Internal Audit Department
NeighborWorks® America

Audit Review of

Information Technology
&
Services

Governance

Project Number: NWA.ITS.ITGOV.2016

Audit Review of Information Technology And Services Governance

Table of Contents

February 29, 2016

To: NeighborWorks America Audit Committee

Subject: **Audit Review of Information Technology and Services (Governance)**

Please find enclosed our draft audit report for the Information Technology and Services (Governance) review. Please contact me with any questions you might have.

Thank you.

Frederick Udochi
Chief Audit Executive

Attachment

cc: P. Weech
T. Chabolla
J. Bryson
L. Williams
D. Konda

Function Responsibility and Internal Control Assessment
Audit Review of Information Technology & Services (Governance)

Business Function Responsibility	Report Date	Period Covered
Information Technology And Services	February 29, 2016	October 1, 2015 Through January 31, 2016
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 Effective**

This report was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing.*

[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 – IT&S Governance Policies are not formally issued in the Administrative Manual NWA Management approved the official policies covering ***Information Security*** and ***Acceptable Usage*** in November, 2015 for the Information Technology and Services (IT&S) process. IT&S Management anticipates that two (2) other polices [***IT Governance*** and ***IT Asset Management***] currently in their draft and review stage will be approved by NWA Management during FY2016. The formal issuance of governing policies in the Administrative Manual is necessary to manage any process. **Risk Rating**: (b) (6)	**Yes**	**Recommendation 1 – Complete the formal issuance of IT&S draft Governance Policies in the Administrative Manual** Internal Audit recommends that IT&S Management strives to have these two draft policies approved and distributed by NWA Management in the Administrative Manual by the end of FY2016.	**Yes**	IT&S has received approval for the following policies covering – Information Security, Acceptable Usage, IT Asset Management, and IT Governance. Formal issuance of these policies will be via the updated NW Administrative Manual.	Q3 FY2016	IA 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
Observation 2 – An Incident Response Plan / Policy, Procedures, and Training is not formalized IT&S Management advised that work is being conducted on a draft Computer Security Incident Response Team (CSIRT) Plan as required under the issued ***Information Security Policy***. This plan references continuity of operations while minimizing any impact to NWA. The Office of General Counsel is currently leading this effort and is working closely with the IT&S Division. Further, IT&S is currently working with Human Resources to incorporate incident identification and reporting into the updated computer based training provided to NWA staff. Management expects the formal adoption and staff training by the end of FY 2016. **Risk Rating:** (b) (6)	**Yes**	**Recommendation 2 – Formally adopt an Incident Response Plan / Policy, Procedures, and Training** An Incident Response Plan performs an important step in the ***Information Security Policy***. Internal Audit recommends that IT&S Management strive to have the Incident Response Plan's adoption and appropriate staff training completed as planned by the end of FY 2016.	**Yes**	IT&S and OGC are working closely to update and finalize procedures for handling information privacy related incidents. Computer based training modules focused on Information Privacy and Security were reviewed during Q2 FY016. IT&S is working with Human Resources to incorporate these modules into staff training plans.	Q4 FY2016	IA 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
Observation 3 – IT&S' Operational Performance Metrics Internal Audit identified internally developed IT&S performance metrics [Scorecard / Benchmarks] for Project Management metrics, Helpdesk ticket performance, and overall comparative financial budget performance for the division on a quarterly basis. However, other IT&S processes existing within the governance framework also require monitoring metrics. For example, a performance metric to measure and track the turnaround time for the pre-testing and implementation of critical application patches (within 30 days) would be a Key Performance Indicator. The **3M** principle is applicable – *Measure-to-Monitor–to-Manage*. **Risk Rating:** (b) (6)	**Yes**	**Recommendation 3 – Develop additional Operational Performance Metrics** Internal Audit recommends the development of additional internal IT&S performance metrics [Scorecard / Dashboard] that allows management to evaluate the efficiency and effectiveness of the IT&S processes. This can help to exhibit its value to the organization and help to reduce potential service complaints. A governance framework will help to develop system wide Key Goal Indicators (KGIs) that are measured using Key Performance Indicators (KPIs)	**Yes**	IT&S has recently implemented an IT Service Management (ITSM) tool. This tool will be used in order to gather operational performance metrics as it pertains to service requests. The data gathered over the next quarter will be used to create a baseline.	Q4 FY2016	IA 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
