Internal Audit Department
NeighborWorks® America

Audit Review of the Business Continuity Plan (BCP) Management and Documentation

Project Number: ADMN.BCP.2013

Audit Review of Management of BCP

Table of Contents

August 9, 2013

To: NeighborWorks America Audit Committee

Subject: Audit Review of the BCP Management and Documentation

Please find enclosed the final audit report of the Management of BCP review.

Please contact me with any questions you might have. Thank you.

Frederick Udochi
Director of Internal Audit

Attachment

cc: E. Fitzgerald
M. Forster
C. Wehrwein
J. Bryson
T. Frett

Function Responsibility and Internal Control Assessment

Audit Review of the BCP Management and Documentation

Business Function Responsibility	Report Date	Period Covered
Administrative Services	August 9. 2013	June 20, 2013 to July 2, 2013
Assessment of Internal Control Structure		
Effectiveness and efficiency of operations		**Generally Effective**[1]
Reliability of financial reporting		**Not Applicable**
Compliance with applicable laws and regulations		**Not Applicable**

This report was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing.*

[1]**Legend for Assessment of Internal Control Structure: 1. Generally Effective:** The level and quality of the process is satisfactory. Some areas still need improvement. **2. Inadequate:** Level and quality of the process is insufficient for the processes or functions examined, and require improvement in several areas. **3. Significant Weakness:** Level and quality of internal controls for the processes and functions reviewed are very low. Significant internal control improvements need to be made.

Executive Summary of Observations, Recommendations and Management Responses

Summarized Observation; Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response
Observation No. 1 **Policy Statement with Roles and Responsibilities** Based on the review performed, Internal Audit noted that NeighborWorks' BCP does not contain a policy statement denoting who has overall responsibility for the coordination, development, and maintenance of the BCP. **Risk Rating:** (b) (4)	Yes	**Recommendation No: 1** **Policy Statement with Roles and Responsibilities** Internal Audit recommends that NeighborWorks establish a BCP oversight team to have overall responsibility of BCP coordination, development, and maintenance. The BCP oversight team should consist of members from the Finance, Administrative Services, and Information Management divisions. The Oversight team should develop a corporate-wide BCP to include a general BCP policy and BCP retention policy statements as well as a corporate-wide functional organizational chart. The BCP policy statement should be approved by senior management and communicated to all management and staff. The BCP policy statement should state who is responsible for the development, maintenance, and testing of the corporate-wide BCP. The functional chart should include the names of the members of the BCP oversight team and their respective duties related to the BCP.	Yes	Management will update the BCP to include the listing of the Oversight team responsible for the BCP coordination, development, and maintenance, to include the recommended divisions (Finance, Admin Svcs and IM), along with the advice and consent of the Officers. The retention policy statement will be added to Chapter 5 of the BCP and the Oversight team's statement of normal operation resumption declaration will be added to Chapter 2 that outlines the overall mission.	March 31, 2014	Internal Audit accepts Management's Response.

Summarized Observation; Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response
Observation No. 2 **Plan Maintenance** Based on the review performed, the BCP does not adequately define a BCP maintenance strategy. **Risk Rating:** (b) (4)	Yes	**Recommendation No: 2** **Plan Maintenance** Internal Audit recommends that the Plan Maintenance section of the BCP be updated to state that the newly revised plans will be distributed or made available to all authorized employees and instruct employees to discard superseded plans upon receipt of a new plan. A status report on business continuity planning should be provided to oversight team every time a new plan is distributed. Additionally, version controls should be incorporated to track changes to the plan and all changes should be formally presented to and approved by the BCP oversight team.	Yes	As part of the final changes to the BCP, which has undergone significant overhauls to its content and format over the past 18 months supported by an external consultation, Administrative Services and Facilities will include a protocol for communicating to all staff when downstream changes are made effective in the plan, when to discard all previous versions of the BCP, and ensure that the process for the new plan distribution is clearly outlined. AS&F will also ensure the location of the most updated BCP (both electronically and manually) and that version controls are tracked, updated and handled appropriately, including requisite protocols for reviews and approvals including the BCP oversight team.	March 31, 2014	Internal Audit accepts Management's response.

