed to determine if these alternate plans warrant adjustment.

Electronic Payment Systems (EPS)

The BCP should address alternate arrangements in the event EPS, such as ATM systems and electronic funds transfer (EFT) systems are inoperable. When mainframe systems are down, ATM switches cannot communicate with host systems to validate withdrawal requests. Therefore, management should consider plans for pre-established withdrawal limits based on the institution's relationship with the customer. In addition, the financial institution should prepare for an increase in potential branch traffic when ATM systems are down. Pre-established agreements with various cash delivery

services within and outside of the local area should also be considered to ensure that ATMs are adequately stocked with cash to meet potential customer demands when service returns.

BCP guidelines should also address alternate plans for retrieving and transmitting EFTs when payment systems are disrupted. Alternate solutions may include manual procedures for calling in or faxing wire and automated clearinghouse requests to correspondent banks. In addition, web based systems or third-party software may be used to conduct EFTs.

Management should also ensure that redundant EPS are included at recovery sites for immediate activation, and thorough documentation should be maintained to ensure timely posting of applicable entries when systems are recovered.

Liquidity Concerns

Management should ensure that the BCP addresses liquidity and cash concerns, and annual budget projections should include an analysis of potential cash needs to cover emergencies. During a disaster, power and communication systems may fail, requiring the use of cash to purchase supplies and necessary services due to inoperable ATM, debit, and credit card systems. Funding the short-term needs of your employees and customers should be considered when determining the amount of cash to have on hand during a disaster. If management is aware of an approaching emergency, cash limits for various locations within and outside the potential disaster area should be assessed to determine how much cash is needed. Management should also establish agreements with cash providers, delivery services, and transportation providers, within and outside trade areas that are subject to a common disaster, to ensure timely delivery of cash. Management should ensure that borrowing lines have been pre-established and funds are readily available during an emergency. Customer notification regarding the security of depositor's funds is also important since a perceived liquidity crisis could evolve if customer confidence is impaired.

Alternate methods of obtaining delivery of the financial institution's cash letter should also be considered since typical transmission methods may be unavailable during an emergency. For example, document imaging systems using remote capture technology may provide an alternative method for the electronic delivery and processing of a financial institution's cash letter.

Financial Disbursement

The BCP should address guidelines regarding purchase authorities beyond approved policy limits and expense reimbursement options for financial institution personnel during a disaster. In addition, management should also consider distributing higher limit credit cards or establishing a separate checking account, which designates individuals who can sign checks in the event of an emergency or who have authorized debit card access that could be utilized to purchase emergency supplies.

Manual operations

Management should determine whether automated tasks could be conducted manually if automated systems are inoperable. For example, if the network, mainframe, or Internet is not functioning, management should determine if employees could fulfill their daily duties using traditional, non-technical procedures. The BCP should provide specific guidelines addressing manual procedures for critical functions, such as back-office operations, loan operations, and customer support. Management should maintain back-

up records to ensure that customer account information (account numbers, customer names, addresses, account status, and account balances) is readily accessible during a disaster. The BCP should also address the distribution of hard copy documents, equipment, and supplies, as necessary. The BCP should also include instructions for dealing with customer requests during downtime, keeping track of daily transactions, reconciling general ledger accounts, documenting operational tasks, and posting manual entries after system recovery. Furthermore, to ensure that the institution's staff understands how to perform these manual procedures, the BCP should include employee training and testing guidelines.

Other Considerations

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

- Prevention and preparedness, including the determination of adequate insurance coverage based upon threats and the resulting loss potential identified in the BIA;
- Awareness programs designed to prepare customers for a disaster, using various methods such as statement stuffers, web postings, and advertisements;
- Reconciliation of recovery times with business unit requirements;
- Disaster declaration and plan implementation processes;
- Understanding of local, state, and federal emergency preparedness requirements and related programs available to manage disasters;
- Recovery progress reports; and
- Regularly reviewing, evaluating, auditing, testing, modifying, and maintaining the BCP based on changes in personnel and their responsibilities, changes in business operations, and gaps identified in the BCP based on test results and audit recommendations.

Appendix H: Testing Program - Governance and Attributes

Governance

Board of Directors and Senior Management

The board and senior management should establish a testing program appropriate for the size, complexity, and risk profile of the organization and its business lines. They should ensure that the testing program demonstrates the institution's ability to meet its requirements for continuity of operations. The board and senior management should establish clear lines of authority and responsibility for all parties involved with developing, implementing, and monitoring the continuity testing program. They should also review and approve the continuity testing program at least annually, ensure that appropriate follow-up on test results is performed, and review test results.

Institutions may employ various approaches for ensuring coordinated and consistent testing across the organization and support for various quality assurance activities, including consistent standards for testing and reporting. For example, many institutions have created a business continuity oversight function, under the direction of a senior manager, with accountability and authority for business continuity planning and testing across the organization. The business continuity function is supported by a team of liaisons assigned from within the business lines and support functions. Some institutions rely on a steering committee, comprised of representatives from business and support functions, to ensure a coordinated and consistent approach to business continuity planning and testing. Regardless of the approach taken, it is the responsibility of the board and senior management to ensure that sufficient resources and qualified staff are allocated to the business continuity testing effort.

Business Line management

Business line management should have ownership and accountability for testing continuity of business operations, including applications and processes. While business line management has overall responsibility for testing their business processes and related interdependencies, they should coordinate with the enterprise-wide business continuity plan (BCP) testing function and support areas, such as IT and facilities management. Ultimately, business line management should ensure that its BCP is continually updated based on test results and changes in business processes.

IT Function

The IT function should have ownership and accountability for testing recovery of the institution's systems, IT infrastructure, telecommunications, and the infrastructure of alternative computing facilities. Moreover, the IT function has custodial responsibility for business line data and applications. IT should coordinate with business line management and staff to establish test environments suitable for business line testing and should continue to coordinate throughout the testing process. Additionally, the IT function should, through effective management of the test schedule, provide sufficient opportunities for the various business functions to test the operational consistency of primary and alternate computing facilities. The IT group is responsible for maintaining the technology test environment, including controls such as change and configuration management and information security.

Crisis Management

The board and senior management should ensure that the business continuity testing program includes the institution's crisis management capabilities. The testing program should include exercises to demonstrate that the crisis management program effectively meets the institution's objectives for responding to a crisis situation, including identifying and declaring emergencies, providing a central point for the management of an event, and coordinating internal and external communications and human resource issues.