Observation 4 – Personally Identifiable Information (PII) and compliance with Payment Card Information (PCI) under Data Security Standard (DSS) V3 Internal Audit was informed by IT&S management that the plan to implement recommendations based on the findings of the Protiviti 2014 Risk Assessment on PII and PCI have been significantly addressed in multiple areas. Management is continuously evaluating and mitigating where possible the other findings identified in this Risk Assessment report. However, Management is aware that (b) (4), a software platform that maintains certain PII and PCI information has (b) (4) improvement limitations which (b) (4) the PII and PCI standards. **Risk Rating:** (b) (6)	**Yes**	**Recommendation 4 – Formulate a plan to address PII and PCI compliance under Data Security Standard (DSS) V3** Internal Audit strongly recommends that NWA management in coordination with IT&S management consider the possible (b) (4) the credit card payments used by different training programs. The potential high risk of a data breach and the related aftermath of costs, fines, and reporting requirements should be balanced against the (b) (4). This recommendation is consistent with Strategic Recommendation 2 provided by Protiviti in their 2014 report.	**Yes**	Currently there are two major project initiatives underway to replace (b) (4) NWA management will reassess the risk pertaining to PII/PCI related data to determine if any cost-effective interim security enhancements are feasible at the end of Solution Design phase of each of these project initiatives. Otherwise, a comprehensive set of solutions will be provided to address these issues when these long-term project initiatives are successfully completed.	Q4 FY2017	IA 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
Observation 5 – Inactive User Accounts remain on Active Directory (AD) Internal Audit noted that a terminated employee's User Account access is removed by IT&S based on notifications from either Human Resources or the employee's department supervisor. For contractors or temporary employees, their user accounts are deactivated based on IT&S original input of an expiration date. User Accounts that remain inactive but available for re-activation present a security vulnerability if not removed from the list of User Accounts Active Directory (AD) (see testing in **Appendix C**). **Risk Rating:** (b) (6)	**Yes**	**Recommendation 5 – Implement a review for the removal of inactive User Accounts** Internal Audit recommends that preferably, a monthly review is performed on User Accounts to identify inactive User Accounts for removal from AD. The frequency of reviews should not exceed any three-month period.	**Yes**	IT&S agrees with internal audits recommendation. User accounts reviews will take place at least quarterly. Review will take into consideration any outstanding FOIA requests, record retention requirements and associated impact.	Q4 FY2016	IA 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
Observation 6 – A need to formally adopt periodic Risk Assessments Internal Audit noted that management utilized an external vendor (Protiviti) in 2014 to perform an IT risk assessment. Further, Protiviti in their Finding # 3.13.2 (page 63) noted that NWA had not performed an annual risk assessment in the past and recommended that an assessment be conducted annually. Using the 2014 Protiviti report, IT&S management has addressed and continues to resolve the gaps noted by the report. Going forward, the industry standard within a governance framework (e.g. COBIT or COSO) strongly recommends that a documented annual IT risk assessment be undertaken in order to identify any new or changing risks. In this manner they can be evaluated and addressed for timely mitigation. **Risk Rating:** (b) (6)	**Yes**	**Recommendation 6 – Increase the frequency of IT&S Risk Assessments** Internal Audit recommends that the IT&S Division perform periodic documented IT risk assessments. The frequency of these documented periodic IT risk assessments can consist of a combination of some years when it is performed solely in-house as self-assessments and other years by an outside vendor who can provide valuable insight to current developments and trends in this ever changing environment.	**Yes**	IT&S agrees that formal risk assessments should take place at least annually. The recommendations provided by the external risk assessment were acknowledged. The recommendations provided guidance for strategic investments and major initiatives during FY2015 into FY2016. A significant number of administrative (i.e. – policies, procedure development), physical (i.e. – cameras installation) and technical (i.e. – hard disk encryption, vulnerability scanning tools) controls have been established to address the gaps identified. IT&S is in the process of a network redesign and	Q4 FY2016	IA 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
				cloud migration. Any risks associated with these initiatives are being evaluated internally by key stakeholders prior to execution. In addition, IT&S is planning to engage with an external / independent assessor to conduct an IT Risk assessment in [redacted].		

