Internal Audit Department
NeighborWorks® America

Audit Review of the IT Restoration Services Restoration/Recovery Exercise

Project Number: IM.ResRec.2011

Audit Review of the IT Restoration Services Restoration/Recovery Exercise
Internal Audit Department Project # IM.ResRec.2011

Table of Contents

Project Completion Letter

November 16, 2011

To: NeighborWorks America Audit Committee

Subject: **Audit Review of the IT Restoration Services Restoration/Recovery Exercise**
Internal Audit Department Project # IM.ResRec.2011

Please find enclosed the final audit review report of the Corporation's IT Restoration Services Restoration/Recovery Exercise at the (b) (4) site in (b) (4).

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

Frederick Udochi
Director of Internal Audit

Attachment

cc: (b) (4)

Function Responsibility and Internal Control Assessment

Audit Review of the Restoration Services Restoration/Recovery Exercise

Business Function Responsibility	Report Date	Period Covered
Information Management/Network Operations Center	November 16, 2011	September 29 2011– September 30 2011
Assessment of Internal Control Structure		
Effectiveness and Efficiency Operations		**Inadequate**[1] Recommendations in specific areas are noted below.
Reliability of Reporting		**Inadequate** Recommendations in specific areas are noted below.

[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

Summary of Observations and Recommendations[2]:

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	Internal Audit Comments on Management Response
Observation No. 1 **Business Continuity Plan (BCP)** The current Business Continuity Plan (BCP) is outdated (i.e., last updated in 2006; therefore, the recovery exercise performed and observed was not clearly tied to or driven by goals within the BCP. **Risk Rating:** (b) (4)	**Yes**	We recommend the BCP be updated and future rehearsals, exercises, and test be prioritized and aligned with the BCP.	**Yes**	The Business Continuity Plan will be updated in FY12. Administrative Services & Facilities is in the process of acquiring an outside consultant to assist with the coordination and establishment of a comprehensive and updated BCP. The consultant will ensure the updated BCP carefully integrates activities such as Leadership, emergency response, personnel preparedness, and strategies to facilitate systems continuity.	9/30/2012	Internal Audit accepts Management's response.

[2] The observations and recommendations in this section are summarized at a high level for informational purposes. To obtain a full, detailed explanation of each, please refer to the "Observations and Recommendations" section. Management's response is directly related to the detailed observations and recommendations noted in the "Observations and Recommendations" section.

