Internal Audit
NeighborWorks® America

Audit Review of

WeConnect Cloud Application

IT Security

Project Number: NW.ITS.CLDSEC.2017

Audit Review of WeConnect Cloud Application IT Security

Table of Contents

November 20, 2017

To: NeighborWorks America Audit Committee

Subject: Audit Review of WeConnect Cloud Applications IT Security

Enclosed is our draft audit report for the WeConnect Cloud Applications IT Security review. Please contact me with any questions you might have.

Thank you.

Frederick Udochi
Chief Audit Executive

Attachment

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

Function Responsibility and Internal Control Assessment
Audit Review of WeConnect Cloud Applications IT Security

Business Function Responsibility	Report Date	Period Covered
IT&S	November 20, 2017	October 2016 – August 2017
Assessment of Internal Control Structure		
Effectiveness and Efficiency of Operations		**Generally Effective**[1]
Reliability of Financial Reporting		**Not Applicable**
Compliance with Applicable Laws and Regulations		**Not Applicable**

This report was 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.

Summary Results of Procedures Performed

Objective	Design	Operation	Finding Reference
Architecture			02
Review of Cloud Agreements			05
Change Management			01
Disaster Recovery			04
Review of Information Security Processes and Monitoring			01
Review of Logical Access Permission Management			06
Review of Processes to Reduce Exposure to Vendor Lock-in			03
Review of SOC Reports			04
Information Security Program			06

Key:	
	No issues noted from procedures performed
	Opportunities for improvement
	Deficiency noted
	Significant deficiency/material weakness

Executive Summary of Observations, Recommendations and Management Responses

Summarized Observation Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response
Observation No. 1 **Monitoring Tools** Applications supported in a cloud model should allow for monitoring tools to be put in place to monitor for unauthorized activity. Our review of the eight cloud applications which are maintained by different cloud service providers in the United States and Canada indicated that monitoring tools have not been implemented across all of the cloud environments that maintain NeighborWorks® America's applications. **Risk Rating**: (b) (4)	**Yes**	**Recommendation No. 1** **Monitoring Tools** We recommend that management implement software and related support processes to maintain monitoring of NeighborWorks® America's data and applications supported by the various cloud services providers.	**Yes**	Monitoring for unauthorized access, suspicious activity, and unauthorized application changes is a continual process, and we have implemented or plan to deploy tools in each area: Single Sign On uses only (b) (4) to validate NetSuite, UltiPro, and its accompanying expense and purchasing applications. A monthly monitoring report	(b) (4)	IA accepts management 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
				synchronizes and monitors for any discrepancies between (b) (4) and the UltiPro employee roster. A user cannot authenticate into any Cloud application without an active (b) (4) account. This is a best practice improvement available through the Cloud SaaS usage of SSO and is further strengthened by (b) (4) . A 2018 major initiative for (b) (4)		

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
				[redacted] is underway to ensure: "the [redacted] access the right [redacted]". IT&S intends to acquire a [redacted] solution that will [redacted] from all WeConnect application and provide immediate alerts on suspicious activity. We're also in the process of researching the capabilities of a [redacted] that will be used to monitor web traffic and		

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
				prevent high risk threats and vulnerabilities (e.g. – Distributed Denial of Service of web assets, SQL injection, etc.). Daily report of all NetSuite application changes is emailed to key monitoring personnel in IT&S, IA, etc. We are working to add additional monitoring reports.		
Observation No. 2 **Vendor Lock-in** NeighborWorks® America has approximately eight applications that are maintained by various cloud service providers. Because	**Yes**	**Recommendation No. 2** **Vendor Lock-in** We recommend that management implement processes to receive periodic back-up's of transactional and master data files from the	**Yes**	IT&S agrees that planning and preparing for a possible move is part of enterprise risk management. However, NetSuite and its parent	Q4 FY2019	IA accepts management 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
the applications are operated in a SaaS cloud deployment model, the eight cloud vendors maintain complete control of NeighborWorks® America's data, which includes human resources, payroll, procurement, and general ledger information. A process has not been put in place for NeighborWorks® America to make or receive periodic back-ups of data from the applications maintained by cloud service providers. **Risk Rating:** (b) (4)		various cloud service providers.		Oracle provide the industry's best and secure data centers. The periodic backup recommendation really adds more risk to an operational area that is solidly solved by our current vendors and our operations would be made less secure by adding manual periodic backups. Please refer to http://www.netsuite.com/portal/assets/pdf/ds-data-center-factsheet.pdf for more information		

