Internal Audit Department
NeighborWorks® America

Audit Review of

Cloud Service Provider Agreements

Project Number: NW.OGC.CLDAGRMNTS.2019

Audit Review of Cloud Service Provider Agreements

Table of Contents

April 9, 2019

To: NeighborWorks America Audit Committee

Subject: **Audit Review of Cloud Service Provider Agreements**

Attached is our draft audit report for the **Cloud Service Provider Agreements** review. Please contact me with any questions you might have.

Thank you.

Frederick Udochi
Chief Audit Executive

Attachment

cc: M. Rodriguez
S. Rice
R. Bond
R. Simmons

Function Responsibility and Internal Control Assessment
Audit Review of Cloud Service Provider Agreements

Business Function Responsibility	Report Date	Period Covered
Information Technology & Services	April 9, 2019	October 1, 2016 to December 31, 2018
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.

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 **Inconsistency in the Number of Cloud Service Providers/Subscriptions in Corporate Inventory Documents** The three (3) Inventory documents[2] provided to Internal Audit by IT&S, Administrative Services and Finance, report different number of Cloud Service Providers as well as different number of Cloud Service subscriptions that were signed and executed due to A. IT&S was not consistently looped in for hardware/software purchase made by Program Office; B. Lack of Office of General Counsel (OGC) Contract Review; and	**Yes**	**Recommendation 1** Internal Audit recommends the following: A. Implementation of a formal messaging to all staff to reemphasize the significance of including IT&S when acquiring software and/or hardware for their Program Office, regardless of the dollar amount and particularly for Cloud service subscriptions. Marking the IT RELATED checkbox when a PO is created/maintained by PO Managers in NetSuite should be a mandatory fill before the PO can be processed;	**Yes**	A: IT&S is creating a formal message to staff regarding purchasing technology related services / hardware using the pcard. B: addendum to security protocol. Identify vendors, scope of services, (Jason to send taxomony/language for review). Meet with Procurement, IT&S to ensure all parties agree. Use OGC portal to track concurrence on part of all parties.	A: 12/31/19 B: 03/31/20	Internal Audit accepts Management's response

[2] The three inventory documents reviewed: 1. ITVendorRiskManagementTrackingSheet.xslx provided by IT&S, 2. NWA BCP Application Matrix.xlsx provided by Administrative Service and 3. SoftwareLicenseCloudBasedResults564.xls provided by Finance.

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
C. Inability to identify/report on vendors who are Cloud Service Providers. **Risk Rating**: (b) (5)		B. OGC to take into consideration a joint effort with IT&S and Procurement, in addition to the contract template, to provide a baseline disclosure template to establish standards and conformity in the areas of Cloud service taxonomy and terminology, benchmarked against best practices. C. Corporation undertakes an effort led by IT&S, in conjunction with Finance and Procurement, to standardize the terminology used to describe Cloud Service Agreements and Subscribers in order to report and classify these transactions in a consistent manner.		B: IT&S will provide OGC with taxonomy / terminology advice. OGC will create an addendum to the existing security protocol regarding standards and best practices. Will use OGC portal to track concurrence on part of all parties. C: OGC will consult with Finance to determine if NetSuite can be modified to track Cloud Service Provider type (IaaS, PaaS, etc.). If not, will rely on Inventory Mgmt system being set up by IT&S. Will target top 10 - 15 Cloud Service Providers who manage high risk assets or highly sensitive data	C: 03/31/2020	

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 2 **Lack of Central Repository for the Storage of Cloud Service Agreements and Supporting Documents** Internal Audit observed that currently, there is no central repository to store the signed/executed contracts/CSAs and Cloud service subscriptions, regardless of dollar amount. **Risk Rating**: (b) (5)	**Yes**	**Recommendation 2** Until a long term, permanent solution can be rendered, Internal Audit recommends OGC, IT&S and Finance take into consideration the following suggestions as an interim workaround to consolidate Cloud Service Agreements and all supporting documents to a central location to achieve the integrity of the organization's Cloud base agreements and service subscriptions: - NEST - Create specific folder on Shared Drive (Network Drive P:\SHARED.DIR) - Create specific Contract Library using SharePoint	**Yes**	OGC, IT&S & Procurement believe NEST system should be used as master repository for Cloud Service agreements and supporting documents.	12/31/2019	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 Responses to The Audit Review of: Cloud Service Provider Agreements		
# Of Responses	**Response**	**Recommendation #**
4 (3 responses to Recommendation 1)	Agreement with the recommendation(s)	2
	Disagreement with the recommendation(s)	

Background

NeighborWorks America (NWA) has currently been in the process of shifting from on-site applications to off-site (hosted cloud-based) systems under the software licensing and delivery models of Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) (see Appendix A). These various cloud delivery service models come with service agreements which we refer to as Cloud Service Provider Agreements subsequently referred to as Cloud Service Agreements (CSA's). The CSAs should contain governing agreements between the cloud customer and the cloud provider. This is still a developing arena (cloud provider agreements) however there are industry best practices and standards that have begun to emerge and at the very least there should exist (a) A customer agreement (b) Acceptable Use Policy agreement and (c) Service Level Agreement. In addition, though centrally hosted, NWA 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.

