Internal Audit Department
NeighborWorks® America

# Audit Review of

# Active Directory Management

Project Number: NW.ITS.IAM-ADM.2025

# Audit Review of Active Directory Management

## Table of Contents


Function Responsibility and Internal Control Assessment ..... 2

Executive Summary of Observations, Recommendations, and Management Responses ..... 3

Implementation Roadmap – High Risk Observations ..... 17

Risk Rating Legend ..... 18

Background ..... 19

Objective ..... 19

**Scope** ..... 19

Approach ..... 20

Detailed Observations and Recommendations ..... 21

Conclusion ..... 29

# Function Responsibility and Internal Control Assessment
# Audit Review of Active Directory Management

| Business Function Responsibility | Report Date | Period Covered |
|---|---|---|
| Active Directory Management | August 1, 2025 | Point in Time (Design) Q2 2025 |
| **Assessment of Internal Control Structure** | | |
| Effectiveness and Efficiency of Operations | | (b) (5) |
| Reliability of Financial Reporting | | **Not Applicable** |
| Compliance with Applicable Laws and Regulations | | **Not Applicable** |

This report was 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 and Timeline |
|---|---|---|---|---|---|---|
| **Observation 1**<br><br>There are (b) (4) [redacted]<br>These legacy systems are at an elevated risk of exploitable vulnerabilities.<br><br>**Risk Rating**: (b) (4) [redacted] | **Yes** | **Recommendation**<br><br>Update the Asset Management Policy to include statements for handling end-of-life and legacy systems. For all legacy systems, NeighborWorks should either decommission or isolate them from the environment. (b) (4) [redacted].<br><br>**Implementation Timeframe: 0-6 months** | **Yes** | The identified servers are (b) (4) [redacted] | Will work to secure funding if funded by FY27. | IAD accepts management response with an understanding of potential funding constraints; however, IAD is not aligned with an FY27 implementation date, as it is outside of the standard 12-month implementation timeframe |

| 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 and Timeline |
|---|---|---|---|---|---|---|
| **Observation 2**<br><br>Multiple Domain Controllers (b) (4) [redacted] to reduce the likelihood of compromise.<br><br>**Risk Rating:** (b) (4) [redacted] | **Yes** | **Recommendation**<br><br>(b) (4) [redacted].<br><br>**Implementation Timeframe: 0-3 months** | **No** | (b) (4) [redacted] For systems with Internet Explorer, the only option in this environment is to disable it locally or through Group Policy. | 0-3 months | IAD accepts management response and designates 12/30/25 as the estimated implementation date based on the timeline provided by management. |
| **Observation 3**<br><br>(b) (4) [redacted].<br><br>**Risk Rating:** (b) (4) [redacted] | **Yes** | **Recommendation**<br><br>(b) (4) [redacted] | **Yes** | The security team will identify the tools, applications, processes, and procedures required to implement application allowlists on Domain Controllers. | 0-3 months | IAD accepts management response and designates 12/30/25 as the estimated implementation date, based on the timeline provided by management. |

| 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 and Timeline |
|---|---|---|---|---|---|---|
| | | **Implementation Timeframe: 0-3 months** | | | | |
| **Observation 4**<br><br>(b) (4) [redacted] Implementing secure administrative hosts allows for greater control and security surrounding admin activities.<br><br>**Risk Rating:** (b) (4) [redacted] | **Yes** | **Recommendation**<br><br>(b) (4) [redacted]<br>Secure hosts must be actively monitored to ensure security of the administrative accounts.<br><br>Update the Privileged Access Management Policy to include requirements to use secure administrative hosts for all admin activities.<br><br>**Implementation Timeframe: 0-3 month** | **Yes** | We will implement Privileged Access Workstations (PAWs) or Secure Admin Workstations, which will be dedicated exclusively to performing sensitive administrative tasks. | 1-5 months | IAD accepts management response and designates 2/28/26 as the estimated implementation date, based on the timeline provided by management. |

| 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 and Timeline |
|---|---|---|---|---|---|---|
| **Observation 5**<br><br>(b) (4) [redacted]<br><br>**Risk Rating:** (b) (4) [redacted] | **Yes** | **Recommendation**<br><br>Enforce the current MFA policy for privileged access. Implement MFA for server log ins and update the current policy to include server log ins.<br><br>**Implementation Timeframe: 0-3 months** | **Yes** | Revised Management's Response to IA Recommendation: The security and infrastructure teams will collaborate to implement MFA on Domain Controllers. We will verify whether the organization's current MFA service is compatible with legacy Domain Controllers. If compatibility issues arise, we will utilize alternatives such as Secure Administrative Hosts (SAHs). | 0-6 months | IAD accepts management response and designates 3/30/26 as the estimated implementation date, based on the timeline provided by management. |
| **Observation 6**<br><br>(b) (4) [redacted] | **Yes** | **Recommendation**<br><br>(b) (4) [redacted] | **Yes** | (b) (4) [redacted] | Will work to secure funding if funded by FY27 | IAD accepts management response with an understanding of |