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
				regarding the level of security.		
Observation No. 3 **Oversight of Cloud Providers** Service Organization Control (SOC 1 and 2) reports help maintain oversight and visibility of controls at cloud service providers and hosting facilities. Our review of the oversight for cloud service providers indicated the following; (i) we were unable to identify a formal process in place to review the SOC reports and perform follow-up on concerns identified that may adversely impact the assets of NeighborWorks® America; (ii) evidence could not be provided to show that a SOC report was received for	**Yes**	**Recommendation No. 3** **Oversight of Cloud Providers** ▪ We recommend that management put oversight processes in place to require obtaining and reviewing a current SOC 1 or 2 report for each of the cloud service provider. ▪ Oversight procedures should also require follow-up to determine the risk implication to NeighborWorks® America's assets for adverse opinions or	**Yes**	IT&S has an established process in place to request Service Organization Control (SOC 1 and 2)/SSAE 16/SSAE 18 as a part of the acquisition/procurement process. The service provider during this audit were handled within the purchasing program office at the time of acquisition and did not go through centralized procurement.	Q4 FY2018	IA accepts management 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
the following cloud service providers. (b) (4) - Grants Management (b) (4) - Checking Writing (b) (4) - Grants The SOC report provided was not within 12 months for (b) (4). The initial SOC report provided covered the period 11/2014 to 10/2015 for (b) (4). A more current SOC report was obtained during our fieldwork. **Risk Rating:** (b) (4)		high exception rates. ▪ We also recommend that the Corporation require and request the annual delivery of SOC reports or the equivalent of all applications in WeConnect including those we were unable to obtain as part of this review.		IT&S requests and reviews SSAE 16 SOC reports on annual basis. At the time of this review IA had not provided us with their most current report because they had yet to complete their independent assessment.		
Observation No. 4 **Cloud Service Provider Agreements** Our review of cloud vendor agreements indicated that a process is not in place to ensure that all agreements	**Yes**	**Recommendation No. 4** **Cloud Service Provider Agreements** ▪ We recommend that the Office of General Counsel determine the baseline	**Yes**	The Office of General Counsel (OGC) will continue to review agreements that are provided to them via the Procurement Process and	Q2 FY 2018	IA accepts management 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
have a standard informational (that protects the information assets of the Corporation) requirement that should always be included in such agreements. Concerns identified were as follows: ▪ Cloud Provider Service Agreements did not always specify a specific timeframe for returning NeighborWorks® America's data and related assets in the event that the business relationship with the cloud service provider is terminated. ▪ Cloud agreements did not always specify a timeframe to notify NeighborWorks® America in the event of a data breach.		disclosures that should be included in all finalized cloud service agreements. ▪ Implement processes to ensure that the Information Security addendum is part of the finalized contract. ▪ Implement processes to ensure that all cloud service agreements are subject to review by the Office of General Counsel.		NeighborWorks America Program Offices. IT&S will work with Procurement, Office of General Counsel and WeConnect Service Providers to update the terms and conditions with their agreements to be in line with or include NeighborWorks America's Information Security Addendum. Finance and Administration Division (specifically Information Technology & Services and		

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
▪ Cloud service agreements did not always specify disaster recovery contingencies. ▪ Two of the eight cloud vendor agreements did not reference the service level requirements needed by the Corporation (ASC-Procurement also known as (b) (4) and (b) (4) -Check Processing). ▪ One cloud agreement was not signed (fully executed) by both parties (Adaptive Insights) based on the copies provided to Internal Audit. ▪ We were unable to obtain evidence of a formal review process by the Office of General Counsel on the majority of Cloud				Procurement) and Office of General Counsel agree to develop a formal policy and communication to the organization that states all cloud service provider agreements, regardless of cost, must be reviewed and approved by Office of General Counsel before finalizing the agreement.		

