Internal Audit Department
NeighborWorks® America

Audit Review of

Privileged/Non-Privileged Access Management Policies

Project Number: NW.ITS.IAM-PNP.2024

Audit Review of Privileged/Non-Privileged Access Management Policies

Table of Contents

Function Responsibility and Internal Control Assessment
Audit Review of Privileged/Non-Privileged Access Management Policies

Business Function Responsibility	**Report Date**	**Period Covered**
Corporate	October 21, 2024	January 1, 2023 through January 31, 2024
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 Neither the Access Management Policy nor the Privileged Access Management Policy identify or detail storage locations or methods for maintaining system identities. In order to ensure that only authorized individuals can access business resources, organizations are required to implement, maintain, and regularly update acceptable system identity databases so as to serve as a central repository in the event of a security risk.[2] The database should include digital identities, their access type, and the associated assets – all of which should be	**No**	**Recommendation 1** **Define and Document Storage Locations** Update the Access Management and Privileged Access Management policies to clearly specify the storage locations of system identities. These locations should be secure, easily accessible to authorized personnel, and regularly updated and maintained per industry standards. Governance of the storage locations should be incorporated into the policies.	**No**	NeighborWorks IT is following NIST v2.0 as its cybersecurity framework. CCM is another cybersecurity framework that is geared more towards the evaluation of Cloud Service Providers. NeighborWorks does not provide Cloud Services we are a consumer of cloud services. Our vendors that provide cloud services must adhere to CCM. We are willing to provide information that proves the vendors of NeighborWorks IT owned services are		IA accepts management response. Internal Audit accepts IT use of CCM as a comparable framework against which to evaluate Cloud Service Providers on the provision that management provides information documenting that its vendors are CCM certified.

[2] The Cloud Controls Matrix Version IV (CCMv4.0), Identity and Access Management control 03 (IAM-03): Identity Inventory

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
documented in the official access management policy. **Risk Rating**: (b) (5)		Additionally, ensure the Access Management and Privileged Access Management Policies are regularly reviewed and updated to reflect any changes in storage methods, technology, or organization security practices.		CCM certified. Lastly in version 2 of the Access Management and Privileged Access management policies we have added a section for compliance review stating the policies will be reviewed annually.		
Observation 2 Neither the Access Management Policy nor the Privileged Access Management Policy reference a detailed separation of duties structure. In order to ensure that no user can solely initiate, access, alter, or delete data,[3] organizations are required to clearly define segregation of duties as relates to system authorization and access. The basic principles governing an	**Yes**	**Recommendation 2a** **Define and Implement a Separation of Duties Structure** Update the Access Management and Privileged Access Management Policies to explicitly define a detailed separation of duties framework. Both policies should specify and ensure that no	**Yes**	In version 2 of the Access Management and Privileged Access management policies we have clearly defined roles and responsibilities that show the separation of duties. We have also defined that System Owners should conduct regular reviews of roles that are	02/25	IA accepts management response.

[3] CCMv4.0, IAM-01: Identity and Access Management Policy and Procedures; and IAM-04: Separation of Duties

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
acceptable separation of duties structure require the following incompatible duties to be segregated: 1) authorization and approval; 2) custody and maintenance; and 3) recording and reporting.[4] **Risk Rating**: (b) (5)		single individual can perform end-to-end tasks without oversight or approval. This can be attained by ensuring that the following duties are clearly segregated in both policies and procedures: *Authorization and Approval* – Individuals responsible for initiating requests for system access or changes should not be the same individuals who approve those actions. *Custody and Maintenance* – Individuals responsible for the custody of		assigned in the system to ensure their validity. IT&S can only control training for IT owned systems. System Owners must be held accountable for ensuring they manage the training for their end users.		

[4] Ferroni, Stefano. "Implementing Segregation of Duties: A Practical Experience Based on Best Practices." ISACA, https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/implementing-segregation-of-duties-a-practical-experience-based-on-best-practices?utm_source=isaca_internal&utm_medium=share_link

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
		systems or data should not have the authority to approve or authorize changes. *Recording and Reporting* – Individuals responsible for recording transactions or activities should not also be responsible for reporting or validating the accuracy of those records. **Recommendation 2b** **Regular Access Reviews** Implement periodic reviews of access rights to ensure roles and responsibilities remain segregated. Doing so will help detect any violations of the separation of duties structure.				