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: Information Technology and Services (Governance)		
# Of Responses	**Response**	**Recommendation #**
6	Agreement with the recommendation(s)	1,2,3,4,5,6
	Disagreement with the recommendation(s)	

Background

Information Technology and Services (IT&S) governance defines the policies and procedures under which the IT&S division functions, and works to ensure compliance with these policies and procedures. This helps to specify the roles and responsibilities of the three major groups serviced by IT – its customers, stakeholders, and regulators. Appropriate governance will provide the leadership, organizational structures and processes that sustains and extends the organization's strategies. Also, following such a structured approach, it will provide IT with the means and the ability to monitor its performance. The IT governance goal can be summarized as follows:

- To assure that there is business value derived from IT investments.

- To mitigate potential risks that are associated with IT. To do this, management is obligated to implement a governance framework that addresses an organizational structure, its functional roles for both the technical and business processes, and their associated applications within the IT infrastructure.

To achieve these objectives, IT should utilize a specific governance framework to follow such as COBIT 5 (Control Objectives for Information and related Technology), the International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) 2700 series, or Information Technology Infrastructure Library (ITIL). Within such a governance framework, or an appropriate hybrid framework, management is able to identify its current status and work on areas for improvement over a period of phased-in implementation.

Objective

Internal Audit conducted this review with the following specific objectives:

- Obtain a high-level understanding of policies and procedures in place to administer and monitor IT&S Governance processes
- Obtain assurance that the processes to administer IT&S Governance are incorporating the five (5) elements of IT&S Governance from the Capability Maturity Model (CMM) in **Appendix B**:
    - Strategic Alignment
    - Delivery of Value
    - Risk Management
    - Resource Management
    - Performance Measurement

- Obtain assurance that the process steps as designed and implemented through the current policies and procedures align to the five elements for IT&S Governance.

In order to achieve these objectives, the review of IT&S Governance evaluated the current overall governance framework by determining the current status level within specific IT&S governance areas.

Scope

To evaluate IT&S governance, Internal Audit engaged IT&S management in a review of the current status of their many processes including policies implemented, or policies in the process of being implemented during the period October 1, 2015 through January 31, 2016. These policies, processes, and related procedures were evaluated and classified within the five (5) governance components.

Methodology

Internal Audit began this review with an Introductory Meeting which was held on December 10, 2015. The objective was to identify the significant stakeholders within the IT&S process and provide general information on the scope of the audit review. This was followed up with a self-assessment questionnaire to management. Based on the responses, management was further interviewed and provided with additional follow-up questions regarding any observations. Also, management provided documentation in support of the process areas being evaluated in order to support the current status of functional achievement.

For example, management identified the status of new IT&S policies approved by senior management and any that were in a draft stage. IT&S management also identified collaboration efforts with other divisions [such as The Office of General Counsel and Human Resources] to formalize the procedures and the training for staff required for responding to IT security incidents. Internal Audit, in addition, reviewed the Protiviti 2014 Risk Assessment that focused on the level of compliance by NeighborWorks America for securing Personally Identifiable Information (PII) and its compliance with Payment Card Information (PCI) under Data Security Standard (DSS) V3 (see **Appendix A**).

