

Internal Audit
NeighborWorks® America

**Audit Review of the
Disaster Recovery & Business
Continuity Plan (DR & BC Plan)**

Project Number: NW.CORP.DR-BC.2017

Audit Review of the DR & BC Plan

Table of Contents

Function Responsibility and Internal Control Assessment	3
Risk Rating Legend.....	13
Background	14
Objective	14
Scope.....	14
Methodology	15
Observations and Recommendations	16
Conclusion	18

To: NeighborWorks America Audit Committee

Subject: **Audit Review of the Disaster Recovery & Business Continuity Plan**

Enclosed is the final audit report of the Disaster Recovery & Business Continuity Plan.

Please contact me with any questions you might have.

Thank you.

Frederick Udochi
Chief Audit Executive

Attachment

cc: J. Bryson
R. Bond
T. Chabolla
R. Simmons
T. Frett
W. Bowman

Function Responsibility and Internal Control Assessment
Audit Review of the DR & BC PLAN

Business Function Responsibility	Report Date	Period Covered
Administrative Services And IT&S	August 29, 2017	April 5, 2017 Through August 29 2017
Assessment of Internal Control Structure		
Effectiveness and efficiency of operations		(b) (5)
Reliability of financial reporting		Not Applicable
Compliance with applicable laws and regulations		Not Applicable

This report was reissued February 15, 2024 in accordance with a recommendation by the Government Accountability Office (GAO-23-105944, June 14, 2023).

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 Observation, 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 Gaps Identified in the Current DR & BC Plan During the introductory meeting held April 5th 2017, it was brought to our attention that there were completion gaps identified in the current BCP and DRP project update being performed by an external consultant Bazilio Cobb Associates. In an informal presentation the final project presentation slide was shared, which identified gaps and remediation efforts, some of a critical nature which were yet to be completed. Internal Audit observed that there were no established timelines, action items, and deliverables with owners planned and/or scheduled	Yes	Recommendation No. 1 Implement Plan with Established Criteria and Assignment of Ownership Internal Audit recommends that management implement a plan with established timelines, action items, deliverables and assigned ownership for accountability to implement the recommendations of the external consultant Bazilio Cobb Associates most especially for the items considered critical for the Corporation.	Yes	The external consultants identified the following critical recommendations. Final communication of BCP program to all staff from top down. BCP will be reviewed, policy added, and updates made and finalized. It will be communicated and made available to all staff. BCM Policy created to be included in BCM Manual. BCM Policy is being written and will be reviewed by Officers, SLT, and then added to the BCM Manual. Ensure plan testing dates and timelines are outlined.	February 28, 2018. January 31, 2018. January 31, 2018.	Internal Audit Accepts Management's Response

Executive Summary of Observation, 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
as a follow up to remediation. Note: As an update to this report a formal presentation was made to the Officers of the Corporation August 28, 2017 in which the identified gaps had been completed. Risk Rating: (b) (5)						

Executive Summary of Observation, 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. 2 Lack of a Regular Testing Schedule of DR & BC Plans Internal Audit also observed that there has not been any regular periodic update or testing exercise of the DR & BC plans since the fiscal year 2013. Testing of critical business continuity and disaster recovery processes are essential to the success of any DR & BC Plans. Risk Rating: (b) (5)	Yes	Recommendation No. 2 Requirement of Exercise or Testing Regime We recommend that management require some exercise or testing regime to be an integral part of the DR & BC Plan. Exercises or tests are generally considered the most effective way of keeping a DR & BC program current and executable. Tests must be held at periodic intervals and should address a variety of scenarios and/or critical elements of the plan. In addition there must be a method to track issues and gaps uncovered in the test with the ability to track remediation efforts.	Yes	BCM process testing framework is already included in section 4 of the drafted BCM Program manual. The manual will be further updated to include specific test types and a timeline as to when the tests should occur annually as well as the necessary follow up once testing concludes. IIT&S has committed to supporting and assisting with the necessary testing. <i>See attached BCM Program Manual</i>	January 31, 2018.	Internal Audit Accepts Management's Response

