Internal Audit Department
NeighborWorks® America

# Audit Review of

# Cyber Attack Incident Response II

Project Number: NW.ITS.CIR.2025

# Audit Review of Cyber Attack Incident Response II

## Table of Contents

# Function Responsibility and Internal Control Assessment
# Audit Review of Cyber Attack Incident Response II

| Business Function Responsibility | Report Date | Period Covered |
|---|---|---|
| Incident Response | April 23, 2025 | Point in Time (Design)<br>Q1 2025 |
| **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 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>The current recovery policy does not include system prioritization and as of Q1 2025 there was no evidence of underlying documented procedures in place for system recovery. Additionally, policies did not (b) (4) [redacted]<br><br>**Risk Rating**: (b) (4) [redacted] | **Yes** | **Recommendation 1**<br><br>Update the backup and recovery policies and document procedures to include system prioritization and recovery dependencies. (b) (4) [redacted] | **Yes** | Due to funding constraints in FY26, IT&S (b) (4) [redacted] | TBD Major activities are outlined in the Disaster Recovery Plan | IAD accepts management response pending management confirmation of an estimated date of implementation. |
| **Observation 2**<br><br>Based on the evidence provided, [redacted] | **Yes** | **Recommendation 2**<br><br>NeighborWorks should implement measures to | **Yes** | IT&S have measures and capabilities in place to isolate | 7/30/2025 | IAD 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 |
|---|---|---|---|---|---|---|
| (b) (4)<br><br>**Risk Rating**: (b) (4) | | (b) (4) | | backup as outlined in the organization policy. (b) (4) Staff that have been assigned backup admin operations will be granted usernames and passwords that only support backup operations. | | |
| **Observation 3**<br><br>(b) (4) | **Yes** | **Recommendation 3** | **Yes** | | 8/30/2025 | IAD 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 |
|---|---|---|---|---|---|---|
| [redacted]<br>**Risk Rating:** [redacted] | | [redacted] | | [redacted] | | |
| **Observation 4**<br><br>The current backup procedures are not aligned with the Disaster Recovery Plan. (b) (4) [redacted] | **Yes** | **Recommendation 4**<br><br>NeighborWorks should ensure application owners and stakeholders identify realistic Recovery point Objectives, Recovery Time Objectives, and Maximum Tolerable Downtimes. The policy and underlying procedures should be updated to align | **Yes** | Due to funding constraints for FY25 and FY26, the development of the organization DRP that prioritizes the business unit requirements will be delayed. IT&S will review current national standards for recovery of systems, applications and networks. IT&S | TBD | IAD accepts management response pending management confirmation of an estimated date of implementation. |

| 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:** [redacted] | | with these objectives. (b) (4) [redacted] | | will update the current policy to ensure RTO objectives are in-line with national standards for Disaster Recovery Plan.(b) (4) [redacted] | | |

| 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>The Incident Response Policy calls for establishing communication plans, roles and responsibilities, training, and procedures for gathering and analyzing evidence. Currently, these underlying procedures are in progress but not approved and published.<br><br>**Risk Rating:**<br>(b) (4) | **Yes** | **Recommendation 5**<br><br>NeighborWorks should establish critical procedures such as evidence gathering, preservation, and analysis, communications, containment strategies, incident training, and clearly defined roles and responsibilities to ensure key stakeholders acknowledge the published incident response process. | **Yes** | Due to funding constraints in FY26 the establishment of the incident response team will be delayed until funding is available to ensure that activities that are not currently covered in the current plan will be established for the incident response team. The development of Standard Operation Procedures for communication, roles and responsibilities, and incident response training will ensure IT&S | TBD | IAD accepts management response pending management confirmation of an estimated date of implementation. |