Facilities Management

The facilities management function should have ownership and accountability for testing the recovery of the institution's physical plant and equipment, environmental controls, and physical security. Environmental controls for data centers and the facilities that house critical business functions should be included in the institution's continuity testing program. When data centers or business functions are housed in vendor facilities, contracts should specify the requirements of the vendor for testing continuity of those facilities.

Internal Audit

The internal audit department, or another qualified independent party, plays an important role in providing an independent review of the adequacy of the overall business continuity testing program. The depth and frequency of audit activities and reporting should be scaled to the criticality of the operation. While the scope of audit activities and deliverables may vary, in all cases they must encompass an independent and objective evaluation of the effectiveness of the testing program.

As part of the review of the testing process, internal audit should determine the reasonableness of the underlying assumptions that were made in developing the test program. The reasonableness of underlying assumptions, as well as the adequacy of test plans, scenarios, schedules, and reports, should be evaluated relative to (1) the size and complexity of the institution, (2) the criticality of the business line, and (3) the risk and impact of a possible business disruption. Audit should observe test exercises to assess the control environment of alternative locations, verify the results, ensure that proper reporting and escalation mechanisms are established and utilized, and ensure that test plans are updated to reflect prior test results.

Testing Strategy

Enterprise-wide testing strategies should be developed to properly validate the BCP. Management will achieve greater confidence in their testing strategies when consideration is given to the following elements and complexity issues:

Elements

The test strategy should encompass at least three elements: staffing, technology (data, systems, applications, and telecommunications), and the facilities that house the staff and technology environments.

- Staffing-Testing strategies should include demonstrations of the staff's ability to support business processes, including the processing and settlement of transactions, communication with key internal and external stakeholders, and reconciliation of

transactions and books of record. Strategies may need to address the ability of staff to support increased workloads resulting from the transfer of processing to alternate sites for extended periods of time. For institutions that have implemented split processing business models, any aspects of the client relationship model that present challenges or complexities to the transfer of workloads across sites, and related dependencies, should be identified and incorporated into testing strategies. In addition, testing strategies should demonstrate the effectiveness of the institution's management succession plans.

- Technology-Testing strategies for technology should include the data, systems, applications, network, and telecommunications necessary for supporting business activities. In the event system recovery is dependent upon the retrieval of data files, programs, and other items maintained at the back-up facility; off-site testing procedures should only include the use of these back-up items to properly replicate the loss of any master data files and programs maintained at the main facility. Back-up data files should also be tested frequently to assess the integrity of the information, to determine if the data is being saved in the correct format, and to ensure that applicable files can be retrieved in a timely manner. Alternatively, institutions may employ other processes for data replication, such as synchronous and asynchronous data replication. Regardless of the data replication process used, the process for demonstrating consistency of data across different processing environments should be included in the testing strategy. In addition, strategies should test processes to recreate any data lost during a switch to alternate processing facilities, and periodic reviews of telecommunications services should be conducted to determine circuit diversity.

- Facilities-Testing strategies for business functions should encompass environmental controls, workspace recovery, and physical security to ensure continuity of facilities and environmental systems at primary and alternate processing sites. Testing strategies should include the adequacy of back-up power generators and heating, ventilation, and air conditioning systems to meet business recovery objectives at operating centers. Workspace recovery test strategies should include assessments of the availability and adequacy of workspace, desktop computers, network connectivity, e-mail access, telephone service, and physical security controls. For institutions relying on the physical relocation of hardware, software, or data storage devices to recover the technology infrastructure and applications at alternate locations, the facilities testing strategy should address the secure transportation of these items.

Complexity

Organizations should develop testing strategies that demonstrate their ability to support connectivity, functionality, volume, and capacity using alternate facilities. The testing strategies should encompass internal and external dependencies, including activities outsourced to domestic and offshore business and technology service providers.**For critical business functions, test strategies and plans may need to extend beyond network connectivity and include transaction processing to assess capacity and data integrity.**

Test Planning

Crises management Test Plans

Test scenarios, plans, and objectives should include the institution's crisis management

function to demonstrate the institution's ability to respond effectively to contingency events. The crisis management program should be tested, with particular emphasis on the institution's capability to gather information about the threat or event, initiate the BCP, and communicate relevant information to the appropriate staff, customers, vendors, service providers, regulators and other public authorities. Crisis management test plans should address the ability of crisis management team members, and their alternates, to carry out their designated responsibilities under various event scenarios.

Test Scripts

Test scripts provide sequential procedures related to testing specific business or technology functions. Test scripts can be readily used by employees to test business processes within pre-established timeframes, and test scripts should include references to production documentation and procedures. Each test script should clearly document the test objective and procedures, including:

- Detailed information regarding the application, business processes, system, or facility to be tested;
- Sequential test steps to be performed by employees or external parties;
- Prompts for test participants to record quantifiable test metrics;
- Procedures to be followed for manual work-around processes, if applicable;
- A detailed schedule for completion of the test;
- Prompts for participants to record issues encountered with the continuity plan during the test; and
- Prompts for participants to record suggestions for improving continuity plans and associated test methods.

Test scripts may include steps for rotating staff involved in specific tests to simulate the inaccessibility of key employees during a disaster.

TESTING EXPECTATIONS FOR CORE CLEARING AND SETTLEMENT ORGANIZATIONS AND FIRMS THAT PLAY SIGNIFICANT ROLES IN CRITICAL MARKETS

The guidance provided in this section describes additional expectations regarding business continuity testing for those organizations that perform core clearing and settlement activities in critical financial markets (core firms) and those organizations that process a significant share of transactions in critical financial markets (significant firms). These organizations have been advised by their regulators that they have met the definition of a core or significant firm as set forth in the "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" (Sound Practices Paper).

Core and significant firms that are subject to the Sound Practices Paper should develop verification strategies and execute testing activities to validate the implementation of the interagency guidelines. The following discussion is not meant to limit the testing

strategies or activities of core and significant firms and should be read in conjunction with more comprehensive guidance, available in the public and private sectors, to evaluate the scope and test the effectiveness of business continuity plans.