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
Provider Service Agreements for the specific components of the cloud relationship from a legal perspective. **Risk Rating:** (b) (4)						
Observation No. 5 **Information Security Processes** ▪ A process is not in place to perform periodic risk assessments of the Information Security threats associated with each of the eight cloud service providers to determine whether adequate processes are in place to mitigate the risk. ▪ Current processes do not provide for a form of	**Yes**	**Recommendation No. 5** **Information Security Processes** ▪ We recommend that processes should be implemented to perform risk assessments of each cloud service provider. ▪ Follow-up should be performed to determine if vulnerability assessments can be	**Yes**	IT&S is in agreement with this observation and recommendation. IT&S intends to have an external penetration exercise conducted during this fiscal year. IT&S will work with NWA Application /Business Process Owner to address potential risks pose	(b) (4)	IA accepts management 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
penetration testing or vulnerability assessment from cloud service providers. To date, this type of testing has been received from two of the eight cloud service providers. ▪ There is no segregation of duties related to system administration and Information Security Administration for the Active Directory and Single Sign-on as well as SaaS applications to include UltiPro (Human Resources and Payroll and NetSuite). Currently, system administration personnel handle both system administration and user access. ▪ Processes have not been put in place to only log		provided at least annually by each cloud service provider. ▪ Processes should be implemented to separate system administration from functional activities. We strongly recommend that Information Technology & Services be required to serve as system administrators and the information security administration function. This can be accomplished by logging a trouble or change ticket using the Corporation's CAB change management process		with administrators performing functional tasks. As mentioned within a prior response, IT&S intends to increase monitoring capabilities with the implementation of (b) (4) [redacted] solution.		

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
into accounts with escalated system administration permissions when needed and to maintain a normal user account for day-to-day activities. Employees that support UltiPro and NetSuite applications log on to accounts that have system administrator permissions, rather than using these accounts only when needed. **Risk Rating:** (b) (4)		to account for and track the use of system administrator accounts.				

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 Responses to The Audit Review of: WeConnect Cloud Applications IT Security		
# Of Responses	**Response**	**Recommendation #**
5	Agreement with the recommendation(s)	1,2, 3,4,5
	Disagreement with the recommendation(s)	

Introduction

NeighborWorks® America's management implemented a comprehensive ERP system that was cloud-based, internally branded as WeConnect on October 1, 2016. This was a major shift from having on-site applications to off-site (cloud-based) under the software licensing and delivery model of Software as a Service (SaaS). This is a model by which software is licensed on a subscription basis and is centrally hosted. Even though centrally hosted, the Corporation is still responsible for establishing and maintaining security assurance around cloud-based information technology assets from unauthorized access, use or disposition and the integrity of data or transactions that reside within. This review is being undertaken to make an assessment on that assurance given also that cloud-based applications are new to the organization.

Internal audit co-sourced this project with SB & Company LLC to provide technical expertise in the area of cloud-based applications security and a profile of the staff can be found in Appendix A. SB & Company performed certain procedures to identify any related risks to NeighborWorks® America's WeConnect cloud environment. The scope of the WeConnect cloud security audit is included below.

Scope

The scope of this audit review entailed the following:

- To determine that the architecture allows for adequate support processes of the WeConnect cloud applications.
- That Cloud agreements maintain a standard set of disclosures across all providers.
- Processes are in place to receive and review SOC reports for all service providers.
- Processes and procedures are in place to provide for the appropriate logical access permissions.
- Processes and procedures are in place to reduce risk exposures to vendor lock-in.
- Processes and procedures are in place to prevent or detect unauthorized changes.
- Processes and procedures are in place for the disposal of data.
- Processes and procedures are in place for an Information Security Program.

Methodology

In order to perform this audit, we performed the following procedures:

- Reviewed the architecture and cloud service deployment model.
- Reviewed the cloud service agreement for each cloud service provider.
- Reviewed processes for review and follow-up on SOC reports for cloud service providers.
- Reviewed the appropriateness of logical access permissions to cloud applications.
- Reviewed processes and procedures to reduce risk exposures to cloud vendor lock-in.
- Reviewed processes and procedures to prevent or detect unauthorized changes to cloud applications.
- Reviewed processes and procedures for the disposal of data by cloud service providers.
- Reviewed processes and procedures for information security of assets maintained by cloud service providers.

