Introduction

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

An inadequate BCP exposes an FHLBank to operational risk. The inability to fulfill legal obligations and provide continuous services in a disaster may result in legal liability to the institution well as a tarnished reputation in the marketplace.

The critical path for recovery must be well defined when responding to a widespread loss of the FHLBank's computer systems and services. The BCP must address the critical functions and processes of the FHLBank and clearly identify priorities in personnel and technology to restore business activities with maximum speed and minimum impact to customers.

Planning and processing for a disabling event not only requires a commitment from an FHLBank's management and employees, but the incurrence by the FHLBank of additional costs associated with the operation of alternate facilities and communication networks, transportation of people, equipment and supplies, and payment of overtime pay.

The BCP should be designed to communicate to appropriate FHLBank staff the activities that are to be undertaken to restore the FHLBank's operations if the facilities or critical systems are temporarily or indefinitely inaccessible. The BCP should provide for the restoration of facilities, communications, computer hardware, software, personnel, and other components necessary for the continuity of critical FHLBank functions.

Regulatory Environment

The primary regulations, standards and guidance that pertain to business continuity planning are set forth below. The discussion does not address the application of authorities other than the FHLBank Act and the regulations, interpretations and issuances of the Finance Board to the FHLBanks. The examiner should ensure that the application of such authorities to an FHLBank has been considered by the FHLBank and its legal counsel.

1) Rules and Regulations of the Federal Housing Finance Board, which include the

following parts and sections relevant to business continuity planning:

Part 917 of the Finance Board's rules and regulations addresses powers and responsibilities of the FHLBank boards of directors and senior management. In particular, Section 917.3, Risk Management, and Section 917.6, Internal Control System, are pertinent.

2) ***Advisory Bulletins of the Federal Housing Finance Board*** that provide supervisory guidance relating to the topic of business continuity planning are the following:

   Advisory Bulletin 03-2, dated February 10, 2003, and Advisory Bulletin 02-3, dated February 13, 2002, which provides guidance on specific attributes to be considered by FHLBanks in the formulation of their business continuity plans, and the establishment of bilateral agreements with other FHLBanks.

   Advisory Bulletin 05-05, dated May 18, 2005, which provides guidance on the risk management responsibilities of the board of directors, senior management and risk management.

3) ***The Information Technology Examination Handbooks for Business Continuity Planning and Operations and other issuances*** issued by the Federal Financial Institutions Examination Council that address specific controls and procedures as to business continuity planning.

FHLBank Environment

Within the FHLBank System, the BCP organizational structure, and content may vary. Each FHLBank and the Office of Finance (OF) approaches BCP differently due to different recovery philosophies, geographical areas, services offered, customer base, recovery needs, and technology infrastructures. Most FHLBanks have recovery plans divided by business unit (BU), and often coordinated by an enterprise-wide recovery plan. Other FHLBanks will centralize the BCP function, which consolidates the detailed recovery plans for all BUs into one master recovery plan. Regardless of the organizational structure, the following six factors are critical aspects of effective business continuity planning:

1) Business continuity planning and recovery should be conducted within an enterprise-wide framework that includes appropriate executive level sponsorship.
2) A thorough business impact analysis (BIA) and risk assessment is the foundation of an effective BCP.
3) Business continuity planning and recovery is more than the recovery of the technology; it is the recovery of business processes.
4) The effectiveness of a BCP can only be validated through thorough testing or practical application.
5) The BCP and test results should be subjected to independent audit.

6) A BCP should be periodically updated to reflect and respond to changes in the institution.

The first phase in developing a BCP is to perform a BIA. All business functions and departments should be included in the BIA, not just information technology. This phase identifies the potential impact of uncontrolled events on the FHLBank's business processes. During this phase management should determine what and how much is at risk by identifying critical business functions and prioritizing them. Management should estimate maximum allowable downtime for critical business processes, establish recovery objectives, and identify potential points for backlogged transactions. Recovery priorities for business processes should identify essential personnel, technologies, facilities, communications systems, vital records, data, and supplies.