| 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 and Timeline |
|---|---|---|---|---|---|---|
| (b) (4)<br>**Risk Rating:** (b) (4) | | (b) (4)<br>**Implementation Timeframe: 0-3 months** | | (b) (4)<br>The Protected Users group is a feature requiring the domain function level to be elevated to 2012R2 or higher. (b) (4) | | potential funding constraints; however, IAD is not aligned with an FY27 implementation date, as it is outside of the standard 12-month implementation timeframe. |
| **Observation 7**<br>(b) (4)<br>**Risk Rating:** (b) (4) | **Yes** | **Recommendation**<br>(b) (4) | **Yes** | (b) (4) | Will work to secure funding. If funded by FY27 | IAD accepts management response with an understanding of potential funding constraints; however, IAD is not aligned with an FY27 implementation date, as it is outside of the standard 12-month |

| 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 and Timeline |
|---|---|---|---|---|---|---|
| | | **Implementation Timeframe: 0-3 months** | | | | implementation timeframe. |
| **Observation 8**<br><br>(b) (4) [redacted]<br><br>Having a high number of Enterprise Administrators and Domain Administrators does not follow least privileged principle.<br><br>**Risk Rating:** (b) (4) | **Yes** | **Recommendation**<br><br>Perform a user access review for all administrative accounts and remove all unnecessary privileges.<br><br>**Implementation Timeframe: 0-3 months** | **Yes** | We will conduct a user access review to identify each administrative account, its role, and its owner. Unnecessary and unused accounts will be removed to meet the least privileged requirements. | 3-9 months | IAD accepts management response and designates 06/30/26 as the estimated implementation timeframe, based on the timeline provided by management |
| **Observation 9**<br><br>While separate administrator accounts have been created for | **Yes** | **Recommendation**<br><br>Enforce the current policy and remove all privileged access | **Yes** | We will identify each non-designated administrator account, its role, | 0-3 months | IAD accepts management response and designates 12/30/25 as the |

| 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 and Timeline |
|---|---|---|---|---|---|---|
| users with elevated privileges, (b) (4) [redacted]<br><br>**Risk Rating:** (b) (4) | | from non-designated administrator accounts.<br><br>**Implementation Timeframe: 0-3 months** | | and its owner, and remove all privileged access from these accounts to enforce the current policy and meet the least privileged requirements. | | estimated implementation timeframe, based on the timeline provided by management. |
| **Observation 10**<br><br>While Privileged Access Management (PAM) has been enabled for NeighborWorks' M365 environment, (b) (4) [redacted]<br><br>**Risk Rating:** (b) (4) | **Yes** | **Recommendation**<br><br>Implement a Privileged Access Management solution to temporary grant access into privileged groups. PAM solution must capture logs for administrator activity.<br><br>**Implementation Timeframe: 0-12 months** | **Yes** | We will identify a Privileged Access Management (PAM) solution compatible with our legacy systems to temporarily grant access to privileged groups and capture logs for administrator activity. | If funding is available for the product and implementation, 9-12 Months | IAD accepts management response and designates 9/30/26 as the estimated implementation timeframe, based on the timeline provided by management. |

| 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 and Timeline |
|---|---|---|---|---|---|---|
| **Observation 11**<br><br>(b) (4) [redacted]<br><br>**Risk Rating:** (b) (4) | **Yes** | **Recommendation**<br><br>Enforce the current Information Security Policy and classify all assets based on importance to business operations and impact. All critical assets must be prioritized for security and monitoring.<br><br>**Implementation Timeframe: 0-12 months** | **Yes** | We will collaborate with each program and business owner to identify and classify all assets based on their importance to business operations and impact, prioritizing critical assets for enhanced security and monitoring. | 0-12 months | IAD accepts management response and designates 9/30/26 as the estimated implementation timeframe, based on the timeline provided by management. |
| **Observation 12**<br><br>NeighborWorks configuration management program is ad-hoc, - benchmarks (b) (4) [redacted] | **Yes** | **Recommendation**<br><br>Document a formal configuration management program that includes benchmarks, defined period of review, and procedures for | **Yes** | We will develop and implement a formal configuration management program that includes documented benchmarks, a defined review period, and | 6-12 months | IAD accepts management response and designates 9/30/26 as the estimated implementation timeframe, based on the timeline |