Executive Summary of Observation, 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. 3 Informational Gaps Identified in the DR & BC Plans Internal Audit also conducted a gap-analysis on the draft DR & BC Plan as much of the planned recovery is based on the assumption of the restoration of Information Technology and Services (IT&S). In the absence of untimely IT&S recovery: • The absence of relevant information on an alternative workaround plan to support mission critical processes and deadlines such as payment. • The plans did not contain a list of	Yes	Recommendation No. 3 Review and Make Provisions for Identified Gaps Internal audit recommends that management review the above informational gaps and plan to make provision for items considered to be critical to the full recovery process.	Yes	We are aware of the gaps between divisional recovery expectations and IT&S recovery abilities. We will be addressing ways to remedy those gaps or creating a workaround plan and documenting it in the divisional plans. The	April 30, 2018.	Internal Audit Accepts Management's Response

Executive Summary of Observation, 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
applications that will be accessible with and without VPN/NWA network to perform mission critical items not defined in plans. However, the plans did contain a list of critical applications and categorized business processes by their criticality.			Yes	divisions will work with IT&S to complete this. Management will update the plans based on a list provided by IT&S that identify which applications need VPN/NWA network access. <i>see the attached NWA BCP Application Matrix</i>	January 31, 2018.	
• Information gap on how procurement policies would apply for the replacement of personnel, IT, equipment and/or facilities in times of business continuity operations and whether business			Yes	Procurement policy for a BCP Incident is being created by SVP Procurement and will be included in the BCP Manual or Policy. HR will be consulted to include a recruitment plan	January 31, 2018.	

Executive Summary of Observation, 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
continuity efforts and timelines would be impacted. Risk Rating: (b) (5)				for critical personnel replacement and that information will be included in the BCP Manual. The current BCM Manual includes a section on how loss of facility will be addressed in case of a BCP or disaster recovery need.		

Executive Summary of Observation, 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. 4 Incorrect Property Listing on Insurance Coverage We reviewed the insurance coverage for completeness of corporate assets identified and subject to coverage. We however noted that the insurance policy listed a New Jersey address under commercial and property insurance and further determined that NW does not officially maintain an office there any longer. Risk Rating: (b) (5)	Yes	Recommendation No. 4 Update Property Listing on Insurance Coverage We recommend that management remove this property listing from the commercial and property section of the insurance policy and ensure that subsequent revisions or updates to the insurance policy occur in real time and in a timely manner.	Yes	Management has noted to remove this location from the property schedule during the upcoming renewal. Finance is responsible for the annual insurance renewals and will consult with Facilities to ensure the property listings are correct and updated.	April 1, 2018.	Internal Audit Accepts Management's Response

Executive Summary of Observation, 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. 5 Failure to Consistently Adhere to Change Management Processes It was noted in our questionnaire that not all application changes are currently adhering to the established change management process due to the fact that the current change management process has not been widely communicated. Change management provides a framework and form of guidance for the process of change for staff and ensures consistency whenever there is a change process such as in a disaster recovery exercise. Risk Rating: (b) (5)	Yes	Recommendation No. 5 Integrate Change Management Processes into DR & BC Plans It is recommended that management integrate the change management process of the Corporation into the DR & BC Plans. Elements of the current Change Authorization Board (CAB) would help facilitate this process.	Yes	The draft BCP Manual addresses changes to the BCP and includes forms and checklists to track those changes. We will also work with the SVP IT&S to look at the CAB process and if there are additional elements we can add to BCP to strengthen the change management, we will add those elements. <i>See attached BCM Program Manual</i>	January 31, 2018.	Internal Audit Accepts Management's Response