Summarized Observation; Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response
Observation No. 3 **Risk Categories** Based on the review performed, NeighborWorks' BCP does not adequately define risk categories. The plan only addresses the critical risk category. **Risk Rating** (b) (4)	Yes	**Recommendation No. 3** **Risk Categories** In addition to critical business functions, Internal Audit recommends that the BCP be updated to define risk categories for essential/necessary and desirable business functions. For each risk category identified, Management should specify the functional area, the equipment supporting the systems /function in that area and the restoration period. Recovery of these systems must be based upon an assessment of the impact of its loss and the cost of recovery.	Yes (see clarification in management response)	Management will formally introduce a legend into the BCP defining the varying risk categories for corporate operations. Regarding the issue of "critical" and "essential" business processes, management caveats that these terms are often used interchangeably such as in the terms "mission essential" and "mission critical." Management references the latest federal guidance stating that "a subset of those [government] functions that are determined to be critical activities are defined as the organization's essential functions. These essential functions are used to identify supporting tasks and resources that must be included in the organization's continuity planning process." So critical activities are the essential functions that must be identified. During the BIA phase, management in each division reviewed business	March 31, 2014	Internal Audit acknowledges Management's response with the understanding that more than one risk category will be defined as part of the legend.

Summarized Observation; Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response
				functions and earmarked the ones that were critical. Management will include a statement in the BCP consistent with the federal guidance referenced above.		

Summarized Observation; Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response
Observation No. 4 **Business Disruptions due to Security Incidents** Based on the review performed, the BCP only outlined response procedures for natural disasters and severe weather but does not document instructions for business disruptions caused by serious Information Security incidents such as loss of records or data, IT system failures, and cybercrimes. **Risk Rating:** (b) (4)	Yes	**Recommendation No: 4** **Business Disruptions due to Security Incidents** Internal Audit recommends that the BCP be updated to include instructions for business disruptions caused by serious Information Security incidents such as cybercrimes, loss of records or data, disclosure of sensitive information, or IT system failure.	Yes (see clarification in management response)	Management will update the BCP to clarify that the base IT recovery procedures are applicable regardless of the nature of the incident that triggers the need to respond. Additionally, cross-references will be added to the BCP denoting applicable plans and procedures that appropriately live outside of the BCP. Additionally, Information Management is in the process of developing an updated IT Security plan where elements will naturally affect the BCP; the BCP will be updated as necessary upon its completion and a cross-reference will also be added for this plan.	March 31, 2014	Internal Audit accepts Management's response.

Summarized Observation; Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response
Observation No. 5 **Transition between Phases of the BCP** Based on the review performed, the BCP document does not identify at what point one phase of the BCP lifecycle will terminate and the next phase will commence. **Risk Rating:** (b) (4)	Yes	**Recommendation No: 5** **Transition between phases of the BCP** Internal Audit recommends that the BCP be updated to identify the transition between the following phases of the BCP lifecycle – Emergency, Backup, and Recovery. A dedicated team should be responsible for declaring that normal operations may resume upon consensus from the Disaster Recovery Manager and Departmental Recovery Teams.	Yes	As mentioned in Observation No. 1 above, management will update the BCP to include making the Oversight team responsible for the BCP coordination, development, and maintenance. The coordination section will address the lifecycle transitions, and the Oversight team will be responsible for declaring normal operation resumption consistent with the declaration that will be added to Chapter 2 that outlines their overall mission and responsibilities.	March 31, 2014	Internal Audit accepts Management's response.

Summarized Observation; Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response
Observation No. 6 **Insurance Team** Based on the review performed, the BCP does not indicate who would be responsible for processing and documenting insurance claims in the event of a disaster or business interruption. **Risk Rating:** (b) (4)	Yes	**Recommendation No: 6** **Insurance Team** Internal Audit recommends that the BCP be updated to expressly articulate the role and responsibility of the Finance Department and the Office of General Counsel in the event of a disaster or business interruption as the Insurance Team. This would mitigate any uncertainties as to who has responsibility for managing insurance claims in the event of a disaster or business interruption.	Yes (see clarification in management response)	Management will add clarifying language to the BCP to mitigate any confusion for the execution of insurance claims, denoting the collaborative teaming of OCFO/Finance and OGC under a BCP scenario. As a matter of routine, designated Finance staff are responsible **for** handling the insurance related activities and have responsibilities for 1) the annual renewal of the policies in a timely manner; 2) communicating as necessary with the Insurance Agency, 3) reporting and administering accident and other claims, and 4) handling all requests for insurance certification and verification.	March 31, 2014	Internal Audit accepts Management's response.

Risk Rating Legend:

Risk Rating: HIGH
A serious weakness which significantly impacts the Corporation from achieving its corporate objectives, financial results, statutory obligations or that may otherwise impair the Corporation's reputation.

Risk Rating: Moderate
A control weakness which could potentially undermine the effectiveness of the existing system of internal controls and/or operational efficiency, integrity of reporting and should therefore be addressed.