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	Internal Audit Comments on Management Response
Observation No. 2 **Recovery Exercise** The test objective to recover a file server during the recover/restoration exercise was not achieved due to configuration and connectivity issues. There were also minor scripting, connection, and accessibility issues with a couple of workstations in the rehearsal room. **Risk Rating:** (b) (4)	**Yes**	We recommend Management review its connectivity and configuration specifications and expectations with its hot site vendor (b) (4) Management should also create technical documentation to recover critical components in the event of a disaster. Furthermore, we recommend the reports generated be distributed to the Officers and the BCP custodian at a minimum and the recipients should collectively evaluate the results against the updated BCP and make the necessary modifications to the BCP.	**Yes**	Setup and configuration is reviewed with the vendor before every exercise. Specifications, including network drawings, are forwarded to the vendor and reviewed in a pre-rehearsal conference call. In this instance, the vendor did make some mistakes in setup. At the same time we were introducing new equipment into the recovery process, which added complexity. One goal for any rehearsal is to uncover any potential problems with new equipment or network design, so the rehearsal was successful in that aspect. The IM division will continue the practice of forwarding design documents to the vendor and reviewing that design in the pre-rehearsal conference call. We will also continue to monitor and evaluate the vendor's performance and ability to meet our needs. There is an existing set of technical documents which support the recovery process for various parts of the IT infrastructure. The IM division will continue the current practice of periodic review, enhancement and expansion of documentation as needed. In addition, the IM division will share test results with the officers and appropriate BCP management commencing with the next rehearsal.	7/1/2012	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	Internal Audit Comments on Management Response
Observation No. 3 **Business Continuity and Recovery Document** We observed that the Business Continuity and Recovery Process document version 1.1 dated 8/9/11 **only** describes the process and procedures for standing up NeighborWorks' equipment at the hot site**.** This document had little or no documentation of mission critical processes, systems technology components, including the location and configuration of such components in order to facilitate availability and accessibility of relevant information to authorized third parties or in the event of turnover. **Risk Rating:** (b) (4)	**Yes**	The current document (Business Continuity and Recovery Document) is a small part of the comprehensive IT Business Continuity/Disaster Recovery to support the overall BCP. We recommend the document specify recovery methodologies, strategies, and detailed instructions that support the BCP policies for restoring operations. We also recommend Management update its inventory of hardware, software, applications, and network assets and document within the IT BC/DR document. Furthermore, we recommend this documentation be maintained under change control processes.	**Yes**	Management agrees additional, updated documentation, including an updated system recovery prioritization, is required for the corporation. However, since the recovery process is not a server-based rebuild of application, database and network servers, the level of documentation is greatly reduced. As noted during the audit, due to the significant use of virtualization, recovery is greatly simplified; documentation needs are reduced as is complexity in the recovery process. Operating systems and software are not re-installed - the server is recovered as a whole. This in turn reduces the amount of detailed instruction, additional materials and simplifies the process. IM does maintain inventory information of hardware and software assets. Of course, these assets change with regular frequency and since they are already maintained in an inventory document, that documentation can be referenced as a supplement to the IM BC/DR plan.	7/1/2012	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	Internal Audit Comments on Management Response
Observation No. 4 **Testing Policy** We noted that the test plans and test summaries for the May and September 2011 exercises did not: • Provide sufficient information in defining test elements against explicit test objectives and success criteria. • Contain a schedule detailing the time frames for each test or provide much detail about scope, objectives, scenarios, and logistics. • Establish a clear process for documenting outputs from the test and for identifying key learning outcomes and potential improvement actions In addition there was not a clearly defined process for reporting test results and test outcomes. **Risk Rating:** (b) (4)	**Yes**	We recommend Management develop a testing policy that gives higher priority to recovering mission-critical systems. The policy must set a schedule and expectations for testing enterprise-wide continuity functions, business units, and support functions. We also recommend IM conduct its test/exercise program under this policy.	**Yes**	The IM division currently rotates testing activity across a variety of critical systems or general functionality depending on the current need. (i.e., general testing due to the introduction of new equipment or backup processes vs. specific system tests). The IM division will review with management the current recovery prioritization matrix and ensure mission critical systems continue to be tested as regularly as possible. The IM division will document a more detailed testing process and goals for future tests and rehearsals. We appreciate that Internal Audit agrees with the current IM practice of periodically rotating non-network staff into the recovery test role to help ensure documentation will support alternative staff in case of an recovery event.	7/1/2012	Internal Audit accepts management's response and notes the adoption of the best practice of integrating periodic rotation of non-network staff as a form of cross training in the recovery test role.

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 Recommendations		
# Of Responses	**Response**	**Recommendation #**
4	Agreement with the recommendation(s)	1, 2, 3, 4
0	Disagreement with the recommendation(s)	N/A

Background

NeighborWorks® America (NeighborWorks) has a Business Continuity and Recovery Services (BCRS) Agreement with (b) (4). Under the contract, (b) (4) agrees to provide a hot site (located in (b) (4)), commission recovery hardware, load operating system, and configure disk volumes within hours of a NeighborWorks declared disaster. (b) (4) also provides:

- A (b) (4) with workstations and (b) (4) to an (b) (4) enterprise-level (b) (4) to perform recovery operations. The (b) (4) includes (b) (4) (b) (4)).
- Five days of supported eight hour block sessions of rehearsals per calendar year.
- Backup and replication of the NeighborWorks production folder at (b) (4).

NeighborWorks also has its own equipment at the recovery site including an (b) (4) The (b) (4) hosts (b) (4). The NeighborWorks Network Operations Center (NOC) is responsible for application and data loading during rehearsals, tests, exercises, and actual disaster recovery.