Executive Summary of Observation, 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. 6 Inconclusive Listing of Microsites for Data Backup Internal Audit has not been able to determine whether all NW microsites (corporate related micro websites) are included in the BCP Application Matrix. Management has indicated that there are plans to migrate these sites to neighborworks.org and shutdown the sites either in fiscal year 2017 or 2018. For example at the time of this review Success Measures was not found on the list. Risk Rating: (b) (5)	Yes	Recommendation No. 6– Update Microsite Listing and Include Migration/Shut Down Dates Internal audit recommends that management update the list of microsites and provide any planned dates for migrations or shut downs in order to proactively update the DR & BC plans accordingly on a timely basis.	Yes	Management provided a list of microsite and future plans for those sites in an email sent on 7/14/2017. <i>Attached please find the email with the list of Microsites and their future plans</i>	October 31, 2017.	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 Disaster Recovery & Business Continuity Plan		
# Of Responses	Response	Recommendation #
6	Agreement with the recommendations(s)	6
	Disagreement with the recommendation(s)	

Background

The goal of a Disaster Recovery & Business Continuity Plan (DR & BC Plan) is to facilitate the process by which an organization is able to recover and restore critical business processes after a disaster or business disruption has been declared. Large, medium, and small companies should prepare for incidents that could disrupt key 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) DR & BC 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' DR & BC PLAN and is administratively responsible for its update and maintenance. A modular approach was adopted in the design of the DR & BC PLAN 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.

In FY 2013 the Corporation had engaged the services of All Hands Consulting a global emergency management consulting company, to conduct a reassessment of the existing DR & BC PLAN and the FY 2013 audit review was undertaken while this consulting engagement was being conducted. In a similar vein this fiscal year 2017, a review was undertaken at the same time as a re-assessment was being conducted by an external consultant, Bazilio Cobb Associates who was engaged by the Corporation.

Objective

To obtain assurance that sufficient measures and responses to disruptions requiring disaster recovery and business continuity efforts have been identified in a documented plan, and that identified risks have been sufficiently mitigated and recognized gaps remediated.

Scope

A desk review was performed for the purposes of this review and the scope included the following:

- Determine whether risk assessment, risk monitoring and business impact analysis have been sufficiently evaluated to include the prioritization of business objectives in recovery, resumption, and maintenance of all aspects of the business in addition to the IT components.
- Determine if recovery, resumption, and maintenance activities of all aspects of the business, including recovery of the technology components have been incorporated in planning efforts, tested when possible, and documented with scheduled periodic review of the Enterprise-wide Business Continuity Plans.
- Identify if disaster recovery and business continuity efforts were sufficiently assessed for interdependencies.

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 DR & BC PLAN content were developed and distributed to appropriate staff.

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

Phase 2 – Document Selection

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

Phase 3 – Testing

Following the selection of the DR & BC PLAN to review, Internal Audit inspected each plan for compliance with NIST and COBIT standards².

Phase 4 – 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 Administrative Services & Facilities; Information Technology & Services during an Exit Conference. This report describes the observations for areas of improvement.

² NIST – National Institute of Standards and Technology; COBIT – Control Objectives for Information and Related Technologies.

Observations and Recommendations

Observation # 1 – Gaps Identified in the Current DR & BC Plan

During the introductory meeting, held April 5th 2017, it was brought to our attention that there were completion gaps identified in the current BCP and DRP project update being performed by an external consultant Bazilio Cobb Associates. In an informal presentation the final project presentation slide was shared, which identified gaps and remediation efforts, some of a critical nature which were yet to be completed. Internal Audit observed that there were no established timelines, action items, and deliverables with owners planned and/or scheduled as a follow up to remediation. The reason we could discern from this was due to the staff transitions at the end of the project in which the lead staff had obtained final presentation from consultants without relevant stakeholders such as the Officers of the Corporation. In addition the DR & BC Plans had not been formally signed off as corporate policy documents.

Note: As an update to this report a formal presentation was made to the Officers of the Corporation August 28, 2017 in which the identified gaps had been completed.

Recommendation # 1 – Implement Plan with Established Criteria and Assignment of Ownership

Internal Audit recommends that management implement a plan with established timelines, action items, deliverables and assigned ownership for accountability to implement the recommendations of the external consultant Bazilio Cobb Associates most especially for the items considered critical for the Corporation.

