Internal Audit Department
NeighborWorks® America

Audit Review of

Disaster Recovery and Business Continuity (Cloud Based)

Project Number: NW.ITS.DISASTERREC.2020

Audit Review of Disaster Recovery and Business Continuity (Cloud Based)

Table of Contents

Function Responsibility and Internal Control Assessment 3

Executive Summary of Observations, Recommendations and Management Responses 4

Risk Rating Legend 13

Background 14

Objective 14

Scope 14

Methodology 14

Observations and Recommendations 15

Conclusion 19

Appendix A: Business Continuity Team Structure - Management & Oversight .... A

Appendix B: Disaster Recovery Testing Schedule .... B

January 13, 2021

To: NeighborWorks America Audit Committee

Subject: **Audit Review of Disaster Recovery and Business Continuity (Cloud Based)**

Attached is our draft audit report for the **Disaster Recovery and Business Continuity (Cloud Based)** review. Please contact me with any questions you might have.

Thank you.

Frederick Udochi
Chief Audit Executive

Attachment

cc: M. Rodriguez
S. Ifill
R. Bond
R. Simmons
W. Bowman

Function Responsibility and Internal Control Assessment
Audit Review of Disaster Recovery and Business Continuity (Cloud Based)

Business Function Responsibility	Report Date	Period Covered
Information Technology & Services	January 13, 2021	October 1, 2018 to September 30, 2020
Assessment of Internal Control Structure		
Effectiveness and Efficiency of Operations		**Inadequate**[1]
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 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 1 – Incomplete/Outdated Business Continuity Plans, Process and Procedures. Internal Audit (IA) found the current *NeighborWorks America Business Continuity Management Program Manual* ("BCP"), as well as divisional BCPs require immediate updates in the following areas: **1A: Missing/Outdated Content Details** IA noted several instances where relevant information should be included or updated within the BCP (refer to specifics in the Observation section). Also, some of the recovery processes in the *NW BCP for Information Technology Services* are based on the scenario of "If we are able to speak/communicate with employees" (pg. 7 & 10); the opposite scenario of "what if we	Yes	**Recommendation 1 Updates of Business Continuity Plans** IA recommends updating both the corporate Business Continuity Plan (BCP) and the divisional BCPs as follows: **1A/1B/1C**. Implement defined BCP Maintenance roles and responsibilities in each business unit to ensure timely update/augmentation of the plan content, process and procedures as well as recovery teams contact information. Specific to 1A, include what actions should be undertaken when unable to speak/communicate with employees. **1D**. Develop and implement a list of pre-defined as well as prioritized communication tasks with roles and responsibilities similar to the Disaster Declaration Notification tasks (pg. 40)	Yes	1A- Updates to missing and outdated information in the BCP will be made where applicable. This includes IT&S response to staff communication. Guidance will be added to the NW BCP for Technology Services in the event IT&S personnel are unable to communicate with staff in a disaster. 1B - Administrative Services and Facilities communicated to the Organizational Assessment Division again and will work with them to get their divisional plan created and included in the BCP. IT&S will modify the Cyber Security team in Business Continuity Management (BCM)	4/30/2022 4/30/2022	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
are NOT able to" is not addressed. **1B: Absence of Key Business Unit and Division** Review of the BCP, Section 2, Management Organizational Framework (pg. 8-17), IA noted the absence of the IT&S Cybersecurity and Information Risk Management team. Specifically, the team was not listed within the Business Continuity Management (BCM) Team Structure (Appendix A) and the Information Technology Recovery Team section (pg. 15). This team is especially critical in assessing that the corporation's response and reaction to a declared crisis are effective for services provided (Cloud Based). In addition, divisional business continuity plans are part of the overall BCP. However, IA noted that the Organization Assessment Division (OAD) business continuity plan is not reflected in the BCP. **1C: Outdated Divisional Recovery Teams Information**		within the BCP, to render efficient and effective time management during a crisis. IA also recommends updating the list of critical vendors at the company level with assigned vendor contact roles and responsibilities to serve as a single point of reference for shared cloud services to avoid potential duplicate efforts by divisions during a crisis. **1E.** Design and administer role-based computer-based training (CBT) to heighten employee awareness and familiarity in terms of disaster identification, disaster reporting, and adequate next step process and procedures to minimize business interruptions. **1F**. Designate/identify the local go-to location among all offsite storage locations, this includes DC and all other field offices, where a hard copy and an electronic copy (e.g., thumb drive), of the most current BCP is available should the need		Team Structure (Appendix A) and the Information Technology Recovery Team section (pg. 15) 1C - All divisions are given the same opportunity and reminder to periodically update their divisional plans. Administrative Services and Facilities made quite a few updates over the years and all changes are tracked and recorded. While it is up the division to update their plans when prompted, Administrative Services and Facilities will include a sign off sheet requiring all SVP's indicate they did/did not make any changes. Administrative Services and Facilities will also encourage the divisions to include position titles where applicable and not just names which can change often. Additionally, there is no requirement that the	4/30/2022	