The risk assessment is the second phase in developing a BCP. During this phase management should stress test business processes and BIA assumptions against various threat scenarios. Threat scenarios should range in severity from those with high probability of occurrence but low impact, such as brief power outages, to those with a low likelihood of occurrence but high impact such as hurricanes or terrorist attacks. The risk assessment should consider the impact of a broad range of business disruptions on the institution and its customers; the probability of occurrence; the loss impact on information services, technology, personnel, facilities, and service providers; and the safety of vital records. After completing this phase management should identify business processes having the highest priority and estimate how they may be disrupted under various threat scenarios. Worst case scenarios such as destruction of facilities and loss of life should be considered.

Management may leverage internal expertise by engaging third party consultants to assist with the BIA and/or risk assessment; however, management and the board of directors must determine how identified gaps will be addressed.

With the BIA and risk assessment as the foundation, management can develop the written BCP or address gaps in existing plans. Several FHLBanks have appointed a BCP administrator (BCP Administrator), whose primary responsibilities should include:

a) Developing and maintaining a BCP that is responsive to FHLBank's current operating environment and is based on a thorough BIA and risk assessment;
b) Coordinating periodic testing strategies with FHLBank business lines;
c) Analyzing the results of the tests and revising the BCP where appropriate;
d) Reporting the BCP readiness and results of the periodic tests to FHLBank's executive management and the board of directors; and
e) Coordinating business continuity recovery team (BCRT) activity and responding to identified incidents.

The BCRT should consist of senior management and key/technical employees of critical operations and support functions. Its primary function is to ascertain the extent of the disabling event and begin formulating recovery efforts. Once the recovery plan has been

developed, the BCRT communicates instructions to appropriate staff so that a swift and effective recovery can begin. The BCRT provides information on the status of the recovery to executive management in order to assist it in managing the FHLBank's day-to-day business.

The BCP should be focused upon the resumption of those business activities defined as critical during the BIA phase. The order of recovery should be determined by the priority of business functions. Plans should contain detailed instructions on how to resume business in manual mode when the institution's computer systems are inoperable and how to resume business during different periods of the day. Management should also plan for processing capacity should a disruption occur on high volume processing days. The BCP should also include instructions on how to communicate with employees, customers, trade groups, regulatory agencies and the press should a sudden disabling event occur.

The BCP should be reviewed and tested at least annually. Management should consider developing multi-year test strategies that progressively challenge recovery assumptions and make test exercises more complex and robust over time. Successful test strategies should identify gaps or inadequacies in recovery facilities, personnel, and assumptions so that corrective measures can be taken. Depending on the severity of gaps identified follow up tests may be warranted within short timeframes. Although recovery tests should gradually increase in complexity, management should not unduly jeopardize normal business operations when developing test plans. Each department manager or functional area supervisor should be made responsible for reviewing and, if appropriate, updating his/her area's business continuity plans and communicating any changes to the BCP Administrator. Interdependencies between departments, functional areas, and third parties should also be routinely assessed.

Recovery plans should address the manner in which any backlog of activity and/or lost transactions will be recovered and processed at the recovery site. Plans should identify how transaction records will be brought current from the time of the disaster to the expected recovery timeframes. If manual procedures are to be utilized for any period of time written procedures should be developed and employees adequately trained. Test plans should also demonstrate that the use of manual procedures is feasible and for what maximum length of time.

Recovery facilities may vary greatly within the FHLBank System. Some FHLBanks maintain designated recovery facilities while others rely on third-party vendors to provide recovery services. A combination of the two methods may also provide a viable alternative. Regardless of the arrangement, recovery facilities should be tested at least annually and when equipment or application software is changed to ensure continued compatibility. Physical work space and equipment for required personnel is as important as data processing capacity. Contingency planning for recovery facilities should take into account location, size, computer and telecommunications capacity, and required amenities needed to recover critical business functions and accommodate essential personnel. During the recovery site selection process, scalability should be evaluated in

the event that a longer-term disaster occurs. If the recovery period is of more than short duration, the BCP should be reassessed to determine if tertiary plans are warranted.

When determining the physical location of the recovery site(s), management should consider geographic diversity. Management should subject disaster recovery site alternatives to a threat analysis that assesses the likelihood of wide-spread regional events such as terrorist attacks or natural disasters. Locating a recovery center too close to the primary site or in high risk areas may not sufficiently insulate it from such regional events. In any case, management's assumptions should be thoroughly documented, carefully supported, and periodically approved by the board of directors as the board is ultimately responsible for proximity decisions. Independent third party assessments that specifically address distance issues and the FHLBank's unique location can be valuable in analyzing alternatives and validating recovery assumptions.