Risk Rating: Low
A weakness identified which does not seriously detract from the system of internal control and or operational effectiveness/efficiency, integrity of reporting but which should nonetheless be addressed by management.

Management Response to Audit Review of Database Administration and Controls		
# Of Responses	Response	Recommendation #
6	Agreement with the recommendations(s)	1, 2, 3, 4, 5, 6
0	Disagreement with the recommendation(s)	N/A

Background

The goal of a Business Continuity Plan (BCP) is to facilitate the process by which an organization is able to recover and restore key business processes after a disaster or business disruption has occurred. Large, medium, and small companies should prepare for incidents that could disrupt critical business processes for extended periods of time. Lack of preparedness can expose an organization to a degree of risk that can be detrimental to the business.

NeighborWorks® America's (NeighborWorks) BCP plan was developed to address how the Corporation would respond to a serious incident that caused a disruption to normal operations. The Administrative Services department is the custodian of the NeighborWorks' BCP and also responsible for its maintenance. A modular approach was adopted in the design of the BCP in which each individual Division/Department within a consistent framework documented how it would respond in the event of either a human or natural disaster.

Planning for the business continuity of NeighborWorks in the aftermath of a disaster is a complex task. Preparation for, response to, and recovery from a disaster affecting the administrative functions of the corporation requires the cooperative efforts of NeighborWorks' Divisional personnel and the functional area expertise of third party service providers supporting key BCP efforts. NeighborWorks' BCP records the plan that outlines and coordinates these efforts, reflecting the analyses by representatives from these functional areas and management.

At the time of this review NeighborWorks had recently relocated to a new office space located at 999 North Capitol N.E. Washington D.C. and was reassessing the current BCP in light of the relocation. NeighborWorks engaged All Hands Consulting, a global emergency management consulting company, to conduct Phase II by conducting a reassessment of the existing BCP. As a result, Internal Audit conducted this review with the understanding that NeighborWorks' BCP was undergoing a review and any recommendations made would only serve to enhance and add value to the current exercise of reassessment.

Objective

The audit objective was to obtain assurance that NeighborWorks' BCP documentation was compliant with IT Security Governance and industry best practices for organizations of similar size and function.

Scope

A desk document review was conducted on NeighborWorks' BCP and was limited to reviewing the structure of the BCPs to ensure that at a minimum, key components of the BCP were integrated into the structure. Key components include: Management Support, Risk Assessment/Mitigation, Business Impact Analysis, Business Recovery and Continuity, Awareness Training, Drills/Exercises, and Maintenance. Subsequent to confirming that the table of contents was consistent across all twelve divisional/departmental BCP documents,

Internal Audit selected two of the BCP document to review in detail. The two selected were the November 2012 Executive Summary BCP and the October 2012 Administrative Services and Facilities BCP (See Appendix A for list of the twelve divisional/departmental NeighborWorks BCPs). The scope for this review did not include testing the execution of the BCP or the validity of the content within the BCPs (For example, if all listed crisis team member were active employees, etc).

Methodology

The methodology used to perform this desk review included the use of relevant guidelines outlined in the Control Objectives for Information and related Technology framework (COBIT), System Administration Networking and Security Institute (SANS), International Organization for Standardization (ISO) 270001-2, ,and the National Institute of Standards and Technology (NIST). The Corporation's non-profit status and industry will dictate the degree to which the recommended best practices may be relevant or required. The methodology involved the following three Phases:

Phase 1 – (Information Gathering)

Questionnaires – Questionnaires regarding the BCP content were developed and distributed to appropriate staff.

Interviews – Interviews were conducted with the appropriate staff for an understanding of the BCP structure. The walkthroughs permitted Internal Audit to observe, assess, and gather information regarding the BCP structure.

Phase 2 – (Document Selection)

The BCP Executive Summary document was selected because it contains information pertinent to all department level BCP documents. The Administrative Service and Facilities BCP document was judgmentally selected to review because its table of contents and structure is consistent with all the remaining twelve divisional/departmental level BCPs.

Phase 2- Testing

Following the selection of the BCP plan to review, Internal Audit inspected each plan for compliance with NIST and COBIT standards. The availability[2] impact and risk ratings for each finding were established during this phase as well.

Phase 3 – Reporting

Once the risk rating was established, recommendations were developed and the Internal Audit team documented the results in this report and presented the report to the

[2] Availability- The goal of Availability is to ensure that data and services are available when needed and often addresses single points of failure.

Administrative Services & Facilities team during an Exit Conference. This report describes the observations for areas of improvement.