Verification Strategies

In general, core and significant firms should have a comprehensive, risk-based approach for testing and evaluating the effectiveness of all of its internal business continuity arrangements. It would be appropriate to include documented strategies and plans to determine whether the core or significant firm has established the facilities and arrangements necessary to assure substantial achievement of the recovery objectives and other expectations set forth in the Sound Practices Paper. In this regard, the Sound Practices Paper advises core and significant firms to routinely use or test their individual internal recovery and resumption arrangements for connectivity, functionality, and volume capacity. It is also suggested that significant firms, which have back-up sites within the current perimeter of synchronous back-up technology or that rely primarily on employees from the same workforce as the primary site, confirm that their plans would be effective if a wide-scale disruption affects both sites.

Moreover, in light of the dependencies between core firms and significant firms and the potential impact that a prolonged disruption of clearance and settlement activities would have on the operation of the financial system, verification strategies should include an external component. This external component should help the agencies and core and significant firms assess whether there is a consistent level of resilience across critical financial markets and whether their recovery arrangements are compatible.

Because of their critical role in the operation of financial markets, the external verification strategies of core firms should include ample opportunities for significant firms to test their recovery of critical clearing and settlement activities from their alternate processing sites. Significant firms are expected to test with the relevant core firms from their alternate sites and meet any testing requirements the core firms establish specifically for significant firms and for participants more generally. Significant firms should take advantage of these opportunities to test their ability to meet the recovery time objectives (RTOs) set forth in the Sound Practices Paper from their geographically dispersed alternate sites. Core firms and significant firms also are encouraged to participate in pertinent market-wide and cross-market tests (such as the "street tests" sponsored by the Securities Industry Association, Bond Market Association, and Futures Industry Association) that test connectivity from alternate sites and include transaction, settlement, and payment processes, to the extent practical. Verification strategies should incorporate lessons learned from prior tests and exercises to improve their effectiveness in validating back-up strategies.

Testing Scope

Internal testing activities should confirm that each core and significant firm has identified all clearing and settlement activities, as well as the systems that support or are integrally related to the performance of those activities, for each critical market in which they are core or significant. These activities should also be designed to demonstrate the core and significant firm's ability to complete pending material payments and transactions, access funding, manage material open risk positions, and make related entries to books and records in the event of a wide-scale disruption from alternate geographically dispersed data centers and operations facilities. Moreover, testing activities should confirm that such critical clearing and settlement activities could be recovered within RTOs set forth in the Sound Practices Paper.

As noted earlier, test programs should address external interdependencies, such as connectivity to markets, payment systems, clearing agencies, messaging services, and other critical service providers. Moreover, test programs should validate the effectiveness of internal and external communication protocols with stakeholders. Test scenarios should include a wide-scale disruption in which primary data centers and operations facilities are rendered inoperable for some period without notice, making it necessary to recover critical clearing and settlement activities from an alternate site. Core firms should confirm that resumption of critical clearing and settlement activities can be sustained at alternate sites. Core or significant firms that use the same alternate sites or whose alternate sites rely on the same employees as their primary sites should assume that employees at primary sites are unavailable to clear or settle pending transactions for several days, or are that some employees are unavailable for longer period of time.

Supervisory Expectations

Examination and supervisory activities will include evaluations of verification strategies and test plans in order to assess whether core and significant firms, which are subject to the Sound Practices Paper, have achieved the resilience necessary to protect the financial system from a wide-scale disruption. Verification strategies should be incorporated into implementation plans and should have an external as well as internal component. If a core or significant firm finds it necessary to make incremental changes in its recovery strategies, it should modify its verification strategies and test plans to incorporate those changes. Core and significant firms should perform robust testing to assess the effectiveness of their recovery strategies. Verification strategies, test plans and test results should be documented and subject to a qualified, independent review, such as an internal or external audit. The agencies will evaluate a core and significant firm's verification strategies and test plans, the execution of such strategies and plans, and the test results.

Appendix I: Laws, Regulations, and Guidance

Federal Financial Institutions Examination Council

- FFIEC: Lessons Learned from Hurricane Katrina: Preparing Your Institution for a Catastrophic Event (June 2006)

Federal Deposit Insurance Corporation

- 12 CFR Part 364: Interagency Guidelines Establishing Standards for Safety and Soundness, Appendix A (N/A)
- 12 CFR Part 364: Interagency Guidelines Establishing Information Security Standards, Appendix B (N/A)
- FIL-6-2008: Interagency Statement on Pandemic Planning (February 6, 2008)
- FIL-25-2006: Influenza Pandemic Preparedness Interagency Advisory (March 15, 2006)
- FIL-84-2002: Interim Sponsorship Policy for Government Emergency Telecommunications Service (GETS) Cards (August , 2002)
- FIL-68-2001: 501(b) Examination Guidance (August 24, 2001)
- FIL-81-2000: Risk Management of Technology Outsourcing (November 29, 2000)

Federal Reserve Board

- 12 CFR Part 208: Interagency Guidelines Establishing Standards for Safety and Soundness, Appendix D-1 (N/A)
- 12 CFR Part 208: Interagency Guidelines Establishing Information Security Standards (State Member Banks), Appendix D-2 (N/A)
- SR Letter 07-18: FFIEC Guidance on Pandemic Planning (December 12, 2007)
- SR Letter 06-5: Influenza Pandemic Preparedness (March 15, 2006)
- SR Letter 06-3: Interagency Supervisory Guidance for Institutions Affected by Hurricane Katrina (February 3, 2006)
- SR Letter 05-24: Interagency Questions and Answers for Financial Institutions in Response to Hurricanes Katrina and Rita (December 2, 2005)

- SR Letter 05-17: Katrina Related Marketing Practices Invoking the Name of the Federal Reserve (September 22, 2005)
- SR Letter 05-16: Supervisory Practices Regarding Banking Organizations and Consumers Affected by Hurricane Katrina (September 15, 2005)

National Credit Union Administration

- 12 CFR Part 748: Guidelines for Safeguarding Member Information, Appendix A (N/A)
- 12 CFR Part 749: Record Preservation Program and Record Retention, Appendix A and B (N/A)
- NCUA Letter to Credit Unions 08-CU-01: Guidance on Pandemic (January 2008)
- NCUA Risk Alert 06-Risk-01: Disaster Planning and Response (April 2006)
- NCUA Letter to Credit Unions 06-CU-06: Influenza Pandemic Preparedness (March 2006)
- NCUA Letter to Credit Unions 02-CU-17: e-Commerce Guide for Credit Unions (December 2002)
- NCUA Letter to Credit Unions 01-CU-21: Disaster Recovery and Business Resumption Contingency Plans (December 2001)
- NCUA Letter to Credit Unions 98-CU-12: Business Resumption Contingency Planning (June 1998)