On September 29th and 30th, 2011, the NOC team performed a recovery exercise with the primary objective to recover a production file server at the (b) (4) site and Internal Audit (accompanied by a consultant from (b) (4), See Consultant Profile at Appendix A) observed the process and procedures employed. (See additional information/details at the Recovery Exercise section below)

Objective

The objective of this review was to:

- Assess the adequacy of the established restoration and recovery protocols pertaining to the HP site;
- Observe the September 29-30, 2011 recovery exercise with the view of evaluating the conduct and outcome of the process; and

- Evaluate NeighborWorks post mortem analysis and activities.

Scope

The scope for this engagement included:

1. Reviewing the existing policies and procedures to be performed during a recovery exercise and how those policies and procedures are aligned with the Business Continuity and Disaster Recovery Plan and industry best practices.
2. Obtaining assurance the planned exercise supports specific and identified components of NeighborWorks' BC/DR Plan.
3. Observing the September 29th/30th recovery exercise to evaluate whether or not the executed procedures are aligned with the existing policies/procedures and industry best practices.
4. Observing the September 29th/30th exercise to determine whether the test results demonstrate the readiness of employees to achieve NeighborWorks' recovery and resumption objectives.
5. Evaluating test results from the exercise to ensure that test objectives were achieved and that business continuity successes, failures, and lessons learned are thoroughly analyzed.

This engagement did not include a site survey/evaluation or an analysis of the BC/DR arrangements/contracts with third party vendors. A detail of the audit approach/methodology adopted is summarized at Appendix A.

Recovery Exercise - Recover File Server (b) (4)

The September 2011 exercise was an announced functional test, which means that the team knew the testing would occur and the specific objectives of the test. An announced test is helpful for the initial test of procedures. It gives teams the time to prepare for the test and allows them to practice their skills. Functional exercises are used to validate specific functions within the organization. Typically, these exercises address a particular function of the BCP (e.g., emergency notification, mobilization, or data recovery). The recovery exercise conducted in September 2011included the following BC/DR practices:

- System recovery on an alternate platform from backup media

- Coordination among recovery teams
- Internal and external connectivity
- System performance using alternate equipment
- Restoration of normal operations
- System recovery at the alternate processing site

The table below summarizes the test and the test outcomes.

Title of Test	Recover File Server
Business Unit Involved in test	NOC
Location of Test	(b) (4)
Date and time of Test/Training	9/29/2011: 8 a.m. – 5 p.m. 9/30/2011: 8 a.m. – 12 p.m.
Expected duration of Test	No timeline was provided for the exercise planning and execution.
Objectives of Test: 1. Recover file server (b) (4) 2. Update (b) (4) Software 3. Perform maintenance	
Type of Test *(Desktop review, Desktop scenario or walkthrough test, Functional test Full scale/live test)* A Functional test to validate team's ability to restore a file server from backup media from the hot site.	
Test Participants:	

Participant	Title	Role
(b) (4)	(b) (4)	Participant
(b) (4)	(b) (4)	Participant
(b) (4)	(b) (4)	Participant
(b) (4)	(b) (4)	Participant
(b) (4)	(b) (4)	Observer - Audit
(b) (4)	(b) (4) – IT Consultant	Observer – Data Collection, Audit
(b) (4)	(b) (4) Account Services Manager	(b) (4)
(b) (4)	(b) (4) Recovery Support Technician	(b) (4)

Resources for Test:

As described in the configuration setup diagram, the test plan, and in the system configurations specified in the (b) (4) contract.

Test Action Steps:

1. Isolate test environment from live NeighborWorks' WAN by (b) (4)
2. Finalize network adjustments and configurations settings for test environment
3. Enable (b) (4)
4. Establish network and virtual environment
5. Install backup/replication software on recovery workstations
6. Import backups
7. Restore file server to restore point
8. Login to file server to verify connectivity and functionality
9. Erase data from disks upon completion of rehearsal
10. Reconnect to live environment

Test Results

The primary objective of the exercise was not achieved.

- File server not successfully restored during period of observation. File server was still being restored when we left site on day two of exercise.
- Backup software (b) (4) successfully updated
- Maintenance on NeighborWorks' equipment at recovery site not performed.