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
Within the BCP each division's business continuity plan has been included with a respective recovery team member list. IA's review found that for all divisions included had outdated recovery team lists comprised of inactive staffers whose employment has been either terminated or changed due to internal transfer to another business unit. Similarly, new hires have also not been added to the lists. **1D: Redundant Lines of Communication** According to COBIT controls, during a crisis, effective communication must ensure information flows throughout the corporation; communication should also be ensured with external parties, such as customers, suppliers, regulators and shareholders. IA noted several Cloud Service Providers (CSPs) are identified as Critical Vendors in multiple divisional business continuity plans due to shared services (e g (b) (5) [redacted] . The BCP does		present itself to obtain a copy during a crisis. It is critical to keep the storage location information current in all BCPs. Lastly, reviewing and updating the BCP should be conducted at least annually. However, frequent or real-time reviews and updates may be required as changes to the Corporation occur.		changes to employee is immediately reflected in the BCP. These changes can be made during the next divisional updates. 1D – IT&S will coordinate with the organization and lead the effort to update the BCP to provide guidance as to which division/stakeholder should contact critical Cloud Service Providers. 1E - There is no BCP/DR training for staff. NeighborWorks America does not have BCP or DR training program. Administrative Services and Facilities will work with HR to see if there's an option within our existing Grovo system to do this and determine if this type of training is practical and necessary given the wide range of BCP scenarios and divisional plans that are all very different.	4/30/2022 4/30/2022	

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
not provide instructions or guidance as to which division should contact the CSP in case of an event. This could lead to redundant vendor communication flows during a crisis without coordination. **1E: Absence of Disaster Recovery/Business Continuity (Awareness) Training Plan** According to the Crisis Management Implementation Plan in the BCP, the person who observed an incident is to *"Identify potential disaster, Conduct Quick Assessment, then Notify Management and Authorities."* Per the BCP, one of the responsibilities of the BCP Oversight Team is to ensure staff are properly trained on Business Continuity processes (pg. 10). IA was informed that DR/BC training for all staff is not provided. Training would heighten the awareness level as well as to help staff better position themselves in preparing to react to incidents, disasters and crisis in an organized, effective and efficient manner accordingly.				1F - The BCP is located on INW and the Senior Leadership team have copies of the BCP on a FOB that is kept with them at home. This is considered offsite storage location and is redundant as all of them have the same information and there are over 15 of them. IT&S will place a hard copy of the BCP at the offsite location as well.	4/30/2022	