Office of the Comptroller of the Currency

- 12 CFR Part 5.30: Establishment, Acquisition, and Relocation of a Branch (N/A)
- 12 CFR Part 30: Guidelines Establishing Standards for Safety and Soundness, Appendix A (N/A)
- 12 CFR Part 30: Interagency Guidelines Establishing Information Security Standards, Appendix B (N/A)
- OCC Bulletin 2007-49: Pandemic Planning: Interagency Guidance (December 18, 2007)
- OCC Bulletin 2006-26: Disaster Planning - Hurricane Katrina: Lessons Learned (June 15, 2006)
- OCC Bulletin 2006-12: Influenza Pandemic Preparedness [Interagency] (March 5, 2006)

- OCC Bulletin 2006-6: Community Reinvestment Act: Hurricanes Katrina and Rita (February 9, 2006)
- OCC Bulletin 2005-36 [Interagency]: Statement and Order: Hurricanes Katrina and Rita (October 4, 2005)
- OCC Bulletin 2003-14: Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System (April 8, 2003)
- OCC Bulletin 2002-33: GETS (July 23, 2002)
- OCC Bulletin 98-3: Technology Risk Management (February 4, 1998)

Office of Thrift Supervision

- 12 CFR Part 570: Interagency Guidelines Establishing Standards for Safety and Soundness, Appendix A (N/A)
- 12 CFR Part 570: Interagency Guidelines Establishing Information Security Standards, Appendix B (N/A)
- PR 07-089: Interagency Statement on Pandemic Planning (December 12, 2007)
- CEO Ltr 239: Hurricane Katrina: Industry Lessons Learned (June 15, 2006)
- CEO Ltr 237: Interagency Advisory on Influenza Pandemic Preparedness (March 15, 2006)
- CEO Ltr 234: Interagency Supervisory Guidance for Institutions Affected by Hurricane Katrina (February 3, 2006)
- CEO Ltr 165: Financial Banking Infrastructure Information Committee (FBIIC) Interim GETS Sponsorship Policy (July 26, 2002)

External Resources

- The Joint Forum, High-level Principals for Business Continuity (August 2006)
- Pandemic Influenza - Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources (June 2006)
- Statement on Preparations for "Avian Flu" (January 2006)
- Business Pandemic Influenza Planning Checklist (December 2005)
- National Strategy for Pandemic Influenza (November 2005)
- Best Practices to Assure Telecommunications Continuity for Financial Institutions

and the Payment and Settlement Utilities: Report by the Assuring Telecommunications Continuity Task Force (September 2004)

- The President's National Security Telecommunications Advisory Committee: Financial Services Task Report (April 2004)
- Contingency Planning Guide for Information Technology Systems, NIST SP 800-34 (June 2002)

Appendix J: Strengthening the Resilience of Outsourced Technology Services

Background and Purpose

Many financial institutions depend on third-party service providers to perform or support critical operations. These financial institutions should recognize that using such providers does not relieve the financial institution of its responsibility to ensure that outsourced activities are conducted in a safe and sound manner. The responsibility for properly overseeing outsourced relationships lies with the financial institution's board of directors and senior management. An effective third-party management program should provide the framework for management to identify, measure, monitor, and mitigate the risks associated with outsourcing. [23]

When a financial institution relies upon third parties to provide operational services, they also rely on those service providers to have sufficient recovery capabilities for the specific services they perform on behalf of the financial institution. In addition to providing systems and processing, technology service providers (TSPs) may also be retained by a financial institution to provide information technology (IT) recovery capabilities for the financial institution's internal systems. Effective business continuity planning (BCP) and testing demonstrate the financial institution's ability not only to recover IT systems, but also to return critical business functions to normal operations within established recovery time objectives (RTOs). A financial institution should be able to demonstrate the ability to recover critical IT systems and resume normal business operations regardless of whether the process is supported in-house or at a TSP for all types of adverse events (e.g., natural disaster, infrastructure failure, technology failure, availability of staff, or cyber attack [24]).

This appendix discusses four key elements of BCP that a financial institution should address to ensure they are contracting with TSPs that are strengthening the resilience of technology services:

- Third-party management addresses a financial institution management's responsibility to control the business continuity risks associated with its TSPs and their subcontractors.
- Third-party capacity addresses the potential impact of a significant disruption on a third-party servicer's ability to restore services to multiple clients.
- Testing with third-party TSPs addresses the importance of validating business continuity plans with TSPs and considerations for a robust third-party testing program.
- Cyber resilience covers aspects of BCP unique to disruptions caused by cyber events.

Third-Party Management

Establishing a well-defined relationship with TSPs is essential to business resilience. A financial institution's third-party management program should be risk-focused and provide oversight and controls commensurate with the level of risk presented by the outsourcing arrangement. To ensure business resilience, the program should include outsourced activities that are critical to the financial institution's ongoing operations. Attention to due diligence, contract management, and ongoing monitoring of TSPs is important to maintaining business resilience. The FFIEC IT Examination Handbook's "Outsourcing Technology Services Booklet" addresses expectations for managing third-party relationships. This section of the appendix focuses on business-resiliency aspects of third-party management.

Due Diligence

A financial institution should evaluate and perform thorough due diligence before engaging a TSP. A financial institution should consider the maturity of new technologies and gain an understanding of the benefits and risks of engaging TSPs using such technologies during the due diligence process. Improvements in technologies have the potential to strengthen business resilience, but may introduce new and different risks (e.g., shared access to data, virtual exploits, and authentication weaknesses). As part of its due diligence, a financial institution should assess the effectiveness of a TSP's business continuity program, with particular emphasis on recovery capabilities and capacity. [25] In addition, an institution should understand the due diligence process the TSP uses for its subcontractors and service providers. Furthermore, the financial institution should review the TSP's BCP program and its alignment with the financial institution's own program, including an evaluation of the TSP's BCP testing strategy and results to ensure they meet the financial institution's requirements and promote resilience.

Contracts

The terms of service should be defined in written contracts [26] that have been reviewed by a financial institution's legal counsel and subject matter experts before execution. Contract terms that can impact the financial institution's ability to ensure effective business resilience include the following:

- Right to audit: Agreements should provide for the right of the financial institution or its representatives to audit the TSP and/or to have access to audit reports. A

financial institution should review available audit reports addressing TSPs' resiliency capabilities and interdependencies (e.g., subcontractors), BCP testing, and remediation efforts, and assess the impact, if any, on the financial institution's BCP.