Using the information provided and incorporating IT&S management's internal self-evaluation, Internal Audit identified the progress and current status of achievement for IT&S within the five (5) components of a Capability Maturity Model (CMM) in **Appendix B**. Though the goal is to seek the achievement of the "Optimized" level for the five (5) components, it is also accepted that changes in the IT environment can re-set current status levels. Also, the top level may be cost prohibitive to the organization. However, it provides management with a benchmark tool to measure current IT&S governance activity when compared to a best practices standard. Below are the observations and recommendations that resulted from the audit review of IT&S Governance.

Observations and Recommendations

Observation 1 – IT&S Governance Policies are not formally issued in the Administrative Manual

NWA Management approved the official policies covering ***Information Security*** and ***Acceptable Usage*** in November, 2015 for the Information Technology and Services (IT&S) process. IT&S

management anticipates that two (2) other polices [*IT Governance* and *IT Asset Management*] currently in their draft and review stage will be approved by NWA Management during FY2016. The formal issuance of governing policies is necessary to manage any process.

Recommendation 1 – Complete the formal issuance of IT&S Governance Policies in the Administrative Manual

Internal Audit recommends that IT&S Management strives to have these two draft policies approved and distributed with other previously approved policies in the Administrative Manual by the end of FY2016.

Observation 2 – An Incident Response Plan / Policy, Procedures, and Training is not formalized

IT&S Management advised that work is being conducted on a draft Computer Security Incident Response Team (CSIRT) Plan as required under the issued ***Information Security Policy***. This plan references continuity of operations while minimizing any impact to NWA. The Office of General Counsel is currently leading this effort and is working closely with the IT&S Division. Further, IT&S is currently working with Human Resources to incorporate incident identification and reporting into the updated computer based training provided to NWA staff. Management expects the formal adoption and staff training by the end of FY 2016.

Recommendation 2 – Formally adopt an Incident Response Plan / Policy, Procedures, and Training

An Incident Response Plan performs an important step in the ***Information Security Policy.*** Internal Audit recommends that IT&S Management strive to have the Incident Response Plan's adoption and appropriate staff training completed as planned by the end of FY 2016.

Observation 3 – IT&S' Operational Performance Metrics

Internal Audit identified internally developed IT&S performance metrics [Scorecard / Benchmarks] for Project Management metrics, Helpdesk ticket performance, and overall comparative financial budget performance for the division on a quarterly basis. However, there are numerous other IT&S processes existing within the governance framework. IT&S should identify key performance indicators which are drivers to critical IT&S activities such as a performance metric to measure and track the turnaround time for the pre-testing and implementation of critical application patches (within 30 days).These process metrics will provide significant monitoring help to better manage the deployment of resources. The **3M** principle is applicable – *Measure-to-Monitor–to-Manage*.

Recommendation 3 – Develop additional Operational Performance Metrics

Internal Audit recommends the development of additional internal IT&S performance metrics [Scorecard / Dashboard] that allows management to evaluate the efficiency and effectiveness of the IT&S processes. IT&S Management recognizes the need to have its performance be evaluated on a periodic basis in specific areas. This can help to exhibit its value to the organization and help to reduce potential service complaints. A governance framework will help to develop system wide Key Goal Indicators (KGIs) that are measured using Key Performance Indicators (KPIs)

Observation 4 – Personally Identifiable Information (PII) and compliance with Payment Card Information (PCI) under Data Security Standard (DSS) V3

NeighborWorks America through the IT&S Division contracted with Protiviti [a global risk and consulting firm] to undertake an IT Risk Assessment with an emphasis,

> "…to assess any gaps it had in its collection, authorized use, access, security and destruction of Personally Identifiable Information (PII) and its compliance with the Payment Card Information (PCI) Data Security Standard (DSS) V3. This assessment was conducted by Protiviti Security & Privacy Services in Aug and Sept. 2014."[1]

Internal Audit while reviewing the Protiviti 2014 risk assessment report was informed by IT&S management that the plan to implement the report's recommendations with respect to PII and PCI data from external customers have been significantly addressed in multiple areas. In the interim, Management is continuously evaluating and mitigating, where possible, the findings identified in this risk assessment report. Management is aware that one software platform maintaining PII and PCI data, ((b) (4)), has (b) (4) improvement limitations which (b) (4) with the PII and PCI standards. As a result, these fixes are short-term solutions which are being implemented with a future goal to devise a permanent long-term solution.