Risks Associated with Business Continuity Planning

An FHLBank's primary risks relating to business continuity planning are set forth below:

1) Lack of Sound Corporate Governance (Board of Directors and Senior Management Oversight)

a) Key risks and controls are not adequately identified, measured, monitored, and controlled within the framework of an enterprise-wide BCP methodology.
b) BCP does not receive sufficient executive level sponsorship.
c) Risk assessments and/or business impact analyses are inadequate to identify potential threats or sufficiently estimate the resulting impact.
d) Critical recovery needs and timeframes of the FHLBank and its customers are not adequately identified and reflected in recovery planning priorities.
e) Employees do not possess the technical expertise to continue operations in the event of a disaster.
f) Personnel have not been designated to administer the BCP.
g) Duties, responsibilities, and liabilities are not adequately addressed with outside service providers and vendors.
h) A BCP has not been developed and tested.
i) Testing results are not analyzed and reported to the board of directors and senior management. Necessary corrective action is not undertaken to rectify identified weaknesses.
j) Losses due to errors and fraud are not effectively mitigated through insurance or other means.
k) Independent audit coverage and testing is limited; auditors are inexperienced or lack the technical expertise to test the control environment.

2) Operational Risk

a) The BCP has not been adequately developed, communicated to key personnel, tested and kept current commensurate with the degree of complexity of

FHLBank's technological environment to ensure all critical functions can recover in the event of a disabling event.

b) Required data cannot be recreated and required tasks cannot be performed due to a disaster.
c) The recovery site is affected by the same event as the production site.
d) Back-up data is incomplete or inaccessible.
e) The BCP does not provide for alternative manual processes in the event automation is not available at the recovery site.
f) Inadequate testing of the BCP is performed, or the results of the testing are neither reviewed nor evaluated by management. Necessary corrective action is not performed to rectify identified discrepancies.
g) Test transactions are insufficient to validate processing capacity or validate recover objectives at the recover center.
h) Insurance coverage has not been obtained to mitigate risks and exposure, and the extent of effective coverage has not been evaluated.
i) Failure to resume operations within the customer's expected timeframe has led to a damaged reputation in the marketplace.

3) Credit Risk

Legal obligations owed to the FHLBank are not timely satisfied.

Specific Risks Controls Relating to Business Continuity Planning

An FHLBank's controls relating to business continuity planning are set forth below:

1) Corporate Governance

The board of directors and senior management are responsible for identifying, assessing, prioritizing, managing and controlling risks. They should ensure necessary resources are devoted to creating, maintaining and testing the plan. This includes setting policy, prioritizing critical business functions, allocating sufficient resources and personnel, providing oversight, approving the BCP, reviewing test results and ensuring maintenance of the current plan. The effectiveness of the BCP depends on their ability to identify and understand the critical businesses processes of the FHLBank and establishing plans to meet the business process requirements in a safe and sound manner.

2) Insurance

The potential for liability to an FHLBank arising from defects in its business continuity operations and systems of control should be reflected in the FHLBank's annual risk assessment. Written procedures for operations at its designated hot-site should be developed. For example, back-up tapes should be stored off-site and be easily retrievable. Bilateral relationships with one or more FHLBanks may need to be used to effectuate the FHLBank's activities. Each FHLBank must have at least

one back-up system and must test it periodically to ascertain its reliability.

The business continuity plan should address the availability of insurance in the event of a disruption in the institution's business. The potential for losses and errors may increase due to a disabling event. For example, due to a disabling event, personnel may have to process wire transfer transactions in a manual environment, thereby increasing the possibility for losses due to errors and fraud.

The FHLBank may mitigate its risks and liability with the purchase of specific insurance and bond coverage such as director's and officer's liability, errors and omissions, data reconstruction, and fidelity bond coverage. Where an FHLBank mitigates its operational risk through the maintenance of insurance coverage, the adequacy of such coverage relative to actual loss experience should be periodically assessed.