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
Training should be provided to all staff, including those directly responsible for recovery team efforts as well as those not directly engaged on a recovery team. **1F: Unspecified Location Where Spare Hard Copy of Current BCP Are Available During Declared Disaster** According to COBIT business continuity management best practice and per the BCP (pg. 7), a current version of the BCP should be maintained and made available at an off-site storage location. There is no designated offsite storage location(s) identified in the policy and planning documents where a copy of the current BCP is available during a declared crisis. **Risk Rating**: (b) (5)						
Observation 2 Inconsistent Cloud Service Provider Information in Inventory Documents	Yes	**Recommendation 2 Cloud Service Providers Alignment** Internal Audit strongly recommends the alignment of the cloud service providers	Yes	IT&S will review NWA BCP Application Matrix spreadsheet, which was originally created as part of the external audit review conducted by	12/31/2021	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
IA compared the current NWA BCP Application Matrix spreadsheet to the current IT Service Provider Inventory spreadsheet and noticed the two documents do not cross-reference each other in terms of cloud service providers information captured therein. This makes it difficult to establish a single point of reference for the collective information of active CSPs for Divisions to decide whether a specific CSP should be identified as critical vendor to contact during crisis in their respective BCP. This could be another contributing factor to the potential redundant communication as described in 1D. Incidentally, the corporation only has 14 SOC2 reports on file, roughly 18%, to assure the level of security and safety of the provided cloud services, out of the 80 Cloud Service Providers identified in the matrix spreadsheet and the 78 in the Inventory spreadsheet. **Risk Rating**: (b) (5)		(CSPs) between the NWA BCP Application Matrix spreadsheet and the IT Service Provider Inventory spreadsheet to ensure both contain the same cloud service providing vendors the corporation is currently in contract with, in conjunction with completing the implementation of recommendation 2, Designation of Interim Central Repository for All Cloud Service Agreements Using Existing Tools/Applications, from the FY19 audit review Cloud Based Provider Agreements Audit Report, as well as recommendations 3, Implementation of Oversight Process and Procedure for CSPs, from IA's FY17 Audit Review WeConnect Cloud Application IT Security Audit Report.		Bazilio Cobb in 2017, with the more recent information stored in the IT&S Application inventory database. IT&S will consolidate the information in order to provide one centralized data source.		

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 3 **Annual Performance and Review Are Not Practiced According to Test Schedule Outlined in the Policy.** According to Section 4, Performance & Review, in the current *NeighborWorks America Business Continuity Plan Policy*, three (3) tests are outlined to be performed each year, with an update of divisional BCP as needed (Appendix B). Other than the Tabletop Testing, Exercise and Validation test, which was last exercised in April 2019, but was not conducted company-wide to involve all field offices, the other tests are yet to be performed according to IT&S. Failure to perform the annual testing and real time update of the BCPs will subject the corporation to be under-prepared for incidents in assuring NWA business operations to carry on without interruptions. **3A: Absence of Recovery Site Testing (Test Plan, Schedule, Process and Procedures)**	**Yes**	**Recommendation 3** **Development and Implementation of Recovery Site Testing Plan** Internal Audit recommends the corporation adhere to the pre-defined annual performance and review schedule in the policy. Including recovery site testing after the timely completion of the development and implementation of a formal recovery site testing plan to augment Section 4 in the policy document. At a minimum, the site recovery test plan should include the following: • When (test frequency) • Who (roles and responsibilities) • What (results and remedial actions) • Where (on-site and/or off-site) • How (test methods)	**Yes**	3 - Annual testing was being done, however a formal tabletop exercise was not completed for 2020 given we are currently in a national pandemic and in the middle of an actual BCP incident, which NeighborWorks America has successfully been able to navigate. Additionally, not all tabletop exercises will include all divisions and all locations. Some exercises are facility displacement, some are specific to systems being shut down (that only affect some divisions), some exercises will be specific to location. It may not always be feasible from a time and effort perspective to conduct an organizational wide BCP tabletop exercise every year. Administrative Services and Facilities will look at whether this is something	04/30/2022	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
Per the Business Continuity Planning Objectives stated in the BCP, within five business days of an interruption that prevents processing in the primary data center IT management will re-establish critical systems and data at the recovery site. However, recovery site testing has not been conducted nor is it identified as part of the annual testing in the policy since contracting with the current recovery site provider in October 2019. Failure to conduct recovery site testing could place the corporation at a disadvantage to recover and produce desired outcome during any given crisis. **Risk Rating**: (b) (5)				that NW should continue to commit to doing and updating our requirements to specify a reasonable and doable schedule. 3A - Since mid-March 2020, NW personnel have been working from home due to Covid-19. This pandemic has tested and validated many portions of the NW and IT&S BCP disaster plans. In February 2021, IT&S successfully created servers and restored the NIS environment using backups and equipment located (b) (5) data center. Management agrees with the recommendation to conduct a recovery exercise from the (b) (5) data center. However, any test will need to wait	09/30/2022	

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
				until Covid-19 pandemic restrictions are lifted.		