Recommendation 4 – Formulate a plan to address PII and PCI compliance under Data Security Standard (DSS) V3

Internal Audit strongly recommends that NWA management in coordination with IT&S management consider the possible (b) (4) the credit card payments used by different training programs. The potential high risk of a data breach and the related aftermath of costs, fines, and reporting requirements should be balanced against the (b) (4) . This recommendation is consistent with Strategic Recommendation 2 provided by Protiviti in their 2014 report.

Observation 5 – Inactive User Accounts remain on Active Directory (AD)

IT&S stated that a terminating employee's User Account access is removed by IT&S based on notifications from either Human Resources or the employee's department supervisor. For contractors or temporary employees, their user accounts are deactivated based on IT&S' o input of an expiration date at the time of user account's creation. Based on testing performed on twenty-six (26) user accounts, Internal Audit noted that at least four (4) User Accounts were "expired" but not "disabled" in AD. Also, for a fifth User Account that was "disabled" on 11/23/2015, it appears that a subsequent "Logon Time" occurred on 1/.6/2016. User Accounts that remain inactive but available for re-activation present a security vulnerability if not removed from the list of User Accounts in Active Directory (AD). See **Appendix C.**

[1] Protiviti, (b) (4) .

Recommendation 5 – Implement a review for the removal of inactive User Accounts

Internal Audit recommends that preferably, a monthly review is performed on User Accounts to identify inactive User Accounts for removal from AD. The frequency of reviews should not exceed any three-month period.

Observation 6 – A need to formally adopt periodic Risk Assessments

Internal Audit noted that management utilized an external vendor (Protiviti) in 2014 to perform an IT risk assessment (see Footnote 1). Further, Protiviti in their Finding # 3.13.2 (report's page 63) noted that NWA had not performed an annual risk assessment in the past and recommended that an assessment be conducted annually. Using the 2014 Protiviti report, IT&S management has addressed and continues to resolve the gaps noted by the report. Going forward, the industry standard within a governance framework (e.g. COBIT or COSO) strongly recommends that a documented annual IT risk assessment of any new and changing risks be evaluated and addressed for timely mitigation.

Recommendation 6 – Increase the frequency of IT&S Risk Assessments

Internal Audit recommends that the IT&S Division perform periodic documented IT risk assessments. The frequency of these documented periodic IT risk assessments can consist of a combination of some years when it is performed solely in-house as self-assessments and other years by an outside vendor who can provide valuable insight to current developments and trends in this ever changing technology environment.

Conclusion

Information Technology and Services (IT&S) governance should be an integral part of NeighborWorks America's (NWA) overall governance. Going forward, as IT&S Governance is enhanced and strengthened, management will need to evaluate their progression within a governance framework model. Internal Audit has provided management with a benchmarking tool using Capability Maturity Model (CMM). In this CMM the "present state" of IT&S' five (5) governance elements is identified by the highlighted cells in Appendix A. This model can be used to pursue improved performance, where warranted, in the five elements of IT governance.

Additionally, the audit review of IT&S Governance identified six (6) Observations and their related Recommendations that will work to assist the IT&S Division to mitigate certain risks while strengthening the strategic role and value derived from IT&S by NeighborWorks America. Our interactions with the IT&S team were meaningful and productive. Thanks again to the Senior Vice-President and the team for their cooperation and assistance during this review.

Appendix A: Definitions for Personally Identifiable Information and Payment Card Information

Personally Identifiable Information (PII)

The National Institutes of Standards and Technology (NIST), U.S. Department of Commerce in Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information* (April, 2010, page 7) defines PII as,

> "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." So, for example, a user's IP address is not classed as PII on its own, but is classified as linked PII.