| 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 and Timeline |
|---|---|---|---|---|---|---|
| (b) (4)<br><br>**Risk Rating:** (b) (4) | | maintaining compliance.<br><br>**Implementation Timeframe: 0-3 months** | | procedures to ensure ongoing compliance. This will involve conducting configuration scans and benchmarking all servers in our environment. | | provided by management. |
| **Observation 13**<br><br>(b) (4)<br><br>**Risk Rating:** (b) (4) | **Yes** | **Recommendation**<br><br>Enforce the current Access Management Policy and perform quarterly access reviews to ensure all users' access is correct. (b) (4)<br><br>**Implementation Timeframe: 0-3 months** | **Yes** | We will enforce the Access Management Policy by conducting quarterly access reviews to verify user access and identify inactive accounts. (b) (4) | 0-6 months | IAD accepts management response and designates 3/30/26 as the estimated implementation date, based on the timeline provided by management. |

| 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 and Timeline |
|---|---|---|---|---|---|---|
| **Observation 14**<br><br>(b) (4)<br><br>Domain Administrators should not sign into member servers to minimize exposure if the member server becomes compromised.<br><br>**Risk Rating:** (b) (4) | **Yes** | **Recommendation**<br><br>(b) (4) | **Yes** | (b) (4) | 3-9 months | IAD accepts management response and designates 6/30/26 as the estimated implementation date, based on the timeline provided by management. |

| 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 and Timeline |
|---|---|---|---|---|---|---|
| | | groups on all member servers.<br><br>**Implementation Timeframe: 0-3 months** | | | | |
| **Observation 15**<br><br>The Managed Security Service Provider (Arctic Wolf) is set up to monitor all audit logs captured from Domain Controllers. (b) (4) [redacted]<br><br>**Risk Rating:** (b) (4) [redacted] | **Yes** | **Recommendation**<br><br>Enforce the current logging and monitoring policy within the Privileged Access Management Policy. (b) (4) [redacted].<br><br>**Implementation Timeframe: 0-3 months** | **Yes** | Enforcing the logging and monitoring policy within the Privileged Access Management Policy to include all compatible production server logs in the Arctic Wolf SIEM will require additional funding. We will evaluate the need for additional services to meet this requirement. | Will work to secure funding if funded by FY27. | IAD accepts management response with an understanding of potential funding constraints; however, IAD is not aligned with an FY27 implementation date, as it is outside of the standard 12-month implementation timeframe. |

| 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 and Timeline |
|---|---|---|---|---|---|---|
| **Observation 16**<br><br>During discussions with IT operations, a service account, (SVC-PDQ) was identified in the Domain Administrator group. (b) (4) [redacted]<br><br>**Risk Rating:** (b) (4) | **Yes** | **Recommendation**<br><br>Perform an access review for all service accounts to verify (b) (4) [redacted]<br><br>**Implementation Timeframe: 0-3 months** | **Yes** | We will conduct an access review for all service accounts, including SVC-PDQ, (b) (4) [redacted]. | 0-3 months | IAD accepts management response and designates 12/30/25 as the estimated implementation date, based on the timeline provided by management. |
| **Observation 17**<br><br>(b) (4) [redacted]<br><br>**Risk Rating:** (b) (4) | **Yes** | **Recommendation**<br><br>(b) (4) [redacted] | **Yes** | The current environment includes legacy operating systems, applications, and Domain Controllers that rely on (b) (4) [redacted] | Will work to secure funding if funded by FY27. | IAD accepts management response with an understanding of potential funding constraints; however, IAD is not aligned with an FY27 implementation date, as it is outside of the standard 12- |

| 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 and Timeline |
|---|---|---|---|---|---|---|
| | | **Implementation Timeframe: 0-3 months** | | (b) (4) Due to funding constraints, this process will be deferred until funding is available. | | month implementation timeframe. |
| **Observation 18** (b) (4) **Risk Rating:** (b) (4) | **No** | **Recommendation** (b) (4) **Implementation Timeframe: 0-6 months** | **Yes** | (b) (4) | 0-3 months | IAD acknowledges management's acceptance of the recommendation and designates 12/30/25 as the estimated implementation date, based on the timeline provided by management. |

| 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 and Timeline |
|---|---|---|---|---|---|---|
| | | | | (b) (4) | | |

## Implementation Roadmap – High Risk Observations

| # | Recommendation | Risk Rating | 0- 3 Months | 0-6 Months |
|---|---|---|---|---|
| 1 | (b) (4) | (b) (4) | | X |
| 2 | | | X | |
| 3 | | | X | |
| 4 | | | X | |
| 5 | | | X | |
| 6 | | | X | |
| 7 | | | X | |
| 8 | | | X | |
| 9 | | | X | |
| 10 | | | X | |

*These recommendations were also addressed in IAD's *Privileged/Non-Privileged Access Management Policies* audit report issued in FY24 (project # NW.ITS.IAM-PNP.2024).