| 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 |
|---|---|---|---|---|---|---|
| | | | | provides a fully operational capability. | | |
| **Observation 6**<br>[redacted]<br>**Risk Rating:**<br>[redacted] | **NO** | **Recommendation 6**<br>(b) (4) [redacted] | **Yes** | (b) (4) [redacted] | Completed | IAD accepts management response pending IAD validation, which will be completed by 12/30/25. |
| **Observation 7**<br>Specific individuals to fill incident response roles as well as their backups are not documented in the policy or procedure documents.<br>**Risk Rating:**<br>[redacted] | **Yes** | **Recommendation 7**<br>The Incident Response Policy or supporting procedures should clearly document individual's roles within the incident response team as well as the core individuals to be included in the | **Yes** | We currently have a list of IT&S staff and business unit staff, led by the SVP with an assigned manager for each unit, however we have not documented it in the policy. Will be maintained in ServiceNow. IT&S will update its | 12/30/2025 | IAD 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 |
|---|---|---|---|---|---|---|
| | | incident response team. | | policy to include this information. | | |
| **Observation 8**<br><br>The Incident Response Policy identifies the need to create standardized incident documentation templates and minimum documentation standards, but they have not been developed to date. Additionally, key areas such as external reporting process, legal input, and regulatory reporting requirements/guidance are not defined.<br><br>**Risk Rating:** (b) (4) | **Yes** | **Recommendation 8**<br><br>NeighborWorks should establish documentation standards and templates for recording information during an incident. Additionally, NW IT Security should work with Legal to establish an external reporting process and to obtain guidance on any reporting requirements to external entities. | **Yes** | The documentation and template will be stored in ServiceNow ITOM. Standardized templates are incorporated in the ServiceNow implementation project. | 10/30/2025 | IAD 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 |
|---|---|---|---|---|---|---|
| **Observation 9**<br><br>The Incident Response policy states that a communication plan, methods, and procedures must be developed. However, these are currently not in existence.<br><br>**Risk Rating:** [redacted] | **Yes** | **Recommendation 9**<br><br>Communication plans and methods should be established that include emergency notifications, standard communication methods, out of band communication methods, and basic guidelines on relevant stakeholders be documented in communications. | **Yes** | Currently the incident response activities are located in Major Incident Management SOP and the IT Security Incident Response Policy. (b) (4) [redacted] | Completed | IAD accepts management response pending IAD validation, which will be completed by 12/30/25. |

## 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:**<br><br>**Cyber Attack Incident Response II** | | |
|---|---|---|
| **# Of Responses** | **Response** | **Recommendation #** |
| 9 | Agreement with the recommendation(s) | 9 |
| N/A | Disagreement with the recommendation(s) | N/A |

## Background

In August 2024, last fiscal year, the Internal Audit Division issued a report on the Corporation's Cyber Attack Incidence Response with scope limitations resulting from management actions. Based on that report, the Internal Audit Division indicated that a follow-up review would be conducted to re-assess the Corporation's Cyber Attack Incidence on certain internal controls within the area of Incident Response (IR) protocols.

CohnReznick was engaged to conduct this internal audit review and the scope and approach of the audit was determined based on their expertise, information provided to CohnReznick by NeighborWorks' management, prior audit/assessment scope and results, and in collaboration with NeighborWorks Internal Audit team. The objective of this internal audit was to evaluate the design of the in-scope IR controls in place at NeighborWorks. Due to the timing of the planned implementation of the IR Plan in December 2024, it was not feasible to evaluate the operating effectiveness of the controls. This can be the objective of a future internal audit of the IR protocol.

## Objective

The objective of this audit is to assess the current state of NeighborWorks' incident response program. Due to ongoing updates to the program and given the new program is in the process of implementation, the objective of the audit is to assess the design of the program.

## Scope

Internal audit leveraged the CIS framework version 8 to perform the audit. The CIS framework encompasses 18 controls (see image 1) supported by 143 safeguards and is divided into 3 Implementation Groups or maturity levels. Implementation Group 1 (IG1) overall includes the 56 safeguards that the CIS has determined to represent the minimum standard for essential cyber hygiene. IG2 and IG3 include an additional 16 controls and 87 safeguards that organizations should implement based on their relevant cybersecurity threats, risks, and strategy.

Using the CIS framework, CohnReznick has selected and summarized the two in-scope controls and 10 in-scope safeguards into two (2) areas most relevant to NeighborWorks' Incident Response capabilities given its size and resources. The two areas include several Implementation Group 1 (IG1) and three IG3 safeguards

1. 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)***

2. Control 17: Incident Response Management
    a. Designate Personnel to Manage Incident Handling ***(17.1)***
    b. Establish and Maintain Contact Information for Reporting Security Incidents ***(17.2)***
    c. Establish and Maintain an Enterprise Process for Reporting Incidents **(17.3)**
    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)***

## Methodology

For this internal audit, CohnReznick:

- Planned and built an internal audit program approved by NeighborWorks Internal Audit Management.
- Coordinated the initial request list to follow-up for supporting evidence as needed.
- Reviewed policies and procedures, previous internal audit reporting that are relevant to the in-scope controls listed above and conduct discovery sessions as needed.
- Conducted interviews with key stakeholders for the IR process.
- Assessed evidence, to identify, analyze, and document internal control gaps in accordance with best practice utilizing the Internal Audit Division's templates for consistency.
- Performed tests of one (1) sample where necessary, based on risk, to assessment control design.