- Establishing and monitoring performance standards: Contracts should define measurable service level agreements (SLAs) for the services being provided. For business continuity expectations, clear recovery time objectives and recovery point objectives (RPOs) should be addressed.

- Default and termination: Contracts should define events that constitute contractual default (e.g., the inability to meet BCP provisions, SLAs, and/or RTOs) and provide a list of acceptable remedies and opportunities for curing a default.

- Subcontracting: If agreements allow for subcontracting, the TSP's contractual provisions should also apply to the subcontractor. Contract provisions should clearly state that the primary TSP has overall accountability for all services that the TSP and its subcontractors provide, including business continuity capabilities. Agreements should define the services that may be subcontracted, the TSP's due diligence process for engaging and monitoring subcontractors, and the notification requirements regarding changes to the TSP's subcontractors. The contractual provisions should also address the right to audit and BCP testing requirements for subcontractors. Additionally, agreements should include the TSP's process for assessing the subcontractor's financial condition.

- Foreign-based service providers: A financial institution should review data security controls of foreign-based TSPs or foreign-based subcontractors that back up and/or store data offshore. Because information security and data privacy standards may be different in foreign jurisdictions, the contract should clearly address the need for data security and confidentiality to, at a minimum, adhere to U.S. regulatory standards.

- BCP testing: Contracts should address the financial institution's BCP testing requirements [27] for the TSPs. The contract should define testing frequency and the availability of test results. The contract should also include the financial institution's ability to participate in the TSP's BCP testing on a periodic basis. [28]

- Data governance: Contracts should clearly define data ownership and handling expectations during the relationship and following the conclusion of the contract. This may include data classification, integrity, availability, transport methods, and backup requirements. In addition, expectations for data volume and growth should be addressed.

- TSP updates: Contracts should empower a financial institution to request information from its service provider(s) describing the TSP's response to relevant regulations, supervisory guidance, or other notices published by any of the federal banking agencies.

- Security issues: Contracts should clearly state the responsibility of the TSP to address security issues associated with services and, where appropriate, to communicate the issue(s) and solution(s) to its financial institution clients. Additionally, responsibilities for incident response should be incorporated. The contract should include notification responsibilities for situations where breaches in security result in unauthorized intrusions to the TSP that may materially affect the financial institution clients.

Ongoing Monitoring

Management should effectively monitor TSP performance throughout the life of the contract. Effective ongoing monitoring assists the financial institution in ensuring the resilience of outsourced technology services. The financial institution should perform periodic in-depth assessments of the TSP's control environment, including BCP, through the review of service provider business continuity plan testing activities, independent and/or third party assessments [29] , and management information systems (MIS) reports [30] to assess the potential impact on the financial institution's business resilience. The financial institution should ensure that results of such reviews are documented and reported by the TSP to the appropriate management oversight committee or the board of directors and used to determine any necessary changes to the financial institution's BCP and, if warranted, the service provider contract.

Strategic Considerations - Third-Party Management

Financial institution management should ensure business resilience considerations are embedded within their third-party risk management life cycle. This includes addressing business continuity elements within the due diligence process, contract negotiations, ongoing monitoring processes, and processes for termination of the contract. This should also include considerations relative to service providers' use of subcontractors. Finally, the oversight and controls on outsourced activities should be commensurate with the level of risk presented by these arrangements.

The financial institution should ensure that each TSP has a robust third-party management program that includes a review of each subcontractor's business continuity plan. The failure of a subcontractor could result in the failure of the TSP's ability to provide contracted services.

Third-Party Capacity

An increasing concentration risk corresponds to financial institutions' increased use of third-party service providers. That, in conjunction with industry consolidation, has resulted in fewer, more specialized TSPs providing services to larger numbers of financial institutions. This trend increases the potential impact of a scenario in which a TSP is required to support recovery services to large numbers of financial institutions due to a widespread disaster. In addition, a business disruption at a single TSP may affect critical services provided to a large number of institutions dependent on those services. In both scenarios, it is critical that the TSP have sufficient capacity to meet RTOs and RPOs needed by the financial institution clients.

As reliance on technology increases, a financial institution is less able to withstand the absence of a critical serviced function. Outsourcing diminishes the IT self-sufficiency of

financial institution staff because of the increased dependence on the TSP for technical support. The increased reliance on technology for all daily processes means it is no longer feasible for a financial institution to operate manually for an extended length of time. Additionally, because TSPs operate many critical processes, it is difficult for a serviced client to quickly move these processes internally or to another TSP.

Significant TSP Continuity Scenarios

The significant size and client concentration of larger TSPs increases the potential impact of service disruptions across major segments of the financial industry, increasing the importance of resilience for these organizations. Natural disasters, physical threats, and cyber attacks could have a significant effect on servicer capabilities. Beyond physical and cyber threats, financial pressures can lead service providers to make decisions not to invest fully in appropriate security controls or resilience measures that would facilitate continuity of operations. In cases of extreme financial distress, it may not be financially viable for a servicer to continue making necessary product updates, or even to continue operations. Without advance notice or awareness of deterioration in a TSP's financial condition, the financial institution clients might not have appropriate time to make alternate processing arrangements.

TSP Alternatives

It is incumbent on financial institutions and third-party service providers to identify and prepare for potentially-significant disruptive events, including those that may have a low probability of occurring but would have a high impact on the institution. In spite of such planning, there may be circumstances that cause a service to be unavailable for longer than a committed and tested RTO. In these situations, a financial institution and its TSPs should assess the impact on their respective customers and take the necessary steps to minimize the impact of the event. In extreme scenarios, where a TSP can no longer effectively perform its responsibilities, a new TSP may have to assume operations. Depending upon the specific circumstances, a new TSP may convert the financial institution to its systems and move them to its data center. Alternatively, the new TSP could assume control of the existing data center running the existing systems. If no alternate TSP is available, the financial institution may have to move the operations in-house. The latter is generally not a valid option, as the reasons to outsource include a lack of expertise or financial resources to run services in-house and, therefore, moving them with little or no notice would exacerbate these limitations.