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.

<table>
<tr><th colspan="3">Management Responses to
The Audit Review of:

Disaster Recovery Business Continuity (Cloud Based)</th></tr>
<tr><th># Of Responses</th><th>Response</th><th>Recommendation #</th></tr>
<tr><td>5</td><td>Agreement with the recommendations 1A, 1B, 1C, 1D and 1E</td><td>1</td></tr>
<tr><td>1</td><td>Agreement with the recommendation</td><td>2</td></tr>
<tr><td>1</td><td>Agreement with the recommendation</td><td>3</td></tr>
<tr><td></td><td>Disagreement with the recommendations</td><td></td></tr>
</table>

Background

The last Corporate Disaster Recovery (DR) & Business Continuity (BC) audit review was conducted in 2017, prior to the publication of the current version of the *NeighborWorks America Business Continuity Plan Policy* and the *NeighborWorks America Business Continuity Program Manual* in December of 2019. In addition, over the last several years NeighborWorks has transitioned significant business systems and applications to cloud-based platforms. Given the Corporation's dependency on cloud-based platforms and the time since the last audit in 2019; it became imperative to evaluate the current status of the DR/BC Policy and Procedures for its effectiveness and efficiency from a Cloud Based perspective.

Objective

The objective of this review was to obtain reasonable assurance that the corporation has adequate onsite/offsite disaster recovery and business continuity management protocols in place and that the operational risks associated with cloud service providers (CSPs) are adequately managed and monitored.

Scope

The scope of this audit review is outlined as follows:

- Corporate disaster recovery and business continuity program policies, management, process and procedures
- Divisional disaster recovery and business continuity program management, process and procedures
- Onsite and offsite storage and locations
- Active Cloud Service Providers (CSPs) between Q1 FY20 and Q3 FY20

Methodology

Based on COBIT[2] 4.1 and COBIT 5 Control Guidance for Business Continuity Management as well as IT Continuity Planning IA focused on the verification and validation of the following:

- Business Continuity Plan (BCP) Management
- BCP Policy, Standards and Procedures
- Business Impact Analysis (BIA)
- Documentation
- Plan Testing
- Risk Assessment

[2] COBIT: acronym for Control Objectives for Information and Related Technology, is a set of IT control objectives originally developed and released by ISACA (Information System Audit and Control Association) to help the financial audit community better navigate the growth of IT environments; the control framework has since been expanded to apply outside the accounting community to include IT management and information governance techniques.

Below are the observations and recommendations that resulted from the testing performed.

Observations and Recommendations

Observation 1 – Incomplete/Outdated Business Continuity Plans, Process and Procedures.

Internal Audit observed that the current *NeighborWorks America Business Continuity Management Program Manual* ("BCP"), as well as divisional BCPs required immediate updates in the following areas:

1A: Missing/Outdated Content Details

Internal Audit noted several instances where relevant information should be included or updated within the BCP. The following are examples and may not be the only sections that require review and updating:

- Section 4, Exercise Tasks, there is no detailed description for Task 5: Pre-Exercise Notification (pg. 28);
- The Disaster Declaration Notification section (pg. 40), task number nine refers to "communication tasks" which are not defined within the BCP;
- The Disaster Assessment Team is mentioned (pg. 13) and included in the Business Continuity Management (BCM) Team Structure (Appendix A), but not clearly defined (e.g. IT&S Assessment Personnel, Administrative Services Assessment Personnel);
- The previous recovery site, DXC Technology, is still referred to within the BCP (pg. 41) which has been replaced (b) (5)

Lastly, some of the recovery processes in the *NW BCP for Information Technology Services* are based on the scenario of "If we are able to speak/communicate with employees" (pg. 7 & 10); the opposite scenario of "what if we are NOT able to" is not addressed a more probable scenario in the event of a disaster.