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

## Observations and Recommendations

### Observation 1

(b) (4) [redacted]

Without system prioritization, recovery times can be greatly extended and critical decisions during an incident can be difficult to make. Additionally, backup security standards are crucial for ensuring that proper processes developed to protect recovery data from threat actors.

### Recommendation 1

Update the backup and recovery policies and document procedures to include system prioritization and recovery dependencies. [redacted]

[redacted]

**Observation 2**

Based on the evidence provided, (b) (4) [redacted]

Most destructive attacks such as ransomware, especially target backups and backup servers. Often threat actors in these scenarios have gained full administrative access to the domain, server, or cloud environment. (b) (4) [redacted]

**Recommendation 2**

(b) (4) [redacted]

**Observation 3**

(b) (4) [redacted]

(b) (4) [redacted]

[redacted]

**Recommendation 3**

[redacted]

**Observation 4**

The current backup procedures are not aligned with the Disaster Recovery Plan. (b) (4) [redacted]

Without alignment between the backup and recovery procedures and business requirements, defined recovery objectives will not be met.

**Recommendation 4**

Management should ensure application owners and stakeholders identify realistic Recovery point Objectives, Recovery Time Objectives, and Maximum Tolerable Downtimes. The policy and underlying procedures should be updated to align with these objectives. (b) (4) [redacted]

**Observation 5**

The Incident Response Policy calls for establishing communication plans, roles and responsibilities, training, and procedures for gathering and analyzing evidence. Currently, these underlying procedures are in progress but not approved and published.

Without procedure documentation incident response tasks may be delayed and unnecessary mistakes made.

**Recommendation 5**

Management should establish critical procedures such as evidence gathering, preservation, and analysis, communications, containment strategies, incident training, and clearly defined roles and responsibilities to ensure key stakeholders acknowledge the published incident response process.

**Observation 6**

(b) (4) [redacted]

[2] The ntds.dit file is the central database for the Active Directory, storing all essential Active Directory data, including but not limited to: user accounts and passwords; domain and forest configurations; groups, computers, and organizational units (OUs), security identifiers, and group policy data.

**Recommendation 6**

(b) (4) [redacted]

**Observation 7**

The Incident Response Policy included a section with roles and responsibilities for functions such as "NW IT Security", "Office of General Counsel", and "System Owner" (among others). Based on inquiry specific individuals to fill incident response roles as well as their backups are not documented in the policy or procedure documents.

Without key roles and responsibilities clearly defined, high stress scenarios can cause unnecessary conflict and confusion leading to poor decision making.

**Recommendation 7**

The Incident Response Policy or supporting procedures should clearly document individual's roles within the incident response team as well as the core individuals to be included in the incident response team.

**Observation 8**

The Incident Response Policy identifies the need to create standardized incident documentation templates and minimum documentation standards, but they have not been developed to date. Additionally, key areas such as external reporting process, legal input, and regulatory reporting requirements/guidance are not defined.

Without clear documentation standards and procedures, critical information may be lost that would assist in lessons learned or reporting requirements could be missed.

**Recommendation 8**

Management should establish documentation standards and templates for recording information during an incident. Additionally, NW IT Security should work with Legal to establish an external reporting process and to obtain guidance on any reporting requirements to external entities.

**Observation 9**

The Incident Response policy states that a communication plan, methods, and procedures must be developed. However, these are currently not in existence. (b) (4) [redacted]

Without clear communication standards and procedures, key stakeholders may not respond in a timely manner, communication methods may not be secure, and disparate communications could lead to legal or reputational harm.

**Recommendation 9**

Communication plans and methods should be established that include emergency notifications, standard communication methods, out of band communication methods, and basic guidelines on relevant stakeholders be documented in communications.

## Conclusion

The Internal Audit Division notes that many critical components of the IR program are either in place or planned for FY 2025. However, there were several areas of improvement identified above. Critical is the need to align the Corporations Disaster Recovery Plan with realistic objectives. NeighborWorks should prioritize solidifying the backup and recovery process and finalizing the incident response team members, roles, and responsibilities. This prioritization should be ensured and resourced across fiscal cycles.