If operations at a TSP cease, for most applications, the length of time required to convert a financial institution to an alternate system would greatly exceed any reasonable RTO for an application that abruptly ceased. There are three possible solutions in the event of a TSP failure. The first is for the financial institution clients of a failed service provider to assume the operation of the service either by contracting with an alternate TSP or performing the services themselves at the existing site. This would require a steep learning curve for the new TSP or the financial institution clients taking over the application. Second, the financial institution clients could convert to an alternate TSP's application. There would still be a delay, however, as they would need to prepare

infrastructure at the new site, convert data if necessary, and perform functional testing before resuming the service. The third solution would be to move the existing critical infrastructure to an alternate TSP that could successfully and securely take over and run the application or service at its site. This assumes that the alternate TSP would not be affected by the situation that prevented the original TSP from fulfilling its servicing responsibilities and that the alternate TSP would have the necessary expertise to provide the service. [31]

Regardless of the option selected, the ability of an alternate TSP or the financial institution clients to take over processing responsibilities assumes the following items. The problem TSP's data center has workable backup systems or infrastructure that would facilitate transition to an alternate TSP. The alternate TSP (or the financial institution clients) has sufficient capacity in space, systems, and personnel to deliver the service effectively.

A financial institution should have contingency plans in place to address alternatives for the resilience of services supporting critical operations if the current TSP cannot continue to provide the service. These plans should identify alternate TSPs or in-house arrangements and preparations required for such a conversion to the extent possible.

Strategic Considerations - Third-Party Capacity

A critical failure at a service provider potentially could have large-scale consequences. A financial institution should ensure that its TSPs have adequate planning and testing strategies that address severe events in order to identify single points of failure that would cause wide-scale disruption. Given the increased concentration of providers in the TSP industry, a financial institution should ensure that it has identified, and potentially prearranged, a comprehensive set of alternative resources to provide full resilience of operations in such scenarios.

There are certain steps a financial institution can take with their TSPs to plan for the possible failure of critical services. First, the parties can discuss scenarios of significant disruptions that may necessitate transitioning critical services to alternate TSPs. Second, the parties can assess their immediate or short-term space, systems, and personnel capacity to absorb, assume, or transfer failed operations. Last, the parties can identify the most plausible range of recovery options and develop business continuity plans that address restoration of key services. FFIEC member agencies encourage larger, more complex financial institutions and TSPs to consider industry-wide recovery scenarios that strengthen the resilience of the financial services sector. Institutions of all sizes should consider methods to participate through user groups or industry initiatives to test recovery scenarios.

Testing With Third-Party TSPs

Testing is a critical step in the cyclical BCP process and should be sufficient in scope

and rigor to demonstrate the ability to meet recovery objectives, regardless of whether a service is performed in-house or is outsourced. Third parties provide important services to many financial institutions and as such should be included within the financial institution's enterprise-wide business continuity testing program. The testing program should be based on a financial institution's established risk prioritization and evaluation of the criticality of the functions involved. Testing with third parties should disclose the adequacy of both organizations' ability to recover, restore, resume, and maintain operations after disruptions, consistent with business and contractual requirements.

This booklet discusses expectations, governance, and other attributes of an effective BCP testing program and includes an appendix dedicated to governance and attributes of a testing program. [32] In addition, the FFIEC IT Examination Handbook's "Outsourcing Technology Services Booklet" addresses third-party testing considerations. Financial institutions and third parties should apply the concepts from both booklets to their programs for BCP testing with third parties.

Third-party TSPs typically provide services to more than one financial institution, and the largest providers may service hundreds of institutions. When the volume of clients is large, a TSP may not be able to test with all clients in a set period (e.g., annually). A financial institution, however, should be proactive in managing its third-party relationships, including addressing its testing expectations. A financial institution should ensure it is an active participant in its TSPs' testing programs and that these providers have a testing strategy that includes testing plausible significant disruptive events. Because a provider may not be able to test with all clients on a regular basis, financial institutions should register on any waiting list with the TSP. In the interim, financial institutions should obtain documentation on the scope, execution, and results of testing activity conducted for the services they receive. Any test results that impact the financial institution are to be provided to the board. A financial institution should ensure that it understands its TSP's testing process to ensure that the testing is adequate to meet its continuity expectations.

If a third party provides critical services, the financial institution should conduct periodic BCP testing with reasonable frequency. As noted in the FFIEC IT Examination Handbook's "Outsourcing Technology Services Booklet," critical services require annual or more frequent tests of the contingency plan. As with all BCP testing, the frequency should be driven by the financial institution's risk assessment, risk rating, and any significant changes to the operating environment. To the extent that a test is unsuccessful, any issues identified should be tracked and resolved in a timely manner, according to the severity of the issues. The scope of BCP testing with third parties should be commensurate with the level and criticality of services provided and, in some cases, requires an end-to-end exercise. Finally, the right to perform or participate in BCP testing with third parties should be described within the contract governing the third-party relationship.

Testing Scenarios

A financial institution should develop plausible and realistic scenarios of threats that may potentially disrupt business processes and the financial institution's ability to meet both business requirements and customers' expectations. These scenarios should include those threats that may affect services provided by third parties to test the incident response plan and crisis management, including communication processes with third-

party providers and other applicable stakeholders. Testing should demonstrate not only the ability to failover to a secondary site but also the ability to restore normal operations. In addition, the financial institution should develop appropriate scenarios to test their response in the event of a significant event or crisis at the TSP. Scenarios to consider include:

- TSP outage or disruption, resulting in activation of the third party's alternative recovery arrangements. In this scenario, the third party is demonstrating recovery from an outage while the client financial institution has not been directly affected, but the TSP may require some response from the client if auto-failover is not used (e.g., changing telecommunication lines or providers).
- Financial institution outage or disruption. In this scenario, the TSP has not been directly affected but has to react to address the client's recovery activities and needs.
- Cyber events demonstrating the financial institution's and third-party provider's ability to respond quickly and efficiently to such an event. For example, a financial institution's ability to recover from a disruption of critical functions because of a distributed denial of service (DDoS) attack or the ability to recover from a data corruption event should be subject to testing. A financial institution may consider working with an outside party, such as other financial institutions or an industry group, to test these types of events.
- Simultaneous attack affecting both the institution and its service provider.

Testing Complexity

A financial institution should develop testing strategies that demonstrate its ability to support connectivity, functionality, volume, and capacity using alternate facilities. The testing strategies should encompass internal and external dependencies, including activities outsourced to domestic and foreign-based TSPs.