1B: Absence of Key Business Unit and Division

In our review of the BCP, Section 2, Management Organizational Framework (pg. 8-17), Internal Audit noted the absence of the IT&S Cybersecurity and Information Risk Management team. Specifically, the team was not listed within the Business Continuity Management (BCM) Team Structure (Appendix A) and the Information Technology Recovery Team section (pg. 15). This team is especially critical in assessing that the corporation's response and reaction to a declared crisis are effective for services provided in the cloud. In addition, divisional business continuity plans are part of the overall BCP. However, Internal Audit noted that the Organization Assessment Division (OAD) business continuity plan is not reflected in the BCP.

1C: Outdated Divisional Recovery Teams Information

Within the BCP each division's business continuity plan has been included with a respective recovery team member list. Internal Audit's review found that for all divisions included had outdated recovery team lists comprised of inactive staffers whose employment has been either terminated or changed due to internal transfer to another business unit. Similarly, new hires have also not been added to the lists.

1D: Redundant Lines of Communication

According to COBIT controls, during a crisis, effective communication must ensure information flows throughout the corporation; communication should also be ensured with external parties, such as customers, suppliers, regulators and shareholders. Internal Audit noted several Cloud Service Providers (CSPs) are identified as Critical Vendors in multiple divisional business continuity plans due to shared services (e.g., (b) (5) [redacted]). The BCP does not provide instructions or guidance as to which division should contact the CSP in case of an event. This could lead to redundant vendor communication flows during a crisis without coordination.

1E: Absence of Disaster Recovery/Business Continuity (Awareness) Training Plan

According to the Crisis Management Implementation Plan in the BCP, the person who observed an incident is to *"Identify potential disaster, Conduct Quick Assessment, then Notify Management and Authorities."* Per the BCP, one of the responsibilities of the BCP Oversight Team is to ensure staff are properly trained on Business Continuity processes (pg. 10). Internal Audit was informed that DR/BC training for all staff is not provided. Training would heighten the awareness level as well as to help staff better position themselves in preparing to react to incidents, disasters and crisis in an organized, effective and efficient manner accordingly. Training should be provided to all staff, including those directly responsible for recovery team efforts as well as those not directly engaged on a recovery team.

1F: Unspecified Location Where Spare Hard Copy of Current BCP Are Available During Declared Disaster

According to COBIT business continuity management best practice and per the BCP (pg. 7), a current version of the BCP should be maintained and made available at an off-site storage location. There is no designated offsite storage location(s) identified in the policy and planning documents where a copy or copies of the current BCP is available during a declared crisis.

Recommendation 1 - Update the Business Continuity Plans

IA recommends updating both the corporate Business Continuity Plan (BCP) and the divisional BCPs as follows:

1A/1B/1C. Implement defined BCP Maintenance roles and responsibilities in each business unit to ensure timely update/augmentation of the plan content, process and procedures as well as recovery teams contact information. This should also include what actions should be undertaken when unable to speak/communicate with employees.

1D. Develop and implement a list of pre-defined as well as prioritized communication tasks with roles and responsibilities, similar to the Disaster Declaration Notification tasks (pg. 40) within the BCP, to render efficient and effective time management during a crisis. Internal Audit also recommends updating the list of critical vendors at the company level with assigned vendor contact roles and responsibilities to serve as a single point of reference for shared cloud services to avoid potential duplicate efforts by divisions during a crisis.

1E. Design and administer role-based computer-based training (CBT) to heighten employee awareness and familiarity in terms of disaster identification, disaster reporting, and adequate next step process and procedures to minimize business interruptions.

1F. Designate/identify the local go-to location among all offsite storage locations, this includes DC and all other field offices, where a hard copy or copies and an electronic copy (e.g., thumb drive), of the most current BCP is available should the need present itself to obtain a copy during a crisis. It is critical to keep the storage location information current in all BCPs.