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
		Recommendation 2c **Training and Awareness** Conduct regular training for staff to ensure they understand the importance of separation of duties and their role within its structure.				
Observation 3 While the Access Management and Privileged Access Management policies reference the process for access request and approval, (b) (4) [redacted] Organizations are required to document the process by which existing access is (b) (4) [redacted]. The policy should also delineate the set	Yes	**Recommendation 3** **Document the Access (b) (4) [redacted] Process** Update the Access Management and Privileged Access Management policies to include a clearly defined (b) (4) [redacted] user access. The process should outline the steps for (b) (4) [redacted]	Yes	In version 2 of the Access Management and Privileged Access management policies the (b) (4) [redacted] process is defined.	02/25	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 and Timeline
timeframe for access (b) (4).[5] **Risk Rating**: (b) (5)		(b) (4), as well as the procedures for immediately (b) (4) The updated policies should clearly define the timeframes within which access (b) (4) must occur, as well as escalation procedures in the event access (b) (4) is not completed within the established timeframes. Consider industry best standards when deciding on the appropriate timeframes for access (b) (4)				

[5] CCMv4.0, IAM-07: User Access Changes and Revocation

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). Additionally, designate who will be accountable for ensuring timely action and compliance.				
Observation 4 The Privileged Access Management Policy details required multi-factor authentication (MFA) for privileged account access; however, the Access Management Policy does not indicate which authentication method will be utilized. In order to ensure that only authorized and authenticated users access services and resources, organizations are required to document and implement MFA for non-privileged access as well.[6]	**Yes**	**Recommendation 4**: **Implement MFA for Non-Privileged Access** Update the Access Management Policy to require MFA for non-privileged accounts and include the process by which regular reviews of MFA requirements will be conducted. This will ensure that the organization remains up-to-date with evolving security risks and technological advancements. The	**Yes**	IT&S agrees to this for IT owned and managed services. IT&S cannot enforce MFA for all NeighborWorks systems because IT&S does not own all NeighborWorks systems. MFA for non privileged accounts will require budgetary investment from NeighborWorks to ensure it is implemented for IT owned and managed services. This	05/26	IA accepts management response.

[6] CCMv4.0, Identification and Authentication control 2-2 (IA-02): Multi-factor Authentication to Non-privileged Accounts

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
Risk Rating: (b) (5)		policy should specify: the authentication methods to be used (e.g., risk-based authentication, one-time passwords, biometric authentication); and the conditions under which MFA will be enforced for non-privileged accounts. Additionally, incorporate training and guideline implementation into the roll-out plan for users to ensure they know how to set up and use MFA, as well as its importance in protecting the organization from risk.		initiative is currently not budgeted in FY25. IT&S can commit to creating a plan in FY25 but implementation cannot be completed until FY26.		

Risk Rating Legend

Risk Rating: High
A serious weakness which significantly impacts the Corporation from achieving its corporate objectives, financial results, statutory obligations or that may otherwise impair the Corporation's reputation.

Risk Rating: Moderate
A control weakness which could potentially undermine the effectiveness of the existing system of internal controls and/or operational efficiency, integrity of reporting and should therefore be addressed.

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

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

Privileged/Non-Privileged Access Management Policies</th></tr>
<tr><th># Of Responses</th><th>Response</th><th>Recommendation #</th></tr>
<tr><td>3</td><td>Agreement with the recommendation(s)</td><td>2,3,4</td></tr>
<tr><td>1</td><td>Disagreement with the recommendation(s)</td><td>1</td></tr>
</table>

Background

Access Management, commonly referred to as Identity Access Management (IAM), is a system to identify, manage, and protect an organization's access to resources and data. Its primary function is to authorize and authenticate individuals' access to data, applications, and systems based on predefined roles and attributes. Privileged access refers to special access to systems and resources above those provided to a standard user. IT&S is responsible for ensuring that privileged and non-privileged access policies are sound, satisfactorily documented, and fully implemented in a way that minimizes risk to the organization. Internal Audit evaluated the effectiveness of the privileged and non-privileged access management policies against established controls mapped to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) 2.0.

Objective

The objective of this review was to obtain reasonable assurance that the organization's privileged and non-privileged access management policies were developed in accordance with applicable standards and mitigate cyber security risks to the organization.

Scope Timeframe

January 1, 2023, through January 31, 2024

Methodology

Internal Audit held an introductory meeting with the IT&S Executive Vice President/Chief Information Offer and Senior Vice President to obtain a better understanding of the cyber security objectives, controls, and protocols in place to determine the information types that may be needed for this audit review. Following the meeting, IT&S provided Internal Audit with draft copies of its Access Management and Privileged Access Management Policies which were, and are currently, in review with the Office of General Counsel. IT&S reported that no IAM audits had been conducted during the identified scope timeframe of this audit review.

In addition to a review of the draft policies, Internal Audit also conducted a review of all applicable NIST CSF 2.0 Framework standards, as well as various IAM best practice policies and manuals.

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

Observations and Recommendations

Observation 1

Neither the Access Management Policy nor the Privileged Access Management Policy identify or detail storage locations or methods for maintaining system identities. In order to ensure that only authorized individuals can access business resources, organizations are required to implement, maintain, and regularly update acceptable system identity databases so as to serve as a central repository in the event of a security risk.[7] The database should include digital identities, their access type, and the associated assets – all of which should be documented in the official access management policy.