Lessons learned from natural disasters and other events highlight that simple testing of network connectivity with a third party is not adequate. For critical business functions, test strategies and plans should be extended beyond third-party network connectivity and include transaction processing and functionality testing to assess infrastructure, capacity, and data integrity. Documenting transaction flows, as well as developing formal process diagrams or charts, may help ensure that testing effectively identifies interdependencies and end-to-end processes.

In striving to increase the effectiveness of test scenarios over time, the financial institution should, as appropriate, consider the following:

- Performing integrated tests or exercises that incorporate more than one system or application, as well as external dependencies, to gauge the effectiveness of continuity plans for a business line or major function.
- Testing interdependencies where two or more departments, business lines,

processes, functions, and/or third parties support one another.

- Conducting end-to-end exercises to demonstrate the ability of the financial institution to recover a business process from initiation (e.g., customer contact) through process finalization (e.g., transaction closure), including functions provided by a TSP.
- Conducting full-scale exercises that involve recovery of systems and applications in an interactive manner in a recovery environment, including all critical functions and modules provided by a TSP.
- Performing exercises that include the financial institution's third-party provider's subcontractors, vendors, or servicers.

By increasing the scope and effectiveness of testing with TSPs over time, a financial institution should achieve a robust third-party testing program that includes the financial institution's recovery capabilities. Increasing test complexity helps identify weaknesses in the financial institution's business continuity plan. Financial institution management should ensure that any issues identified with either their recovery capabilities or those of their TSPs are documented with action plans and target dates for resolution.

Strategic Considerations - Testing With TSPs

Testing with third parties involves challenges because of the number of clients being serviced and the TSP's need to maintain daily operations. There are a number of strategic objectives, however, that a financial institution needs to address in an effective third-party BCP testing program.

A client financial institution needs assurance that its third-party service providers have the necessary capacity to restore critical services in the event of a widespread disruption or outage. This assurance includes adequate infrastructure and personnel to restore services to financial institution clients and support typical business volumes. Clients gain assurance through an effective BCP testing program.

Because not all clients can participate in every testing activity, TSPs should be transparent about testing activities and results and should provide information that facilitates third-party relationship monitoring. Service providers should share test results and reports, remediation action plans and status reports on their completion, and related analysis/modeling. In most instances, proxy testing [33] will not fully capture each financial institution's unique operational needs; therefore, each financial institution should participate in its TSP's BCP testing program when possible. Appropriate testing for the most likely significant disruptive scenarios provides assurances that financial institutions and service providers will be better prepared to recover from these events.

Following testing, the financial institution should evaluate the results and understand any gaps that may exist between the service provider and the institution. A plan should be developed to ensure these gaps are addressed as appropriate.

Cyber Resilience

The increasing sophistication and volume of cyber threats and their ability to disrupt operations or corrupt data can affect the business resilience of financial institutions and TSPs. Financial institutions, and their TSPs, need to incorporate the potential impact of a cyber event into their BCP process and ensure appropriate resilience capabilities are in place. The changing cyber threat landscape may include the following risks that must be managed to achieve resilience.

Risks

Malware

Malware represents a serious and growing threat to financial institutions and TSPs as it is focused on achieving high-impact objectives, such as data corruption and unauthorized financial transactions. Anti-malware vendors are continually challenged to keep pace with rapidly proliferating malware threats. For example, "zero-day" [34] exploits can result in significant damage. To strengthen resilience against malware threats, financial institutions and TSPs should use a layered anti-malware strategy, including integrity checks, anomaly detection, system behavior monitoring, and employee security awareness training, in addition to traditional signature-based anti-malware systems. Resilience also calls for the more common controls, such as strong passwords, appropriately controlled mobile devices, controls over access to social networks, hardened [35] software and operating systems, and controlled and monitored Internet access.

Insider Threats

Cyber threats can be launched from within a financial institution or TSP by a disgruntled employee or a person placed in the financial institution deliberately to carry out a cyber attack. The financial institution should consider the possibility that a knowledgeable insider may cause a disruptive event and the potential impact of the event on business resilience. Employee screening, dual controls, and segregation of duties are some examples of controls that can help to mitigate the risks of an insider attack.

Data or Systems Destruction and Corruption

A cyber attack may simultaneously target production data and online backups for destruction or corruption. It may also target the destruction of hardware. Data destruction occurs when data are erased or rendered unusable. Data corruption occurs when data

are altered without authorization. Either can occur inadvertently or through malicious intent. In some cases of data corruption, data may appear usable but produce unexpected and undesirable results. A financial institution or TSP may not become aware that data has been corrupted for some period of time after an event, and may find it difficult to determine the extent of the problem. Thus, data corruption may have a greater impact on the financial institution and require a different recovery response than cases of data destruction.

Data replication can be an effective strategy for rapid recovery in the event of data destruction or data corruption. Data replication, however, may also be susceptible to simultaneous cyber attacks, and using this replication strategy may inadvertently result in backup or replicated data being destroyed or corrupted along with the production data. For effective business resilience, the financial institution and TSP should take steps to ensure that replicated backup data cannot be destroyed or corrupted in an attack on production data. If data are replicated in near real time, the financial institution and service provider should consider the vulnerability of their backup systems to an attack that impacts both simultaneously. Management at the financial institution and the TSP should ensure appropriate redundancy controls and segregation of replicated backup data files to provide for sufficient recovery capabilities against these threats.

Another control for consideration is an "air-gap," a security measure in which a computer, system, or network is physically separated from other computers, systems, or networks. An air-gapped data backup architecture limits exposure to a cyber attack and allows for restoration of data to a point in time before the attack began. Alternatively, a periodic read-only data backup entails the transmission of data to a physically and logically separate read-only backup location. These and other emerging data backup techniques address cyber attacks and mitigate the risk of corrupt data being replicated.

The objective of these strategies is to allow financial institutions and TSPs to maintain relatively current data backups without the risk of an attack destroying or corrupting the backup data. Financial institutions and TSPs should develop specific procedures for the investigation and resolution of data corruption in response and recovery strategies. Also, financial institutions and TSPs should ensure that data integrity controls [36] are in place to detect possible corruption in production and backup data.

Some financial institutions have deployed cloud-based disaster recovery services [37] as part of their resilience program. These services have unique data integrity risks and, therefore, financial institution management should assess services before implementation and reassess them periodically after deployment, as the technology, capability, and threats change. Financial institutions should ensure that cloud-based disaster recovery services protect against data destruction or corruption with the same level of assurance as non-cloud-based disaster recovery solutions. Financial institutions and their TSPs should ensure that appropriate security is in place for virtualized [38] cloud recovery services.