Observations and Recommendations

Observations # 1 – Policy Statement and Roles and Responsibilities

Based on the review performed, Internal Audit noted that the BCP under review did not contain a policy statement denoting a central group within the organization that had overall responsibility for the BCP coordination, development, and maintenance including cross-business unit of BCP activities. There was documentation of the coordination, development, and maintenance of the BCP within the individual divisional/departmental BCPs; however, a "chain of command" denoting who makes decisions and coordinates in a disaster or an emergency was not documented for the corporation as a whole. In addition the BCP made no reference to the Corporation's document retention policy.

The roles and responsibilities for overseeing the business continuity planning process should be established and 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.

Senior Management support is necessary for the successful execution of the BCP, especially in the early stages of the emergency.

Recommendation # 1 - Policy Statement and Roles and Responsibilities

Internal Audit recommends that management identify a BCP oversight team within the organization that would be responsible for the management, coordination, development, maintenance, and governance of the BCP. The BCP oversight team should consist of the following personnel at a minimum the Chief Financial Officer, Director of Information Management, and the Director of Administrative Services & Facilities. This should be documented in a BCP policy statement and supplemented with a functional organizational chart showing the chain of command in the event of a crisis. The functional organizational chart should include the names of all key managers and staff, as well as their assigned roles and responsibilities in reference to the BCP. The functional chart should include members of the BCP oversight team with responsibility of developing and maintaining the corporate-wide BCP process. It is also further recommended that the Corporation's Record Retention policy

be referenced in the BCP. The BCP Retention Policy statement will ensure the orderly and proper retention and destruction of all BCP records.

Observation # 2 – Plan Maintenance

Based on the review performed, the BCP does not adequately define a BCP maintenance strategy. Lessons learned from recovery effectiveness reviews and training exercises should be incorporated into the BCP in a timely manner. Ensuring that the BCP reflects current changes is crucial as plans could atrophy over time and become less effective if changes in the environment are not taken into account in a timely manner.

Recommendation # 2 – Plan Maintenance

Internal Audit recommends the proposed oversight team be responsible for establishing the plan maintenance policy/requirements. Internal Audit recommends that the Plan Maintenance section be updated to state that the newly revised plans will be distributed or made available to all authorized employees and instruct employees to discard all plans upon receipt of new plans. A status report on continuity planning should be provided to the oversight team every time a new plan is distributed. Additionally, version controls should be incorporated to track changes to the plan and all changes should be formally presented to and approved by the BCP oversight team.

Observations # 3 – Risk Categories

Based on the review performed, NeighborWorks' BCP only addresses the critical system risk category but does not define the other categories – Essential, Necessary, and Desirable systems risk categories. A comprehensive BCP should include critical as well as essential business processes and systems at a minimum. Critical systems should be assigned the highest priority on the restoration schedule followed by essential business processes and systems. However, necessary, and desirable functions may be suspended for the duration of an emergency and as a result not assigned a restoration schedule.

Recommendation # 3- Risk Categories

Internal Audit recommends that BCP be updated to include the definitions of essential/necessary and desirable risk categories. However, the essential risk category needs only to be assigned to the restoration schedule. For example, critical system should be assigned a Category I and essential systems should be assigned a Category II rating on the restoration schedule. The rating directly responds to the timeline which a disabled business process or system should be restored. A Business Impact Analysis should be performed to establish the additional risk categories mentioned above. Documenting the above mentioned risk categories will enhance the managerial and operational controls of NeighborWorks' BCP processes.

Observations # 4– Business Disruptions due to Security Incidents

Based on the review performed, the BCP only outlined response procedures for natural disasters and severe weather but does not document instructions for business disruptions caused by serious Information Security incidents such as loss of records or data, IT system failures, and cybercrimes.

Recommendation # 4 – Business Disruptions due to Security Incidents

Internal Audit recommends that the BCP be updated to include instructions for business disruptions caused by serious Information Security incidents such as loss of records or data, IT system failures, and/or cybercrimes. Each of the above mentioned scenarios needs to be developed and examined in detail and an analysis prepared of the potential consequences. Each scenario should also be assessed for possibility of occurrence (probability rating) and possible impact (impact rating). Adding the additional response procedures for the above mentioned security incidents will enhance the technical and managerial controls of the BCP process.

Observations # 5– Transition between Phases of the BCP

Based on the review performed, the BCP does not identify the critieria or timelines for the various stages of the BCP lifecycle in the event of a crisis in which a disaster or emergency starts and finishes. The criteria or timelines of the progression of a disaster should be documented within a BCP Lifecycle description. The BCP lifecycle description should include the Emergency, Backup and Recovery phases. The Emergency Phase begins with the initial response of the disaster. The Backup phase begins with the initiation of the appropriate departmental team BCPs for outages enduring longer than specified number of hours. The Recovery phase begins immediately after the disaster and takes place in parallel with the back-up operations at a designated hot site. BCP operations can be terminated when facilities, infrastructure and services are sustainable and reliable.