Recommendation 1: Define and Document Storage Locations

Update the Access Management and Privileged Access Management policies to clearly specify the storage locations of system identities. These locations should be secure, easily accessible to authorized personnel, and regularly updated and maintained per industry standards. Governance of the storage locations should be incorporated into the policies. Additionally, ensure the Access Management and Privileged Access Management Policies are regularly reviewed and updated to reflect any changes in storage methods, technology, or organization security practices.

Observation 2

Neither the Access Management Policy nor the Privileged Access Management Policy reference a detailed separation of duties structure. In order to ensure that no user can solely initiate, access, alter, or delete data,[8] organizations are required to clearly define segregation of duties as relates to system authorization and access. The basic principles governing an acceptable separation of duties structure require the following incompatible duties to be segregated: 1) authorization and approval; 2) custody and maintenance; and 3) recording and reporting.[9]

Recommendation 2a: Define and Implement a Separation of Duties Structure

Update the Access Management and Privileged Access Management Policies to explicitly define a detailed separation of duties framework. Both policies should specify and ensure that no single individual can perform end-to-end tasks without oversight or approval. This can be attained by ensuring that the following duties are clearly segregated in both policies and procedures:

Authorization and Approval – Individuals responsible for initiating requests for system access or changes should not be the same individuals who approve those actions.

Custody and Maintenance – Individuals responsible for the custody of systems or data should not have the authority to approve or authorize changes.

Recording and Reporting – Individuals responsible for recording transactions or activities should not also be responsible for reporting or validating the accuracy of those records.

Recommendation 2b: Regular Access Reviews

Implement periodic reviews of access rights to ensure roles and responsibilities remain segregated. Doing so will help detect any violations of the separation of duties structure.

[7] The Cloud Controls Matrix Version IV (CCMv4.0), Identity and Access Management control 03 (IAM-03): Identity Inventory

[8] CCMv4.0, IAM-01: Identity and Access Management Policy and Procedures; and IAM-04: Separation of Duties

[9] Ferroni, Stefano. "Implementing Segregation of Duties: A Practical Experience Based on Best Practices." ISACA, https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/implementing-segregation-of-duties-a-practical-experience-based-on-best-practices?utm_source=isaca_internal&utm_medium=share_link

Recommendation 2c: Training and Awareness

Conduct regular training for staff to ensure they understand the importance of separation of duties and their role within its structure.

Observation 3

While the Access Management and Privileged Access Management policies reference the process for access request and approval, neither policy sufficiently details the process by which access is (b) (4) Organizations are required to document the process by which existing access (b) (4). The policy should also delineate the set timeframe for access (b) (4).[10]

Recommendation 3: Document the Access (b) (4) Process

Update the Access Management and Privileged Access Management policies to include a clearly defined process for (b) (4) user access. The process should outline the steps for (b) (4) access when users' roles or responsibilities change, as well as the procedures for immediately (b) (4) access upon termination or identification of a security threat.

The updated policies should clearly define the timeframes within which access (b) (4) must occur, as well as escalation procedures in the event access (b) (4) is not completed within the established timeframes. Consider industry best standards when deciding on the appropriate timeframes for access (b) (4). Additionally, designate who will be accountable for ensuring timely action and compliance.

Observation 4

The Privileged Access Management Policy details required MFA for privileged account access; however, the Access Management Policy does not indicate which authentication method will be utilized. In order to ensure that only authorized and authenticated users access services and resources, organizations are required to document and implement MFA for non-privileged access as well.[11]

Recommendation 4: Implement MFA for Non-Privileged Access

Update the Access Management Policy to require MFA for non-privileged accounts and include the process by which regular reviews of MFA requirements will be conducted. This will ensure that the organization remains up-to-date with evolving security risks and technological advancements. The policy should specify: the authentication methods to be used (e.g., risk-based authentication, one-time passwords, biometric authentication); and the conditions under which MFA will be enforced for non-privileged accounts. Additionally, incorporate training and guideline implementation into the roll-out plan for users to ensure they know how to set up and use MFA, as well as its importance in protecting the organization from risk.

[10] CCMv4.0, IAM-07: User Access Changes and Revocation

[11] CCMv4.0, Identification and Authentication control 2-2 (IA-02): Multi-factor Authentication to Non-privileged Accounts

Conclusion

The Privileged/Non-Privileged Access Management policy review identified gaps in IT&S's draft access management policies which could potentially expose the organization to security risks, such as unauthorized access, ineffective incident response, and potential regulatory non-compliance. It should be noted that the existing IT&S draft policies contain many of the key elements for a well-developed IAM plan, including detailed delineation of user roles and responsibilities; however, additional revisions which implement the included recommendations are needed to effectively balance organizational security and control user access to critical information.