In addition, the specific limitations, exclusions, notifications, and other clauses of each policy should be reviewed to determine their effects upon the availability of coverage under specific circumstances. Claims may be rejected if the FHLBank has weak controls or fails to follow its internal procedures.

Examination Guidance

A work program for Business Continuity Planning accompanies this narrative. What follows below are illustrative examples of attributes that should be considered by the examiner in completing the analyses required in that work program. In determining the extent of review and testing to be conducted in completing each analysis, the examiner should take into account his or her assessment of the quality and effectiveness of corporate governance, risk management, internal controls and audit coverage relating to the institution's business continuity planning.

The examiner for this area should evaluate the enterprise-wide methodology for BCP and ensure the appropriate level of coordination within the examination team.

1) Organizational structure

a) Functional organization and reporting structure;
b) Corporate level sponsorship;
c) Identification of key personnel;
d) Primary duties, responsibilities and technical expertise of personnel;
e) Segregation of duties;
f) Cross-training of personnel;
g) Coordination with other departments such as risk management, information technology, treasury and cash management, internal audit, accounting, credit and human resources; and
h) Significant changes in the foregoing since the last examination.

2) Establishment of risk tolerances and the development of key policies and oversight by the board of directors. Evaluate the adequacy of senior management oversight and the risk management function for business continuity, which may include the following:

a) Approved enterprise-wide methodology;
b) Identification of various recovery scenarios ranging in severity;
c) Established maximum downtimes or other triggers for implementing recovery strategies;
d) Designation of a remote recovery site(s). The site should not be so close to the FHLBank it would be affected by the same disaster, but not so far that personnel would not be able to reach site;
e) Alternate power supplies including uninterruptible power supplies (UPS) and back up generators;
f) Adoption of a detailed BCP addressing all critical functions of the FHLBank;
g) Designation of an employee to coordinate the periodic testing of the BCP with relevant departments;
h) Review and reporting of the testing results to senior/line management. If appropriate, corrective action should be taken to rectify identified deficiencies; and
i) Reporting test results and BCP readiness at least annually to the board of directors.

3) Key FHLBank policies and procedures, which may include those relating to the following:

a) Enterprise-wide BCP plan;
b) Business impact analysis and risk assessment;
c) Department or functional area BCP plans (may be reviewed by other examiners having a working knowledge of departmental procedures);
d) Information Technology (IT) Governance;
e) Risk management;
f) Information security;
g) Fraud prevention; and
h) Wire transfer operations.

4) Risk assessment under Part 917 and internal control evaluation under SARBOX

a) Evaluate the effectiveness of the annual risk assessment under Part 917 that identifies the key risks arising from and controls established by the FHLBank over business continuity planning and includes quantitative and qualitative evaluations; and

b) Evaluate the effectiveness of evaluations conducted pursuant to SARBOX that identify the key risks and controls pertaining to financial reporting and evaluate

potential fraud, and procedures implemented to periodically attest to the adequacy of the control environment.

5) Testing performed by external and internal auditors and outside consultants

a) Evaluate the adequacy of the scope and testing performed by external and internal auditors; and

b) Evaluate the adequacy of the scope and testing performed by outside consultants such as penetration testing.

6) Information technology and controls

a) Identify and assess the differences between the production environment and automated and manual systems at the designated recovery site(s) for processing transactions. Coordinate with other examiners to evaluate:

(1) Systems at the recovery site(s);
(2) Timeframes and priority for system recovery;
(3) Dependence upon manual processes;
(4) Limitations on automated interfaces;
(5) Processing capacity;
(6) Physical capacity;
(7) Telecommunications;
(8) Authorized users and other security changes;
(9) Vendor technical support and access to the automated wire system; and
(10) Utilization of spreadsheets, data bases and other user-developed applications.

b) Determine if management has adequately identified and communicated functional differences at the recovery site and developed plans to address identified gaps, which may include manual procedures.

7) Identification and evaluation of controls and significant changes

a) Evaluate workflow and processes to be followed during recovery scenarios as well as controls, including the level and direction of risk and the quality of risk management; and

b) Evaluate any significant changes that have been implemented since the last examination or are being considered that may affect the FHLBank's risk profile such as management, production and recovery site systems, key personnel, regulatory requirements and processing.