Payment Card Information (PCI)

Wikipedia explains PCI in the following way,

> “The **Payment Card Industry Data Security Standard** (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB. Private label cards – those which aren't part of a major card scheme – are not included in the scope of the PCI DSS.
>
> The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud. Validation of compliance is performed annually, either by an external Qualified Security Assessor (QSA) that creates a Report on Compliance (ROC) for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes.”

APPENDIX B: Current IT&S Governance Status

The following table illustrates IT&S' current status within the five (5) governance elements of (i) strategic alignment, (ii) resource management, (iii) risk management, (iv) performance management, and (v) value delivery.

Current Status: Rust Cell	Strategic Alignment	Resource Management	Risk Management	Performance Management	Value Delivery
Optimized	IT is integral to business achieving strategic objectives. IT presents solutions to the business in a proactive manner.	Resources are deployed strategically considering internal and external models using defined evaluation criteria based on strategic objectives.	Risk management is a continuous process coordinated by the board and management. Organization risk tolerance is well known.	A balanced scorecard is utilized to monitor IT effectiveness. The scorecard is presented to the board and other key executives.	IT is viewed as a strategic partner of the business. Solutions are presented to the business, then delivered on time/budget/scope.
Managed	The board or executive management evaluates the business strategy to ensure alignment on a regular basis. Long term, tactical IT plans map to business strategy.	IT projects, purchasing processes, IT asset management processes, and resource management processes are integrated and measured for effectiveness.	Annual IT risk assessments are completed according to accepted methodologies. Preventative controls and monitoring mechanisms help to ensure that key risks are mitigated.	IT fully understands the operational levers that drive the business and these levers are measured, monitored, summarized and reported regularly to stakeholders.	IT is cost-effective in delivering high-quality services that meet the needs of the enterprise. Communication is frequent and structured. IT proactively seeks to enhance business value.
Defined	A formal process to evaluate and prioritize potential IT projects is defined; established criteria are consistently applied to facilitate cross-functional committee decisions.	Processes that integrate projects and maintenance activities are defined and deliver IT assets and resources when needed	Risks are known, prioritized and re-evaluated on a regular basis. Mitigation activities are defined for each risk and some monitoring structures are in operation.	Service levels with the business are defined and tracked. A process to monitor compliance with service level agreements (SLAs) is defined and results are communicated.	IT is viewed as an enabler of business processes and there are activities in place that confirm that business requirements are being met and budget goals are achieved.
Repeatable	IT maintains existing systems, but is viewed primarily as an order taker. Project decisions involve business personnel and require business case format	An organization-wide chart exists and is maintained. A list of applications and infrastructure assets can be generated, but may not be updated regularly	Risks have been identified and some mitigation activities are in place. IT knows how to respond when an incident occurs, but procedures are informal.	Some measurements are taken regularly and communicated consistently. There are gaps between what is measured and what matters to the business	The business views IT as a utility. There are consistent communications between the groups, but IT generally is contacted when there are issues.
Initial	IT projects and service may or may not align with business needs or objectives. Project decisions are made unilaterally or without established criteria	Reporting lines and skill sets are known by management, but are not inventoried or organized. IT asset management practices are informal	IT is unaware of the risks that are present across the company landscape. Risk assessment activities occur occasionally or in response to an incident	Some measurements are taken in a few areas of IT. They may be communicated by some means, but are not used to source issues or to proactively asses issues	Irregular or ineffective communications between IT and the business. Projects are often delayed, do not deliver expected scope, or are over budget

APPENDIX C: A Review of Selected User Accounts Current Access Status

The following table lists the User Accounts reviewed to assist in identifying Active, Expired /Inactive, and Disabled Accounts.