Lastly, reviewing and updating the BCP should be conducted at least annually. However, frequent or real-time reviews and updates may be required as changes to the Corporation occur.

Observation 2 – Inconsistent Cloud Service Provider Information in Inventory Documents
Upon comparing the current NWA BCP Application Matrix spreadsheet[3] to the current IT Service Provider Inventory spreadsheet[4], Internal Audit noticed the two documents do not cross-reference each other in terms of cloud service provider (CSPs) information captured therein. This makes it difficult to establish a single point of reference for the collective information of active CSPs for Divisions to decide whether a specific CSP should be identified as critical vendor to contact during crisis in their respective BCP. This could also contribute to redundant communications as described in 1D.

Incidentally, IA's review of the matrix spreadsheet and the inventory spreadsheet found that the corporation only has 14 SOC 2 reports on file for CSPs. The spreadsheet's list 80 and 78 CSPs, respectively. Roughly 82% of the CSPs listed on the spreadsheets have not provided their SOC 2 report[5]. The SOC 2 reports are essential to obtain from CSPs to assure the level of security and safety of the company's data.

Recommendation 2 Cloud Service Providers Alignment

Internal Audit recommends the alignment of the cloud service providers (CSPs) between the NWA BCP Application Matrix spreadsheet and the IT Service Provider Inventory spreadsheet to ensure both contain the same cloud service providers. This would further augment the implementation of recommendation 2[6] from the FY19 audit review, Cloud Based Provider

[3] NWA BCP Application Matrix spreadsheet: contains the listing of the corporation's critical business processes and the application system supporting each process – includes all platforms. Furthermore, the business continuity sustainability requirements are also identified in terms of Application Recovery Time Objective (ARTO), the division's tolerance for data loss, is data recreation required, etc.

[4] IT Service Provider Inventory spreadsheet: identifies the name of active cloud service providers, service model (IaaS, SaaS, PaaS, etc.) and application system offered by the service provider.

[5] A SOC 2 report is an examination of vendor controls in the areas of security, privacy, availability, confidentiality and processing integrity.

[6] Recommendation 2 (Cloud Service Provider Agreements Audit Report): Consolidate Cloud Service Agreements and all supporting documents to a central location to achieve the integrity of the corporation's Cloud base agreements and service subscriptions.

Agreements Audit Report. As well as recommendation 3[7] from the FY17 Audit Review, WeConnect Cloud Application IT Security Audit Report.

Observation 3 – Annual Performance and Review Are Not Practiced According to Test Schedule Outlined in the Policy.

According to Section 4, Performance & Review, in the current *NeighborWorks America Business Continuity Plan Policy*, scheduled testing, updates and maintenance are outlined to be performed each year, with an update of divisional BCP as needed (Appendix B). Other than the Tabletop Testing, Exercise and Validation, which was last exercised in April 2019, but was not conducted company-wide to involve all field offices, the other actions are yet to be performed according to IT&S. Failure to perform the annual testing and real time update of the BCPs will subject the corporation to be under-prepared for incidents in assuring NWA business operations to carry on without interruptions.

3A: Absence of Recovery Site Testing (Test Plan, Schedule, Process and Procedures)
Internal Audit determined that recovery site testing (an integral part of the BCP maintenance) has not been conducted nor is it identified as part of the annual testing in the policy since contracting with the current recovery site provider in October 2019. The Corporations Business Continuity Planning Objectives states in the BCP, that within five business days of an interruption that prevents processing in the primary data center, IT management will re-establish critical systems and data at the recovery site. Having not undergone a testing procedure provides no assurance of the Corporation's ability to meet planned recovery times as identified. As a result, failure to conduct recovery site testing could place the corporation at a disadvantage to recover and produce desired outcome during any given crisis.