## Risk Rating Legend

| Risk Level | Description |
|---|---|
| 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. |
| 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. |
| Low | A weakness identified which does not seriously detract from the system of internal control and or operational effectiveness/efficiency, integrity of reporting, but should nonetheless be addressed by management. |

| **Management Responses to the Audit Review of:**<br><br>**Active Directory Management** | | |
|---|---|---|
| **# Of Responses** | **Response** | **Recommendation #** |
| 18 | Agreement with the recommendation(s) | 18 |
| 0 | Disagreement with the recommendation(s) | 0 |

## Background

CohnReznick was engaged to conduct an internal audit of certain NeighborWorks internal controls within the area of Active Directory (AD) management. The scope and approach of the audit was determined based on their expertise, information provided to CohnReznick by NeighborWorks' management, and in collaboration with NeighborWorks Internal Audit Division.

## Objective

The objective of this audit is to assess the security of NeighborWorks Active Directory environment, specifically evaluating access controls, privilege management, and compliance with applicable regulatory requirements.

## Scope

The scope of this internal audit has been determined based on our expertise, information provided to CohnReznick by NeighborWorks' management, and in collaboration with NeighborWorks Internal Audit Division. This internal audit covers the following:

- Evaluation of the security and access controls implemented within the NeighborWorks primary Active Directory domain environment.
- Identification and assessment of risks related to privilege escalation and abuse.
- Assessment of the strength and enforcement of password policies and authentication mechanisms; and
- Evaluation of compliance with NIST Cybersecurity Framework (CSF) 2.0 as specified in:
    - Protect - Identity Management, Authentication and Access Control, Awareness and Training, and Technology Infrastructure Resilience
    - Detect – Continuous Monitoring
        - Control 11: Data Recovery
            a. Establish and Maintain a Data Recovery Process *(11.1)*
            b. Perform Automated Backups *(11.2)*
            c. Protect Recovery Data *(11.3)*
            d. Establish and Maintain an Isolated Instance of Recovery Data *(11.4)*

        - Control 17: Incident Response Management
            a. Designate Personnel to Manage Incident Handling *(17.1)*
            b. b. Establish and Maintain Contact Information for Reporting Security Incidents (17.2)
            c. c. Establish and Maintain an Enterprise Process for Reporting Incidents (17.3)
            d. d. Establish and Maintain an Incident Response Process (17.4)
            e. Assign Key Roles and Responsibilities (17.5)
            f. Define Mechanisms for Communicating During Incident Response *(17.6)*

## Approach

For this internal audit, CohnReznick:

- Developed an audit program approved by NeighborWorks Internal Audit Management.
- Coordinated the initial request list and continued to follow-up for supporting evidence as needed.
- Reviewed existing Active Directory policies and procedures, including group memberships for privileged accounts and conducted the following discovery sessions:
    - Assess adherence to the principle of least privilege
    - Identify instances of excessive or unnecessary privileges
    - Evaluate existing controls for monitoring and alerting changes in privilege
    - Assess implementation of MFA where applicable
    - Identify controls for data backup and recovery and evaluate for effectiveness
    - Test for presence of inactive or stale accounts with weak credentials
    - Evaluate domain Group Policy controls for password complexity, expiration, and lockout policies
    - Evaluate specific controls with NIST CSF 2.0 and Microsoft Active Directory management best practices
    - Review audit logs for evidence of control enforcement
- Conducted interviews with key stakeholders for the Active Directory Account Management process.
- Developed a conclusion as to the sufficiency and risk level of the Active Directory policies and procedures as outlined in the aforementioned project objectives.
- Completed a written report covering the identified findings which should also include a roadmap to addressing identified gaps and deficiencies; and
- Reported any observations and recommendations for improvement to the Chief Audit Executive (CAE)

Below are the observations and recommendations that resulted from the audit conducted.