Objective

The objective of this review was to obtain reasonable assurance that the development and evaluation process and procedures for CSAs meet critical program objectives. In addition, to also obtain assurance that the recommendation implementation effort remains aligned with Recommendation 4 from the WeConnect Cloud Application Security audit review[3].

Scope

The scope of this review includes all NWA's Cloud service subscriptions, signed and executed regardless of dollar amount, in the form of:

- Service Contract
- Service Agreement
- Monthly Subscription
- Pay-as-You-Go
- Pay per Use

Methodology

We reviewed three (3) inventory documents authored by IT&S, Administrative Services and Finance respectively against a fourth document compiled by internal audit. Upon reviewing these documents, Internal Audit noticed the discrepancies among the number of Cloud Service Providers and Cloud Service subscribers identified in each document (see Appendix B).

Review and testing were performed to determine the execution of CSA's adhered NWA policies and procedures:

[3] WeConnect Cloud Application Security review was conducted in the FY17 Audit Plan. This audit review concluded with five (5) observations with observation 4 to specifically address Cloud Service Provider Agreements.

1. The Office of General Council (OGC) Contract Review Process was followed to obtain email approval via the OGC Contract Review Portal.
2. A Current Service Organization Control (SOC) Report is provided in either:
   - SOC 1 Type 1, or
   - SOC 1 Type 2, or
   - SOC 2 Type 1, or
   - SOC 2 Type 2
3. IT&S notification of technology assets and services was obtained
4. Information Security Addendum was included in the final contract

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

Observations and Recommendations

Observation 1 Inconsistency in the Number of Cloud Service Subscriptions in Corporate Inventory Documents

We reviewed three (3) inventory documents authored by IT&S, Administrative Services and Finance respectively against a fourth document compiled by Internal audit. Upon reviewing these documents, Internal Audit noticed discrepancies between the number of Cloud Service Providers and Subscribers identified in each document.

We determined the cause of this inconsistency to three areas:

A. IT&S was not consistently looped in for hardware/software purchase made by Program Office. According to section 7.5 of the IT Asset Policy for the Purchase of Hardware and Software in the Corporate Administrative Manual:

"*Business units shall engage IT&S on all technology-related matters pertaining to their selection and purchase. Business units shall obtain the appropriate business unit management approvals and provide a business justification for requests before engaging IT&S.*
All technology selection and purchase decisions should be routed through the IT&S service desk. Peripheral equipment, such as individual printers, may be provided by IT&S to employees, upon submission of business justification and approval from the requestor's senior vice president or vice president."

Regardless of dollar amount, all software/hardware purchases are expected to comply with the corporate policy. In addition, a checkbox labeled IT RELATED was also added to the Purchase Order (PO) screen in NetSuite to further enforce this corporate policy. This checkbox in some instances is not utilized by the user when a PO for IT related hardware/software purchase is being created/maintained.

B. Lack of Office of General Counsel (OGC) Contract Review.

We grouped our sample population of agreements into WeConnect Suite and Others. Of the nine (9) WeConnect Suite contracts reviewed by Internal Audit, the OGC review and approval is 100%. As for Others, eighteen (18) out of thirty-seven (37), i.e. 47% of the agreements reviewed, we determined did not go through OGC Contract Review, or OGC Approval email was unobtainable (see Appendix C).

When a vendor contract/agreement was not created using the generally provided NeighborWorks OGC template, the final draft must go through the OGC Contract Review process for approval prior to contract signing and execution. Without clearing the content through OGC, misunderstanding of service terms and conditions may potentially result.

C. Inability to identify/report on vendors who are Cloud Service Providers.

Internal Audit observed that neither NetSuite nor NEST could produce a vendor listing by the category of Cloud Service Providers. Coding or naming taxonomy referencing CSA's or the various types was not in existence. This limitation further hampers the Corporation's capability to accurately identify the Cloud services agreements and subscriptions with consistency.

These three factors combined causing the inaccurate reporting and classification of agreements and subscriptions resulting in the Corporation not having an accurate count of cloud related IT assets for enterprise risk management and cyber security management.