Problems encountered

- (b) (4)
- (b) (4)
- (b) (4)

(b) (4)

Observations and Recommendations

Observation No. 1: Business Continuity Plan

The current NeighborWorks Business Continuity Plan (BCP) has not been updated since 2006; therefore, the processes and controls within are outdated. As a result of the outdated BCP, the test plan for the restoration/recovery exercise and the process and procedures employed (including the requirements/agreements for a hot site) were not driven by, nor tied to, business goals or the BCP itself.

Recommendation No. 1

We recommend that NeighborWorks Management update its Business Continuity Plan. An updated BCP will institute an organizational policy and establish management plans and controls for BC/DR across all business units. An updated and current BC/DR plan will specify organizational priorities in the event of a disaster. Once organizational priorities are defined, Management may assign responsibility throughout the organization to develop and implement processes and procedures to address the priorities and test the viability of the planned processes and procedures. In addition, in the case of an IT recovery exercise; planned IT exercises (test) would be aligned with the priorities of the organization.

Observation No. 2: Recovery Exercise Results

The primary objective of the exercise was to recover File server (b) (4), which provides shared storage of NeighborWorks' workstation images[3]. This exercise was designed to ensure single or multiple workstations could be quickly recovered to standard configuration in the event of a disaster or corruption. Based on the observation of the recovery exercise performed, the recovery exercise was unsuccessful because the test objectives were not met. The Network Operations Center (NOC) Team conducting the exercise experienced technical difficulties during the first day (9/29) including connectivity and configuration issues, which made the network and virtual environment for the exercise unusually difficult. There were also minor scripting, connection, and accessibility issues with a couple of the workstations in the rehearsal room.

We also noted that a previous exercise conducted on May 5-6, 2011 to (b) (4) was also not successful. Based on the results of these exercises, the Corporation cannot be said to be in a state of readiness for the timely recovery of its systems in the event of a disaster.

[3] Workstation images contain the operating system, applications and data of workstations.

Furthermore, the reports resulting from the rehearsals/exercises conducted in May and September 2011 were provided to a limited audience, which did not include key members of Senior Management and the BCP custodian.

Recommendation No. 2

Although a hot site survey/evaluation or an analysis of the BC/DR arrangements/contracts with third party vendors is outside the scope of this engagement, we strongly recommend, that Management clarify configuration and connectivity responsibilities and expectations with (b) (4) to ensure rehearsals, and more importantly actual recoveries, are successful in the future.

We recommend Management create technical documentation to recover critical components in the event of a disaster (See Observation No. 3). We also recommend that Management establish a testing policy to ensure that its highest priority systems receive first consideration during recovery/restoration exercises and rehearsals at the hot site (See Observation No. 4). An updated BCP/DR plan would furthermore facilitate this recommendation.

We also recommend the reports generated outlining the results of the rehearsals/exercises performed be provide to the Officers, the BCP custodian, and the Business Process owner if specific to a particular business application. By ensuring these key individuals are made aware of the results of recovery/rehearsal/test activity results NeighborWorks Management may be able to collectively make the appropriate modification to the overall BCP and related recovery/restoration expectations.

Observation No. 3 Business Continuity and Recovery Process Document

We obtained and reviewed the Business Continuity and Recovery Process (b) (4) dated (b) (4), which supports the recovery processes and procedures to be performed during the recovery rehearsals/exercises and actual recovery. This document contained good overall guidance for setting up and connecting to NeighborWorks' systems from the recovery site. The NOC team was familiar with the process and systems and was well positioned to execute the plan. The team constantly communicated among themselves and addressed a few areas of the document that required updates, wording clarity and general reorganization. However, the document did not represent a complete Business Continuity/Disaster Recovery Plan for the IT function; it ***only*** described the process and procedures for standing up NeighborWorks' equipment at the recovery site.

Clearly and concisely documented processes ensure that the expertise of how to use systems, and the knowledge of where critical documents are electronically stored should be maintained in order to facilitate availability and accessibility of relevant information to authorized third parties or in the event of turnover. Such inventory should include backup procedures, configuration guidelines, alternate site status and inventory, and standard operating procedures as implemented in production, owned

whether onsite or offsite, and deployed by NeighborWorks. This document had little or no documentation of mission critical processes, systems, technology components and the location and configuration of such components.