Recommendation 3 Development and Implementation of Recovery Site Testing Plan

Internal Audit recommends the corporation adhere to the pre-defined annual performance and review schedule in the policy. This should include the conduct of an annual recovery site testing after the timely completion of the development and implementation of a formal recovery site testing plan to augment Section 4 in the policy document. At a minimum, the site recovery test plan should include the following:

- When (test frequency)
- Who (roles and responsibilities)
- What (results and remedial actions)
- Where (on-site and/or off-site)
- How (test methods)

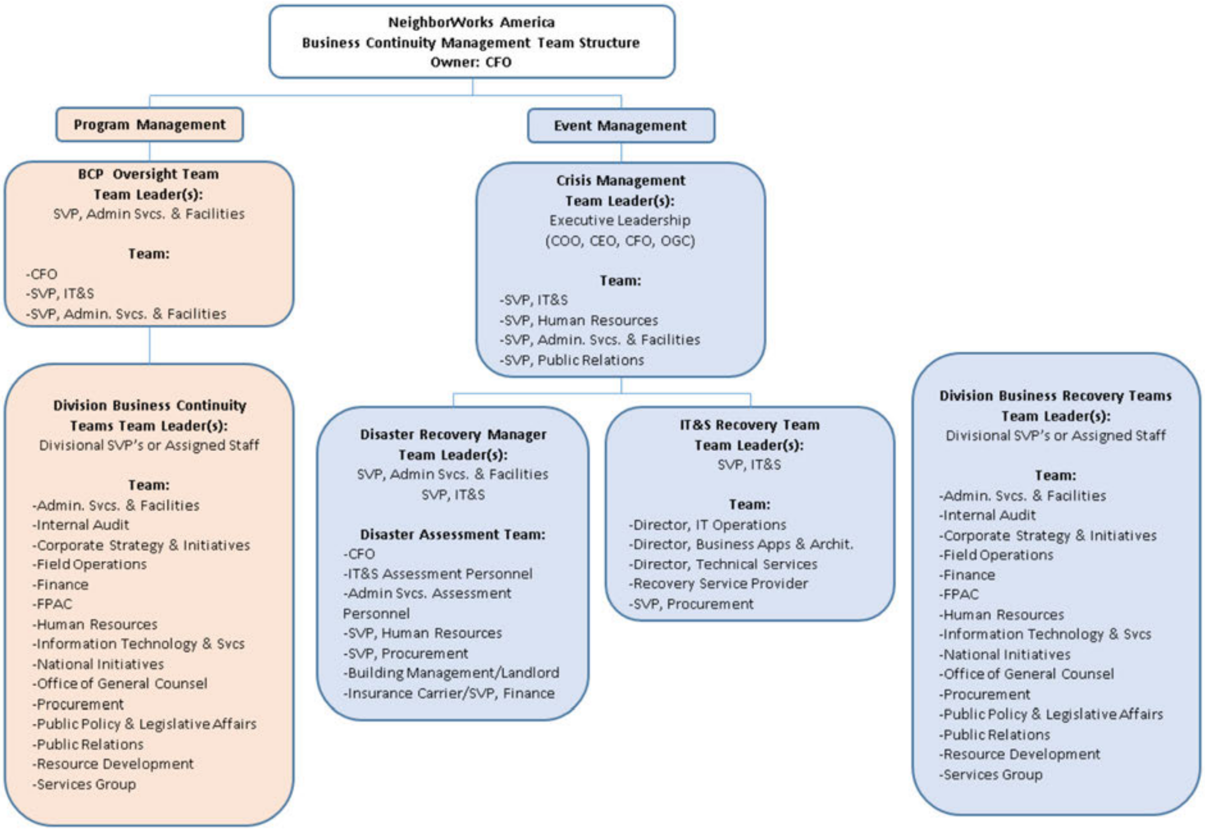
In addition, IT&S should provide Internal audit with a copy of the Test Plan and Test report on completion.

[7] Recommendation 3 ((b) (5) Cloud Application IT Security Audit Report): Implementation of Oversight Process and Procedures for Cloud Service Providers including request for the delivery of annual SOC reports.