Recommendation # 5- Transition between Phases of the BCP

Internal Audit recommends that the BCP be updated to include a detail description of Neighborworks BCP lifecycle (Emergency, Backup, and Recovery phases). Additionally, a dedicated team should be assigned the responsibility of managing disasters throughout the entire BCP lifecycle. Documenting the BCP lifecycle descriptions will enhance the operational controls of NeighborWork's BCP processes. Identifying the various stages of the BCP life cycle would allow for more efficient handling of the crisis as it provides a sense for where the organization is in order to elicit the necessary sense of urgency.

Observations # 6– Insurance Team

Based on the review performed, the BCP does not indicate who would be responsible for processing and documenting insurance claims in the event of a disaster or business interruption. Documenting responsibility in the event of an insurance claim naturally would fall to the Finance Department and Office of General Counsel but stating this explicitly in the

BCP is a form of administrative control and defines roles and responsibilities in the event of a disaster in respect of insurance claims and processing. In the event of a disaster the Corporation and management should be able to have determined roles and responsibilities for insurance claims in order to alleviate any uncertainty.

Recommendation # 6- Insurance Team

Internal Audit recommends that the BCP be updated to expressly articulate the role and responsibility of the Finance Department and the Office of General Counsel in the event of a disaster or business interruption as the Insurance Team. The Insurance Team being knowledgeable of all facets of insurance coverage held by the Corporation will have the capacity in the event of a disaster to aid the Corporation in filing claims to insurance carriers. This would also mitigate any uncertainties as to who has responsibility for managing insurance claims in the event of a disaster or business interruption.

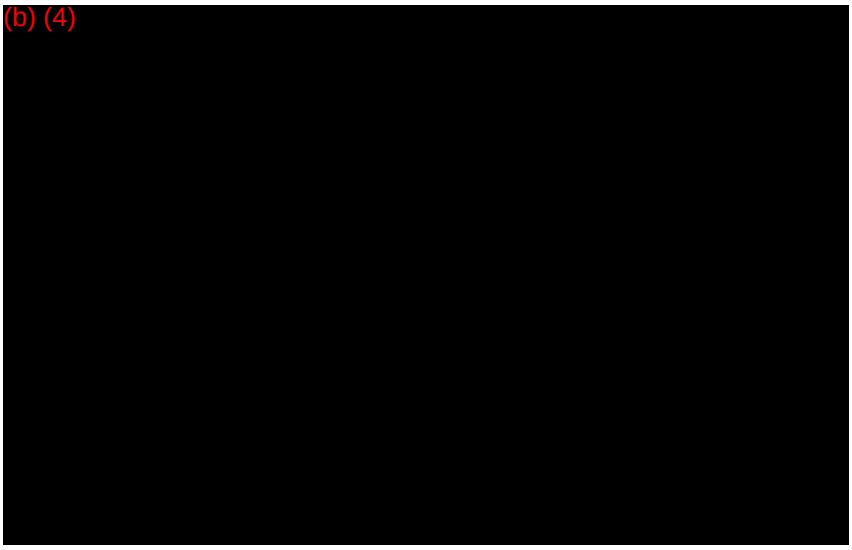
Conclusion

BCP is a critical risk management program with the objective of protecting organizations from potential disruptive activities. The BCP provides the framework for making appropriate risk mitigation decisions and recovery of business systems. The additional observations and recommendations made above should enhance the current BCP framework and supplement the All Hands Consulting assessment to ensure critical and essential business functions are available in the event of a business disruption.

Appendix A

List of BCP Documents Reviewed

(b) (4)



Appendix B

Consultant Professional Profile:

(b) (4) is an IT Security consultant with over 20 years experience in IT Security and Auditing. (b) (4) has held senior consulting positions with (b) (4) auditing firms. (b) (4) has had prior work experience with NeighborWorks America as he conducted the 2007 IT Security Review. Additionally, he has conducted reviews with similar firms such (b) (4) His key strength is his proven ability to work across multiple functional teams and with clients to assess, prioritize, and implement strategic business goals and IT audit objectives. He is effective is advising companies on IT security best practices and implementing IT Audit Frameworks such as COBIT. He is also a member of ISACA and holds CISSP, CSOX/P and CISO certifications.