Recommendation No. 3

We recommend Management develop a more comprehensive BC/DR plan for its IT assets. Such a plan should include the following:

- An updated version of the current Business Continuity and Recovery Process document that is aligned with the overall BCP;
- Specific Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) for mission critical processes and systems[4];
- Metrics and score cards for BC/DR processes; and
- A business impact analyses of NeighborWorks processes and systems.

The Information Management (IM) BC/DR plan must support an updated BCP. It should:

- Determine the platforms, servers, applications, and operating systems that support critical business functions;
- Prioritize processes and systems from a data protection perspective; and
- Document the recovery timeline, methodology, strategy, and instructions for restoring operations in the event of a declared disaster.

We also recommend that Management create technical documentation to recover critical components in the event of a disaster. Management should work closely with technical support teams within the organization to create this documentation as part of the update and maintenance of a BCP. The documentation should be maintained under change control and used/updated during continuity/disaster drills and testing exercises where appropriate.

Observation No. 4 Testing Policy

A testing policy, typically articulated in a BCP, sets expectations and a schedule for enterprise-wide continuity functions such as IT recovery/restoration activity, business units, and support functions. The policy establishes testing/exercising goals to mitigate threats and risks specified in the BCP. Testing strategies should be selected after the recovery objectives and BC/DR priorities, metrics, and other criteria have been determined. Furthermore, a testing policy ensures tests/exercises give a higher priority to recovering mission-critical processes and systems.

[4] Two key metrics to be measured in a disaster recovery environment are the RTO and RPO. RTO is a metric that measures the time that it takes for a system to be completely up and running in the event of a disaster. RPO measures the ability to recover files by specifying a point in time restore of the backup copy.

We noted that the test plans and test summaries for the May and September 2011 exercises did not provide sufficient information in defining test elements against explicit test objectives and success criteria. The documentation did not contain a schedule detailing the time frames for each test or provide much detail about scope, objectives, scenarios, and logistics. There was not a clear process for documenting outputs from the test and for identifying key learning outcomes and potential improvement actions. In addition there was not a clearly defined process for reporting test results and test outcomes to several audiences, including senior management, business line management, risk management, IT management and other stakeholders.

Recommendation No. 4

We recommend that Management identify its business-critical information based on an appropriate risk assessment management process. In a disaster, the first priority is to get the business-critical information, and the associated information systems up and running. Recovery of the information systems and business-critical information is unique to each organization.

In addition we recommend that Management update its BCP to include the articulation of a testing policy. Tests and exercises must clearly demonstrate that the recovery strategies selected meet the recovery requirements of the organization. Contracting for a hot site as well as mobilizing the resources to conduct rehearsals and exercises is expensive which drives the need to ensure that the Corporation's business objectives are effectively and efficiently achieved.

While we acknowledge that tests and exercises must be scaled to the purpose and objective of the test, we recommend that Management use test plans and test scripts that provide sequential procedures related to testing specific business or technology functions so that they can be readily used by secondary staff members, should primary staff members be unavailable, to test business processes within pre-established timeframes. Test plans and 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.

Conclusion

Business continuity encompasses ensuring continuity of operations, contingency planning, disaster planning, disaster recovery, and emergency operations centers; although this review covered the recovery/restoration test exercise it involves more than recovering an organization's IT environment in the event of a disaster. This becomes more significant in the absence of an updated BCP and we hope that Management would strongly take into consideration our recommendations as it embarks on updating the current BCP.

Appendix A

Consultant Professional Profile: (b) (4)

(b) (4) is President and Chief Executive Officer (CEO) of (b) (4) an information, telecommunications, technology solutions, and professional services consulting firm. The consulting firm helps teams and organizations in both the private and public sectors to identify, target, and implement goals (including training and tools adoption) for process, technology, and software improvements.

(b) (4) has over 15 years of experience in the information technology field. 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 objectives. He is effective in building relationships with internal and external customers, partners, and vendors and has a track record in full lifecycle development and integration architectures and methodologies.

He is a member of the *Institute of Electrical and Electronics Engineers* (IEEE) Computer Society. He is also (b) (4) and, formerly, at (b) (4), teaching both online and classroom-based courses in relational and advanced database concepts as well as software engineering and introductory programming.