Observation # 2 – Lack of a Regular Testing Schedule of DR & BC Plans

Internal Audit also observed that there has not been any regular periodic update or testing exercise of the DR & BC plans since the fiscal year 2013. Testing of critical business continuity and disaster recovery processes are essential to the success of any DR & BC Plans. This non-activity has been due to the multiple assignment and re-assignment of functional accountability for this process by transitioning senior management and the probable absence of a DR & BC policy document. The lack of test exercises can result in neglect of the plan which over time will atrophy due to changes in the business environment technology and operating environment which will fail to be reflected in the plans.

Recommendation # 2 – Requirement of an Exercise or Testing Regime

We recommend that management require some exercise or testing regime to be an integral part of the DR & BC Plan. Exercises or tests are generally considered the most effective way of keeping a DR & BC program current and executable. Tests must be held at periodic intervals and should address a variety of scenarios and/or critical elements of the plan. In addition there must be a method to track issues and gaps uncovered in the test with the ability to track remediation efforts.

Observation # 3 – Informational Gaps Identified in the DR & BC Plans

Internal Audit also conducted a gap-analysis on the draft DR & BC Plan as much of the planned recovery is based on the assumption of the restoration of Information Technology and Services (IT&S). In the absence of an IT&S restoration the following critical informational gaps were observed:

- The absence of relevant information on an alternative workaround plan to support mission critical processes and deadlines such as payment disbursements in the event of a disaster.
- The plans did not contain a list of applications that will be accessible with and without VPN/NWA network to perform mission critical items not defined in plans although the plans did contain a list of critical applications and categorized business processes by their criticality.
- Information gap on how procurement policies would apply for the replacement of personnel, IT, equipment and/or facilities in times of business continuity operations and whether business continuity efforts and timelines would be impacted.

Recommendation # 3 – Review and Make Provisions for Identified Gaps

Internal audit recommends that management review the above informational gaps and plan to make provision for items considered to be critical to the full recovery process.

Observation # 4 – Incorrect Property Listing on Insurance Coverage

We reviewed the insurance coverage for completeness of corporate assets identified and subject to coverage. We however noted that the insurance policy listed a New Jersey address under commercial and property insurance and further determined that NW does not officially maintain an office there any longer. This appeared to be an oversight due to not reviewing the policy comprehensively on a regularly scheduled frequency.

Recommendation # 4 – Update Property Listing on Insurance Coverage

We recommend that management remove this property listing from the commercial and property section of the insurance policy and ensure that subsequent revisions or updates to the insurance policy occur in real time and in a timely manner.

Observation # 5 – Failure to Consistently Adhere to Change Management Processes

It was noted in our questionnaire that not all application changes are currently adhering to the established change management process due to the fact that the current change management process has not been widely communicated. Change management provides a framework and form of guidance for the process of change for staff and ensures consistency whenever there is a change process such as in a disaster recovery exercise.

Recommendation # 5 – Integrate Change Management Processes into DR & BC Plans

It is recommended that management integrate the change management process of the Corporation into the DR & BC Plans. Elements of the current Change Authorization Board (CAB) would help facilitate this process.

Observation # 6 – Inconclusive Listing of Microsites for Data Backup

Internal Audit has not been able to determine whether all NW microsites (corporate related micro websites) are included in the BCP Application Matrix. Management has indicated that there are plans to migrate these sites to neighborworks.org and shutdown the sites either in fiscal year 2017 or 2018. For example at the time of this review Success Measures was not found on the list.

Recommendation # 6 – Update Microsite Listing and Include Migration/Shut Down Dates

Internal audit recommends that management update the list of microsites and provide any planned dates for migrations or shut downs in order to proactively update the DR & BC plans accordingly on a timely basis.

Conclusion

DR & BC PLAN is a critical risk management program with the objective of protecting organizations from potential disruptive activities. The DR & BC PLAN provides the framework for making appropriate risk mitigation decisions and recovery of business systems. Management, as a start, should seriously consider the recommendations provided by the Business Continuity Plan (BCP) consultant as part of the efforts to updating the plan and making it fully executable. The establishment of DR & BC policy document would also help greatly in communicating management expectations, training and awareness for employees. The DR & BC plan should be a dynamic document that is constantly subjected to a scheduled frequency of tests and exercises.