Findings and Recommendations

1. Monitoring Tools

Applications supported in a cloud model should allow for monitoring tools to be put in place to monitor for unauthorized activity. Critical areas where some level of monitoring to include prevention and detection software include the following:

- Data Loss Prevention Software: Used to prevent or identify attempts to extract data from the clients' systems at the cloud service provider.
- Data Activity Monitoring: Used to identify unauthorized database activity.
- File Activity Monitoring: Used to identify unauthorized activity on critical application files.
- [redacted]: Used to create a repository of potential security events to alert personnel where follow-up is needed.

Our review of the eight cloud applications which are maintained by different cloud service providers in the United States and Canada indicated that monitoring tools [redacted] s that maintain NeighborWorks® America's applications.

Information Security is aware of this and is working to move forward on the implementation of a [redacted]. However, an assessment needs to be performed to determine if some of the [redacted] that are appropriate to an off-premise technology support model should also be implemented.

Recommendation

We recommend that management implement software and related support processes to maintain monitoring of NeighborWorks® America's data and applications supported by the various cloud services providers.

2. Vendor Lock-in

NeighborWorks® America has approximately eight applications that are maintained by various cloud service providers. Because the applications are operated in a SaaS cloud deployment model, the eight cloud vendors maintain complete control of NeighborWorks® America's data, which includes human resources, payroll, procurement, and general ledger information.

A process has not been put in place for NeighborWorks® America to make or receive periodic back-ups of data from the applications maintained by cloud service providers. Receiving periodic back-ups and verifying that the information could be used to restore applications reduces the risk that the vendor has complete access to data and can prevent the move to another cloud service provider if needed.

Recommendation

We recommend that management implement processes to receive periodic back-up's of transactional and master data files from the various cloud service providers. The conduct of a risk assessment to determine which applications would require such back up may help to reduce the cost of such an arrangement.

3. Oversight of Cloud Providers

Service Organization Control (SOC 1 and 2) reports help maintain oversight and visibility of controls at cloud service providers and hosting facilities. The Common Core Criteria is part of the standard SOC report and provide conclusions on the information technology processes and related controls.

Our review of the oversight for cloud service providers indicated the following:

- There is (b) (4) the SOC reports and perform follow-up on (b) (4) the assets of NeighborWorks® America.
- (b) (4) that a SOC report was received for the following cloud service providers.
  - (b) (4) - Grants Management
  - (b) (4) - Checking Writing
  - (b) (4) - Grants
- The SOC report provided was not within 12 months for (b) (4).
  - The initial SOC report provided covered the period 11/2014 to 10/2015 for (b) (4). A more current SOC report was obtained during our fieldwork.

Recommendations:

- We recommend that management put oversight processes in place to require obtaining and reviewing a current SOC 1 or 2 report for each of the cloud service provider. A current SOC report should cover the last calendar year.
- Oversight procedures should also require follow-up to determine the risk implication to NeighborWorks® America's assets for adverse opinions or high exception rates.
- We also recommend that the Corporation require and request the annual delivery of SOC reports or the equivalent of all applications in WeConnect including those we were unable to obtain as part of this review. Currently unavailable are SOC reports for (b) (4).

4. Cloud Service Provider Agreements

Our review of cloud vendor agreements indicated that a process is not in place to ensure that all agreements have a standard informational (that protects the information assets of the Corporation) requirements that should always be included in such agreements. Concerns identified were as follows:

- Cloud agreements did not always specify a specific timeframe for returning NeighborWorks® America's data and related assets in the event that the business relationship with the cloud service provider is terminated.

- Cloud agreements did not always specify a timeframe to notify NeighborWorks® America in the event of a data breach.

- Cloud service agreements did not always specify disaster recovery contingencies.

- Two of the eight cloud vendor agreements did not reference the service level requirements needed by the Corporation ([redacted] also known as [redacted] and [redacted]-Check Processing).

- One cloud agreement was not signed (fully executed) by both parties ([redacted]) based on the copies provided to Internal Audit.