Recommendation 1

Internal Audit recommends the following based on the observations noted earlier:

A. Implementation of a formal messaging to all staff to reemphasize the significance of including IT&S when acquiring software and/or hardware for their Program Office, regardless of the dollar amount and particularly for Cloud service subscriptions. Marking of the IT RELATED checkbox when a PO is created/maintained by PO Managers in NetSuite should be a mandatory fill before the PO can be processed.

   Internal Audit had made a similar recommendation in the WeConnect Cloud Application Security review. Referencing management response part 3 to Recommendation 4 Cloud Service Provider Agreements in audit report titled WeConnect Cloud Application Security: "*Finance and Administration Division (specifically Information Technology & Services and 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.*", a formal policy had been put in place since August 2018.

B. On the same note, Internal Audit also recommends that OGC takes into consideration a joint effort with IT&S and Procurement, in addition to the contract template, to provide a baseline disclosure template to establish standards and conformity in the areas of Cloud service taxonomy and terminology, benchmarked against best practices.

C. Internal Audit recommends that the Corporation undertakes an effort led by IT&S, in conjunction with Finance and Procurement, to standardize the terminology used to describe Cloud Service Agreements and Subscribers in order to report and classify these transactions in a consistent manner. This would greatly help in mitigating the risk of incorrect counts and misclassification of Cloud Based IT Assets.

Observation 2 Lack of Central Repository for the Storage of Cloud Service Agreements and Supporting Documents

Internal Audit observed that currently, there is no central repository to store the signed/executed contracts/CSAs and Cloud service subscriptions, regardless of dollar amount. Most CSAs under $3,500.00 are managed by individual Program Office through various payment method such as Pay-as-You-Go, Pay per Use, Monthly Subscription, etc.. When inquired on how the decision on payment method was rendered, it was observed that these were legacy contracts. SOC Reports, are currently kept at a separate location on Inside NeighborWorks with secured access granted by IT&S only

The current environment of not having all such agreements and supporting documents (see Appendix D) as well as business information in a central location makes it difficult to obtain an accurate count of IT assets at any given period, obtain an understanding of the nature of the IT assets in terms of assessing cyber security and enterprise risk management effectiveness including the potential loss in cost benefits.

Recommendation 2

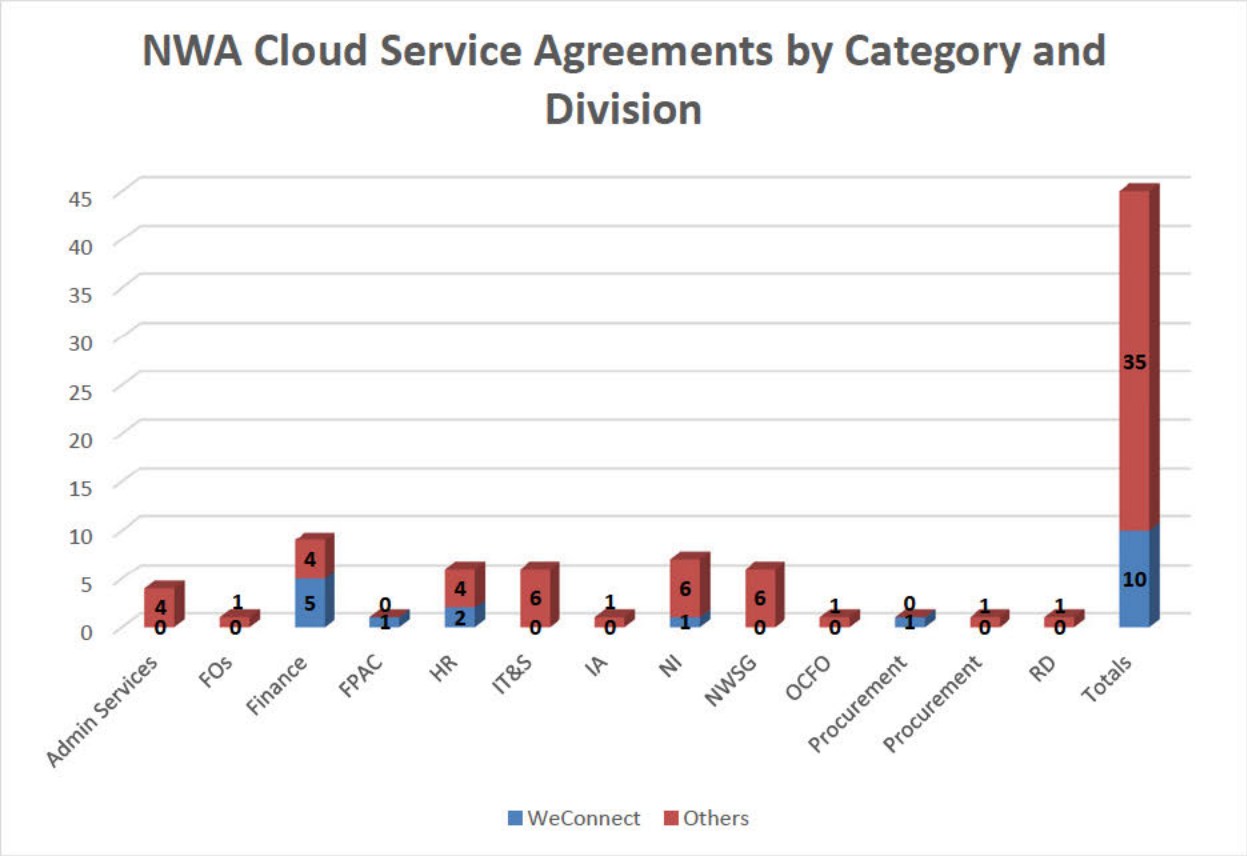
Until a long term, permanent solution can be rendered, Internal Audit recommends OGC, IT&S and Finance take into consideration the following suggestions as an interim workaround to consolidate Cloud Service Agreements and all supporting documents to a central location to achieve the integrity of the organization's Cloud base agreements and service subscriptions:

i. NEST
ii. Create specific folder on Shared Drive (Network Drive P:\SHARED.DIR)
iii. Create specific Contract Library using SharePoint

Conclusion

Despite the fast-growing Cloud service delivery models offered by vendors, ambiguity of service taxonomy and terminology usage can lead to incorrect counts, misclassification or no classifications. It is pertinent that a set of standards and guidelines to baseline Cloud service agreements and subscriptions be established internally, according to NWA's business needs, in a timely manner. Cloud Based services is still evolving in the industry, nonetheless, effective management of the CSA's would still require the basics of management controls for efficiency such as consistent use of terminology and description of IT assets for proper classification and the use of a centralized space for the easy access of all Corporate agreements.

Appendix A Cloud Service Agreements by Category and Division



Appendix B NWA Cloud Service Subscriptions Inventory

Document Title	Document Owner	Version/Last Modified	# of SaaS/ CSAs	# of CSPs
1 ITVendorRiskManagementTrackingSheet.xslx	IT&S	10/26/2018	37	42
2 NWA BCP Application Matrix ITS 2.22.2018 WB 20180907.xlsx	AS	09/07/2018	19	19
3 NetSuite Report: Software Licenses – Cloud Based 2018.xslx*	Finance	12/07/2018	18	18
**Selection criteria: Item = software license.*				

Appendix C OGC Contract Review Portal Utilization Analysis

DIVISION	# OF CSAs	REVIEWED/APPROVED by OGC	UTILIZATION %
Admin Services	4	3	75%
Field Operations	1	0	0%
Finance	9	5	56%
Financial Planning Analysis & Contracts	1	1	100%
Human Resources	6	5	83%
IT&S	6	3	50%
Internal Audit	1	1	100%
National Initiatives	7	4	57%
NWSG	6	3	50%
OCFO	1	1	100%
Procurement	1	1	100%
Public Relations	1	0	0%
Resource Development	1	0	0%
13 Divisions	**45**	**27**	**60%**

Appendix D NWA CSA Documents Repository Analysis

Division	# of Known Cloud Based Systems			# of Known CSPs			# of Known Executed CSAs			Repository of CSA and Documents	
	WC	Others	Total	WC	Others	Total	WC	Others	Total	NEST	Program Office
Admin Services		4	4		4	4		4	4	3	1
Field Operations		1	1		1	1		1	1	1	
Finance	5	4	9	5	4	9	5	4	9	5	4
Financial Planning Analysis & Contracts	1		1	1		1	1		1	1	
Human Resources	2	4	6	2	4	6	2	4	6	5	1
Information Technology & Services		6	6		6	6		6	6	5	1
Internal Audit		1	1		1	1		1	1	1	
National Initiatives	1	6	7	1	6	7	1	6	7	4	2
NeighborWorks Services Group		5	5		6	6		6	6	4	2*
OCFO		1	1		1	1		1	1		1
Procurement	1		1	1		1	1		1	1	
Public Relations		1	1		1	1		1	1		1**
Resource Development		1	1		1	1		1	1		1
Totals:	**10**	**36**	**46**	**10**	**36**	**46**	**10**	**34**	**45**	**30**	**14**

**Gorges hosting agreement (sole source) to be added to NEST as per Robyn German's email dated 11/26/2018.*

***Online subscription to Benchmark Email paid by PCard (e.g. Pay-per-Use).*