## Detailed Observations and Recommendations

**Observation 1 -** (b) (4) [redacted]

Upon review of the NeighborWorks IT asset inventory it was determined (b) (4) [redacted]

**Risk**

(b) (4) [redacted]

**Recommendation**

NeighborWorks Asset Management Policy states that assets should be maintained in an inventory and categorized. (b) (4) [redacted] Management should update the current Asset Management policy to include controls for handling legacy systems. Legacy systems should be either decommissioned or segmented from the rest of the IT environment. Legacy servers that are segmented from the network should have additional monitoring control in place. Where possible, IT and the cybersecurity teams should (b) (4) [redacted]

**Observation 2 -** (b) (4) [redacted]

(b) (4) [redacted]

**Risk**

(b) (4) [redacted]

**Recommendation**

(b) (4) [redacted] The application allowlist should be documented and only include applications necessary to support job functions.
(b) (4) [redacted]

**Observation 3 –** (b) (4) [redacted]

Per inquiry with the IT Operations team, (b) (4) [redacted]

**Risk**

(b) (4) [redacted]

**Recommendation**

(b) (4) [redacted] The application allowlist should be documented and only include applications necessary to support job functions.

**Observation 4 –** (b) (4) [redacted]

(b) (4) [redacted]

**Risk**

(b) (4) [redacted]

**Recommendation**

(b) (4)

**Observation 5 –** (b) (4)

Per inquiry with the IT Operations team, (b) (4)

**Risk**

(b) (4) This can lead to severe consequences like data breaches, identity theft, monetary loss, and reputational damage.

**Recommendation**

(b) (4)

**Observation 6 –** (b) (4)

(b) (4)

**Risk**

(b) (4)

**Recommendation**

(b) (4)

**Observation 7 –** (b) (4)

(b) (4)

**Risk**

(b) (4)

**Recommendation**

(b) (4)

**Observation 8 -** (b) (4)

(b) (4)

The NeighborWorks Privileged Access Management Policy states: "When granting elevated privileged, the concept of least privileged access should be followed."

**Risk**

(b) (4)

**Recommendation**

(b) (4)

**Observation 9 -** (b) (4)

(b) (4)

The NeighborWorks Privileged Access Management Policy states, "When performing non-security functions, users shall use a non-privileged account."

**Risk**

(b) (4) [redacted]

**Recommendation**

Management should enforce the current Privileged Access Management Policy (b) (4) [redacted]

**Observation 10 -** (b) (4) [redacted]

(b) (4) [redacted] The NeighborWorks Privileged Access Management Policy states, "Comprehensive logging of privileged access activities, including account type change will be maintained."

**Risk**

(b) (4) [redacted]

**Recommendation**

(b) (4) [redacted]

**Observation 11 -** (b) (4) [redacted]

(b) (4) [redacted] The Information Security Policy states all asset inventories must include classification levels. (b) (4) [redacted]

**Risk**

(b) (4)

**Recommendation**

Management should enforce the current Information Security Policy and classify all assets based on business operations and impact. (b) (4)

**Observation 12 -** (b) (4)

(b) (4)

**Risk**

(b) (4)

**Recommendation**

(b) (4)

**Observation 13 -** (b) (4)

(b) (4) NeighborWorks Access Management policy states "Quarterly access control audits must be conducted by System Owner to ensure compliance with policies and procedures."

**Risk**

(b) (4)

this means potential misuse of sensitive data, legal and financial consequences, and compromised network security.

**Recommendation**

Management should enforce the current Access Management Policy (b) (4)

**Observation 14 -** (b) (4)

(b) (4)

**Risk**

(b) (4)

**Recommendation**

(b) (4)

**Observation 15 -** (b) (4)

While Arctic Wolf is set up to monitor all audit logs captured from Domain (b) (4) The NeighborWorks Privileged Access Management Policy states, "Regular

monitoring of logs will be conducted to detect and respond to any unauthorized or suspicious activities."

**Risk**

(b) (4)

**Recommendation**

Management should enforce the current logging and monitoring policy within the Privileged Access Management Policy, (b) (4)

**Observation 16 –** (b) (4)

During discussions with IT operations, a service account SVC-PDQ (b) (4)

**Risk**

(b) (4)

**Observation 17 -** (b) (4)

(b) (4)

**Recommendation**

[redacted]

**Observation 18 -** (b) (4) [redacted]

(b) (4) [redacted]

**Risk**

(b) (4) [redacted]

**Recommendation**

(b) (4) [redacted]

## Conclusion

The Internal Audit Division noted that some critical components of the Active Directory environment are in place. (b) (4) [redacted] NeighborWorks should prioritize and ensure policies and procedures are enforced. (b) (4) [redacted]