	Display Name	SAM Account Name	When Created	Last Logon Time	User Logon Count	Last Name	NWA Emp. ?	Term Date	Current Email Access	Network Access Made Inactive	Active Acct.	IT&S Responses
1	(b) (6)		2008-01-08 09:11:10	2016-01-06 14:00:03	6,867	(b) (6)	Yes	11/20/2015	No	11/23/2015	No	
2			2015-09-18 16:19:29	2016-01-06 15:51:17	339		No		Yes	No	Yes	This acct is still valid until 3/31/16
3			2015-09-25 09:12:19	2016-01-11 23:21:07	153		No		Yes	No	Yes	Acct expired but not disabled
4			2015-11-09 11:52:13	2016-01-13 10:22:23	60		No		No	No	Yes	Acct expired but not disabled
5			2016-01-12 16:43:02	2016-01-13 17:30:46	17		No		Yes	No	Yes	Acct disabled
6			2015-12-18 11:59:45	2016-01-14 17:35:07	36		No		No	No	Yes	Acct expired but not disabled
7			2015-12-15 12:08:19	2016-01-15 09:50:48	24		No		No	No	Yes	This acct is still valid until 2/25/16
8			2002-08-08 17:42:46	2016-01-15 21:44:02	8,838		Yes	1/15/2016	No	1/19/2016	No	
9			2015-04-09 10:19:11	2016-01-20 19:48:19	619		Yes	1/22/2016	No	2/4/2016	No	
10			2015-07-10 13:58:53	2015-12-03 14:42:22	160		No		No	12/3/2015	No	
11			2013-02-19 10:17:38	2015-12-04 09:12:11	61		No		No	No	Yes	Acct expired and disabled
12			2015-12-09 16:36:11	2015-12-16 14:31:43	5		No		No	12/23/2015	No	
13			2002-08-08 17:42:45	2015-12-16 18:10:57	7,479		Yes	12/25/2015	No	No	Yes	Acct expired and disabled
14			2015-12-17 15:59:44	2015-12-17 17:04:06	0		No		No	No	Yes	Acct expired but not disabled
15			2015-12-10 09:26:50	2015-12-21 10:03:50	10		No		No	12/22/2015	No	
16			2015-10-27 16:18:17	2015-12-21 14:55:31	70		No		No	No	Yes	Acct expired and disabled

	Display Name	SAM Account Name	When Created	Last Logon Time	User Logon Count	Last Name	NWA Emp. ?	Term Date	Current Email Access	Network Access Made Inactive	Active Acct.	IT&S Responses
17	(b) (6)		2005-07-28 13:02:19	2015-12-26 10:59:03	7,030	(b) (6)	Yes	1/3/2016	No	No	Yes	Acct expired and disabled and mailbox already hidden
18			2015-10-07 16:24:49	2015-12-30 22:50:52	152		No		No	No	Yes	Acct expired and disabled
19			2014-05-08 16:09:08	2015-12-31 11:24:12	2,471		Yes	12/312015	No	No	Yes	Acct disabled and mailbox already hidden
20			2015-11-23 09:52:09	2015-12-31 13:27:55	45		No		Yes	No	Yes	This acct is still valid until 2/23/16
21			2014-05-19 21:54:38	2015-12-31 23:59:59	6,720		No		No	No	Yes	Acct expired and disabled no mailbox
22			2011-02-01 11:27:16	2014-08-21 14:39:13	632		No		Yes	9/30/2014	No	Acct expired and disabled; mailbox not hidden
23			2008-02-25 09:37:24	2014-09-24 13:40:28	701		No		Yes	9/30/2014	No	Acct expired and disabled; mailbox not hidden
24			2015-03-23 12:36:13	2015-04-01 15:21:02	9		No		Yes	4/17/2015	No	Acct expired and disabled; mailbox not hidden
25			2015-03-20 16:30:37	2015-04-13 06:53:32	20		No		Yes	4/13/2015	No	Acct expired and disabled; mailbox hidden (but he had a temp acct first, and that one is disabled but mailbox not hidden)
26			2011-07-13 17:06:42	2015-08-04 10:09:41	3,912		Yes	8/4/2015	Yes	8/4/2015	No	Acct expired and disabled; mailbox is hidden

Report Created On:	**February 18, 2016**
User Log Provided By:	**IT&S**