Information Security

NeighborWorks® America has developed an addendum which defines the organization Information Security requirements. However, the Information Security addendum is not always part of the finalized agreement. The Information Security addendum was not evident in the eight agreements reviewed. Discussions indicated that the addendum is provided early in the process. As a result, the cloud service provider may not comply with these requirements.

Legal Review

We were unable to obtain evidence of a formal review process by the Office of General Counsel on the majority of Cloud Provider Service Agreements for the specific components of the cloud relationship from a legal perspective. We determined that the majority of data centers that maintain NeighborWorks® America's applications and data are located in another state or outside of the United States. Therefore, the laws of other states or provinces (e.g., the Personal Information Protection and Electronic Documents Act - PIPEDA**)** would be applicable and legal cross-border implications need to be evaluated as part of any due diligence prior to purchase. Having the Office of the General Counsel to review the cloud service agreement would ensure that there are no risk exposures from a legal perspective. Currently, two of the eight service providers reside in Canada.

Recommendations

- We recommend that the Office of General Counsel determine the baseline disclosures that

should be included in all finalized cloud service agreements. At a minimum all cloud service provider agreements should consist of; (i) the Customer Agreement, sometimes referred to as the "Master Agreement" "Terms of Service" or simply "Agreement" which describes the overall relationship between the customer and provider; (ii) an acceptable Use Policy (AUP) which prohibits activities provides may consider to be an improper use of their services; and. (iii) Service Level Agreement (SLA) which would describe the service level expectations using various attributes such as availability, serviceability or performance through various metrics.

- Implement processes to ensure that an Information Security addendum is part of the finalized contract.

- Implement processes to ensure that all cloud service agreements are subject to review by the Office of General Counsel.
- We recommend that all Cloud Service Agreements be fully executed.

5. Information Security Processes

Our review of NeighborWorks® America Information Security processes indicated the following:

- A process is not in place to perform periodic risk assessments of the Information Security threats associated with each of the eight cloud service providers to determine whether adequate processes are in place to mitigate the risk.

- Current processes do not provide for a form of penetration testing or vulnerability assessment from cloud service providers. To date, this type of testing has been received from two of the eight cloud service providers.

- There is (b) (4) related to system administration and Information Security Administration for the (b) (4) and (b) (4) as well as SaaS applications to include (b) (4). Currently, system administration personnel handle both system administration and user access. In addition to having functional duties the same staff also have super user rights as the administrator.

- Processes have not been put in place to only log into accounts with escalated system administration permissions when needed and to maintain a normal user account for day-to-day activities. Consultants supporting (b) (4) have been provided accounts with persistent system administration permissions. Employees that support (b) (4) applications log on to accounts that have system administrator permissions, rather than using these accounts only when needed.

Recommendations:

- We recommend that processes should be implemented to perform risk assessments of each cloud service provider.

- Follow-up should be performed to determine if vulnerability assessments can be provided at

least annually by each cloud service provider.

- Processes should be implemented to separate system administration from functional activities. We strongly recommend that Information Technology & Services be required to serve as system administrators for the information security administration function. This can be accomplished by logging a trouble or change ticket using the Corporation's Change Authorization Board (CAB) process to account for the use of system administrator accounts. We, however, noted that the Corporation had reported to the Board in one of its weekly WeConnect status updates that it plans to implement CAB with an estimated completion date by the end of FY 18 Q1.

Conclusion

The WeConnect cloud-based security review is quite significant given the rise in cyber threats in today's environment. We hope that the recommendations raised here would be adopted accordingly in order to provide the necessary framework for monitoring our cloud-based vendors and also in keeping the security and integrity and access to our transactional data secure. We would like to take this opportunity to thank the staff of Information Technology and Services for their cooperation throughout this review.

APPENDIX A - Profile

Position: Principal, IT Risk Consulting Practice Leader

Education: BS from Morgan State University

Certifications: Certified Public Accountant (CPA)

Certified Information Systems Auditor (CISA)

Certified Anti-Money Laundering Specialist (CAMS)

Career Overview:

Rick Williams is an IT Risk Consulting Practice Leader for SB & Company, LLC (SBC) with over 25 years of experience. Before joining SBC, Rick spent time with CitiGroup, Incorporated as a Senior Reviewer and Program Director where he gained experience working with advanced hardware, software and networks including implementation of enterprise messaging.