8) Testing

Conduct testing as appropriate taking testing conducted by other examiners into consideration. The scope of testing should be based on the preliminary review of governance, risk management, internal controls and audit coverage. Specific examples include, but are not limited to the following:

a) Review and evaluate the adequacy of the enterprise-wide BCP methodology including:

   (1) Enterprise-wide plan and business impact analysis; and
   (2) Risk assessment and efforts to address identified gaps.

b) Review the adequacy of the BCP. Examples of specific attributes include, but are not limited to, the following:

   (1) Identification of and establishment of security for the recovery-site(s) including the clear identification of functional differences between the production and the recovery site(s);
   (2) Mirroring or linking critical systems to the recovery-site, back-up of critical systems and data files, and implementation of procedures to retrieve back-up tapes and manual records that are stored off-site;
   (3) Designation of a BCP Administrator, a BCRT and a public spokesman; and
   (4) Identification of critical systems including computer hardware, software, and user-developed applications for the continuation of FHLBank's key functions which includes:

      (a) The establishment of priorities for the recovery of the key functions and processes, including critical timeframes for recovery, and the identification of equipment, utilities, and supplies to be utilized in effecting their recovery; and

      (b) The identification of key/critical functions and processes and the establishment of procedures to preserve or serve as back-up to such functions or processes in the event that these cannot be recovered within established critical timeframes.

c) Review and evaluate the adequacy of a sample of departmental business continuity plans. Consider the following:

   (1) Identification of and establishment of security for the recovery-site(s), including clear identification of functional differences between the production site and recovery site(s);
   (2) Correspondent bank services function, such as wires, safekeeping, deposit services, and affordable housing;
   (3) Credit function, such as advances, collateral, acquired member assets, and

affordable housing;
(4) Finance function, such as accounting, liquidity operations, and investments;
(5) Corporate administration/services function, such as marketing, facilities, security, insurance, human resources, legal, office administration, and purchasing records management;
(6) Emergency contact listing that clearly defines decision-making authority and identifies key/critical employees, and a contact listing for employees, customers and vendors;
(7) Cross-trained employees assigned to assume back-up functions/roles in the event the key/critical employees are not available;
(8) Bilateral agreements governing Fed funds and other dealer relationships; and
(9) Internal audit function.

d) Review the adequacy of BCP test strategies to determine if they are sufficient to validate recovery assumptions;

e) Review the supporting documentation of recent testing and evaluations of key/critical outside service providers maintained by the BCP Administrator. Consider the following:

(1) Coordination of testing with all key/critical functions;
(2) Establishment of objectives and data to be utilized;
(3) Utilization of test plans that include both automated and manual processes as well as different timeframes within the plans such as high volume processing days, and start-of-day, mid-day, and end-of-day processing;
(4) Testing performed on relationships with Fed funds counterparties and securities dealers for alternative sources of liquidity and bi-lateral relationships;
(5) Review of contingency testing performed by key/critical outside service providers, such as SAS 70 reports; and
(6) Recovery testing performed by information technology personnel.

f) Verify that the results of the tests are analyzed and reported to the BCP Administrator, senior/line management, and the board of directors and that deficiencies noted were promptly corrected. Determine whether the FHLBank has taken the following actions:

(1) Evaluation of the adequacy of the test scope, including the identification of clear objectives to be achieved by testing and functions, processes, transactions to be tested;
(2) Assessment of whether the test objectives were completed;
(3) Assessment of the validity and accuracy of the data processed; and
(4) Identification and correction of problems encountered.

9) Assessment of Risks

Summarize the results of the activity or function examined in a separate memorandum. The memorandum must articulate the risks and the management of those risks. It should also clearly and specifically describe the basis and analysis for the assessment. The memorandum should discuss the type(s) of risk (market, credit, operational); the level of the risk (low, moderate, high); the direction of the risk (stable, decreasing, increasing); and the quality of risk management (strong, adequate, weak). A memorandum must be prepared irrespective of whether the examiner's assessment is positive or negative.

10) Items requiring follow-up at the next on-site visitation

Identify key issues that have been communicated to management (written or oral) that require follow-up during the next on-site visitation.