In addition, financial institutions and TSPs should have plans and processes to reconstitute their operations after a destructive attack.

Communications Infrastructure Disruption

Cyber attacks, such as DDoS attacks, can be used to disrupt communications and may

target underlying infrastructures directly. Financial institutions' business resilience strategies depend on functioning communication links between various entities, including TSPs. The following possible scenarios could jeopardize ongoing operations:

- Reliance on a single communications provider, potentially creating a single point of failure.
- Disruptions that affect multiple financial institutions due to TSP concentration.
- Simultaneous disruptions of telecommunications and electronic messaging due to the convergence of voice and data services in the same network.
- Disruption of data and voice communications between other entities and TSPs.

A financial institution should recognize these possible scenarios and plan for alternate communications infrastructure, if available. FFIEC member agencies recognize that it may be difficult to achieve complete data communications resilience through independent redundant infrastructure, but the financial institution should explore alternatives.

Simultaneous Attack on Financial Institutions and TSPs

Business continuity plans frequently rely on the fact that production and backup facilities are separated by geography, such that a disaster in one geographic area will not affect a backup facility located a sufficient distance away. Cyber attacks, however, are not limited by geography and can target facilities located anywhere in the world. For example, a cyber attack can be directed against a financial institution's production and backup facilities simultaneously, rendering both inoperable. Similarly, a cyber attack could target both a financial institution and its TSPs. Cyber attacks may also be executed in conjunction with disruptive physical events and may affect multiple critical infrastructure sectors (e.g., the telecommunications and energy sectors). Financial institutions and TSPs should consider their susceptibility to simultaneous attacks in their business resilience planning, recovery, and testing strategies.

Strategic Considerations - Cyber Resilience

The ability of financial institutions and TSPs to respond effectively to a cyber attack is critical to business resilience. The financial institution should consider the following mitigating controls:

- Data backup architectures and technology that minimize the potential for data destruction and corruption;

- Data integrity controls, such as check sums;
- Independent, redundant alternative communications providers;
- Layered anti-malware strategy;
- Enhanced disaster recovery planning to include the possibility of simultaneous attacks;
- Increased awareness of potential insider threats;
- Enhanced incident response plans reflecting the current threat landscape; and
- Prearranged third-party forensic and incident management services.

Financial institutions and TSPs should consider the cyber risks and controls discussed above, incorporate them into their BCP, as appropriate, and periodically test their ability to resume normal operations after a cyber attack.

Cyber threats will continue to challenge business continuity preparedness. Financial institutions and TSPs should remain aware of emerging cyber threats and scenarios and consider their potential impact to operational resilience. Because the impact of each type of cyber event will vary, preparedness is the key to preventing or mitigating the effects of such an event.

Incident Response

Financial institutions and their service providers should anticipate potential cyber incidents and develop a framework to respond to these incidents. If a financial institution or its TSP is under attack, management should consider the potential impact of any decision to limit or suspend processing and any downstream implications to the financial institution's business partners, customers, or other TSPs. Incident response processes should also address concerns regarding availability, confidentiality, and integrity of data with different sensitivities. [39] Finally, the financial institution and its TSPs should periodically update and test their incident response plan to ensure that it functions as intended, given the rapidly changing threat landscape.

A financial institution experiencing a cyber attack may need to simultaneously investigate an ongoing security incident and execute the financial institution's recovery strategies. As a result, the financial institution and TSP should consider identifying and making advance arrangements for third-party forensic and incident management services. Also, a financial institution relying on such third-party services should plan for potential limited availability during a large-scale cyber event.

Conclusion

When using third-party service providers, management should ensure adequate business resiliency through:

- Third-Party Management, which involves due diligence procedures, regular monitoring, and strategic, integrative considerations with third-party servicers;
- Third-Party Capacity, which considers third parties' abilities to deliver essential services under adverse scenarios, in addition to possible alternatives in the event of third-party failure;
- Testing with Third-Party TSPs, which involves testing the business continuity resilience among the financial institution and third-party service providers, in addition to the review of test results and remediation of any observed weaknesses; and
- Cyber Resilience, which involves identification and mitigation of cyber threats to data and operational infrastructure, as well as effective incident response procedures to cyber attacks.

As stated throughout this appendix, the key concept maintains that regardless of whether the systems and resilience capabilities are managed by the financial institution or TSP, the financial institution's management and board are responsible for the oversight and assurance of continuing operations in a timely manner.

Additional References

- 12 CFR 364, Appendix B, "Interagency Guidelines Establishing Standards for Safeguarding Customer Information"
- 12 CFR 304.3(d), "FDIC Rules and Regulations: Notification of Performance of Bank Services" (also see FDIC FIL-49-1999)
- 12 CFR 208, Appendix D-2, "Interagency Guidelines Establishing Standards for Safeguarding Customer Information"
- 12 CFR 30, Appendix B, "Interagency Guidelines Establishing Standards for Safeguarding Customer Information"
- FFIEC IT Examination Handbook, "Outsourcing Technology Services Booklet"

- FFIEC IT Examination Handbook, "Information Security Booklet"
- FDIC RD Memorandum 2008-020, "Guidance for Managing Third-Party Risk"
- FDIC FIL-81-2000, "Risk Management of Technology Outsourcing"
- FDIC FIL-50-2001, "Bank Technology Bulletin on Outsourcing"
- FDIC FIL-27-2005, "Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice"
- FDIC FIL-44-2008, "Third-Party Risk: Guidance for Managing Third-Party Risk"
- FRB SR Letter 03-09, "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System"
- FRB SR Letter 12-14, "Revised Guidance on Supervision of Technology Service Providers"
- FRB SR Letter 13-19 / CA Letter 13-21, "Guidance on Managing Outsourcing Risk"
- OCC Bulletin 2002-16, "Bank Use of Foreign-Based Third-Party Service Providers"
- OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance"
- NCUA LCU: 07-CU-13, "Evaluating Third-Party Relationships"
- NCUA Supervisory Letter No.: 07-01, "Evaluating Third-Party Relationships"
- NCUA LCU: 01-CU-20, "Due Diligence Over Third-Party Service Providers"

- NIST SP 800-35, "Guide to Information Technology Security Services"

- BITS Framework for Managing Technology Risk for Service Provider Relationships, revised May 2008, Financial Services Roundtable: BITS