Conclusion

Maintaining a practical and current version of both corporate and divisional business continuity policy, process and procedures is critical to the effective management, monitoring and assurance of business continuity during a declared disaster and/or crisis. Real time updates of recovery teams, critical vendors and communication protocols are the base criteria to warrant orderly business conduct during a time of crisis. In addition, the corporation should perform periodic exercise and awareness training to ensure staffers are well prepared to react during any given incident to transition from standard business operation mode to business sustainability mode. As the corporation is steadily moving to cloud-based service providers, timely revision and augmentation to its business continuity policy, process and procedures is essential.

Appendix A: Business Continuity Team Structure - Management & Oversight


NeighborWorks America
Business Continuity Management Team Structure
Owner: CFO
Program Management
Event Management
BCP Oversight Team
Team Leader(s):
SVP, Admin Svcs. & Facilities
Team:
-CFO
-SVP, IT&S
-SVP, Admin. Svcs. & Facilities
Crisis Management
Team Leader(s):
Executive Leadership
(COO, CEO, CFO, OGC)
Team:
-SVP, IT&S
-SVP, Human Resources
-SVP, Admin. Svcs. & Facilities
-SVP, Public Relations
Division Business Continuity
Teams Team Leader(s):
Divisional SVP's or Assigned Staff
Team:
-Admin. Svcs. & Facilities
-Internal Audit
-Corporate Strategy & Initiatives
-Field Operations
-Finance
-FPAC
-Human Resources
-Information Technology & Svcs
-National Initiatives
-Office of General Counsel
-Procurement
-Public Policy & Legislative Affairs
-Public Relations
-Resource Development
-Services Group
Disaster Recovery Manager
Team Leader(s):
SVP, Admin Svcs. & Facilities
SVP, IT&S
Disaster Assessment Team:
-CFO
-IT&S Assessment Personnel
-Admin Svcs. Assessment
Personnel
-SVP, Human Resources
-SVP, Procurement
-Building Management/Landlord
-Insurance Carrier/SVP, Finance
IT&S Recovery Team
Team Leader(s):
SVP, IT&S
Team:
-Director, IT Operations
-Director, Business Apps & Archit.
-Director, Technical Services
-Recovery Service Provider
-SVP, Procurement
Division Business Recovery Teams
Team Leader(s):
Divisional SVP's or Assigned Staff
Team:
-Admin. Svcs. & Facilities
-Internal Audit
-Corporate Strategy & Initiatives
-Field Operations
-Finance
-FPAC
-Human Resources
-Information Technology & Svcs
-National Initiatives
-Office of General Counsel
-Procurement
-Public Policy & Legislative Affairs
-Public Relations
-Resource Development
-Services Group

Source of information: *NeighborWorks America BCP – March 2020.pdf*

Appendix B: Disaster Recovery Testing Schedule

4 Performance & Review

NeighborWorks America, in its need for business continuity management, aims to have annual performance and review through the following timeline and schedule as indicated in Section 4 of the Business Continuity Plan Introduction:

Test Time	Test Name /Description
October	Table Top Testing, Exercise & Validation
	Testing performed with each division/department that includes Loss of facility and/or system loss scenarios.
November	Plan updates, Maintenance & After Action report
	Changes and updates to the BCP based on gap analysis and/or identified deficiency results from the Table Top Exercises. Final execution report, also known as the (AAR) After Action Report will be provided to the officers and include a summary of the TTX and any resulting subsequent changes to the BCP.
Bi-Annual	Divisional/Departmental Plan Check in and changes
	Bi-annual check in with divisions/departments to identify and make any significant changes to divisional/departmental BCP. This includes changes to critical processes or new discoveries as it relates to financial impacts, new system implementations, staffing, divisional/departmental restructures, and/or IT&S related adjustments.
Annual	Information Technology & Services
	IT&S system and applications recovery will be tested at least once a year or subsequent to the implementation of major changes that affect the applications, system or network.
As Needed	Plan Updates
	Any significant changes to the plan will be completed immediately. This includes major changes to the operational and IT& support and infrastructure, changes to leadership and owners that affect the management and oversight framework as listed in Section 2. Of the BCP Manual Introduction.

Data source: *NeighborWorks America Business Continuity Plan Policyty.pdf*