togetherforbetter

AUDIT REPORT

Clark County Can Improve VPN Security

July 2025

ANGELA DARRAGH, CPA, CISA, CFE
AUDIT DIRECTOR
CLARK COUNTY AUDIT DEPARTMENT

Clark County Can Improve VPN Security

Audit Executive Summary

July 2025

Background

Clark County has a need to allow remote users access to the County network using county owned and non-county owned equipment. This is done through a Virtual Private Network (VPN) client. The County VPN technology is software that allows County staff to securely access network resources remotely. VPN allows a secure connection for internet. It encrypts data and hides the address, making it hard for others to track online activities or obtain information that is being transmitted.

Over the past several years, the number of County employees using VPN to access the County network increased substantially due to an increase in remote work options. There are currently 3,603 employee accounts and 170 vendor accounts. The Clark County Information Technology department (IT) is responsible for the implementation and overall management of the VPN applications.

State law requires Clark County to follow specific cybersecurity controls. Clark County follows guidelines issued by the Center for Internet Security (CIS) to comply with this law.[i]

Clark County is also subject to other requirements for securing data. These include the HIPAA Privacy and Security Rule, Payment Card Industry standards, and Criminal Justice Information System standards.

What We Found

- No risk assessment for VPN
- Security requirements do not apply to all users
- Dormant accounts are not disabled after 45 days of inactivity
- Criteria for log reviews needs to be updated
- Some policies and procedures did not have up to date information
- VPN related issues are not resolved in accordance with department guidelines
- VPN backups are not tested periodically

Recommendations

We made 11 recommendations to improve security of the County's VPN solution.

togetherforbetter

Why We Did this Audit.

We conducted this audit to determine whether:

- VPN implementation and configuration are appropriate.
- Policies and procedures are adequate to protect County data.
- Clark County maintains user permissions based on employment status and job duties; and
- VPN activity is monitored.

For more information about this or other audit reports go to clarkcountynv.gov/audit or call (702) 455-3269.

Audit Team

Angela Darragh, Director
Cynthia Birney, Audit Manager
Felix Luna, Principal Auditor
Christopher Hui, Information Systems Auditor
Joshua Cheney, Information Systems Auditor
Daniel Partida, Internal Auditor

Audit Committee

Commissioner Michael Naft
Commissioner April Becker
Commissioner William McCurdy II

About the Audit Department

The Audit Department is an independent department of Clark County reporting directly to the County Manager. The Audit Department promotes economical, efficient, and effective operations and combats fraud, waste, and abuse by providing management with independent and objective evaluations of operations. The Department also helps keep the public informed about the quality of Clark County Management through audit reports.

You can obtain copies of this report by contacting:

Clark County Audit Department
PO Box 551120
Las Vegas, NV 89155-1120
(702) 455-3269

CountyAuditor@ClarkCountyNV.gov

Or download and view an electronic copy by visiting our website at:

https://www.clarkcountynv.gov/government/departments/audit_department/audit-reports

Table of Contents

Background

Clark County has a need to allow remote users access to the County network using county owned and non-county owned equipment. This is done through a Virtual Private Network (VPN) client. The County VPN technology is software that allows County staff to securely access network resources remotely. VPN allows a secure connection for internet. It encrypts data and hides the address, making it hard for others to track online activities or obtain information that is being transmitted.

Over the past several years, the number of County employees using VPN to access the County network increased substantially due to an increase in remote work options. There are currently 3,603 employee accounts and 170 vendor accounts. The Clark County Information Technology department (IT) is responsible for the implementation and overall management of the VPN applications.

State law requires Clark County to follow specific cybersecurity controls. Clark County follows guidelines issued by the Center for Internet Security (CIS) to comply with this law.[ii]

Clark County is also subject to other requirements for securing data. These include the HIPAA Privacy and Security Rule, Payment Card Industry standards, and Criminal Justice Information System standards.

Objectives

Our audit objectives were to review the Clark County IT VPN solution that is implemented within the County Enterprise and to determine whether:

- VPN implementation and configuration are appropriate;
- Policies and procedures are adequate to protect County data;
- Clark County maintains user permissions based on employment status and job duties; and
- VPN activity is monitored.

Conclusions

We found that while VPN applications used by Clark County are generally configured appropriately, there are areas that can be improved.

These include:

- Completion of risk assessments;
- Application of pre-connection security requirements;

- Disabling of dormant accounts;
- Selection of alert criteria;
- Completion of policies and procedures; and
- Testing of backup procedures.

Findings are rated based on a risk assessment that takes into consideration the circumstances of the current condition including compensating controls and the potential impact on reputation and customer confidence, safety and health, finances, productivity, and the possibility of fines or legal penalties. It also considers the impact on confidentiality, integrity, and availability of data.

7 Total Audit Findings

2 High Risk

High risk findings indicate an immediate and significant threat to one or more of the impact areas.

2 Medium Risk Findings

Medium risk findings indicate the conditions present a less significant threat to one or more of the impact areas. They also include issues that would be considered high if one control is not working as designed.

3 Low Risk Findings

Low risk findings are typically departures from best business practices or areas where effectiveness, efficiency, or internal controls can be enhanced. They also include issues that would be considered high or medium risk if alternate controls were not in place.

Findings, Recommendations, and Responses

Finding #1 – A Risk Assessment Was Not Completed for VPN

We found that Clark County IT is not performing a periodic security risk assessment for VPN.

The purpose of a risk assessment is to identify scenarios that could affect the confidentiality, integrity, or availability of data. It identifies potential vulnerabilities and the likelihood of occurrence. This allows management to determine whether any additional safeguards need to be put in place.

Further, Clark County has several departments covered by HIPAA regulations that may use VPN to access data. Federal regulations require a risk assessment for any system handling HIPAA protected data.[iii]

Civil monetary penalties for HIPAA violations can result in fines of between $141 and $71,162 per violation and compliance action plans that could include external monitoring. If a violation is found to be due to willful neglect, penalties can be as high as $2,134,831.

Recommendations

- Complete a written risk assessment for VPN applications to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of data.
- Implement additional security measures as appropriate based on the assessment.
- Review and update the risk assessment annually to ensure risks are at reasonable and appropriate level.

Management Response

- The Enterprise Information Security team will create and complete a risk assessment for the two VPN applications no later than August 14, 2025.

Finding #2 - Security Requirements to Connect to the County Network by VPN Do Not Apply to All Users

Clark County has certain requirements users must meet to connect to the County network through VPN. Requirements include items such as antivirus, antispyware and firewall software that must be installed on the host. We found that the County is not requiring all user types to comply with these requirements.

Requirements for accessing the County network are included in Information Technology Directive 1:

> *7.2.1 Access Control Policy: All hosts, public or otherwise, must be running the latest version of Windows with critical security updates installed and an antivirus package with an up-to-date virus signature database. They must also have a firewall program installed and running. Any host not meeting these requirements is not permitted to login.*

This is also a best practice as identified in the National Institute of Standards and Technology special publication 800-113:

> *4.4 Implement and Test Prototype: Endpoint Security. Only the client machines that pass the security requirements (e.g., firewall, antivirus software) should be granted access to the SSL VPN. If any security mechanism such as a virtual storage space or cache cleaner is enabled during a login session, these mechanisms should erase all data downloaded during the VPN session.*

When the County is unable to verify if hosts accessing the County network fully comply with Clark County requirements, it increases the risk to the confidentiality, integrity, and availability of County data.

Recommendation

Verify all clients connecting to County VPN have the latest version of Windows with critical security updates installed and an antivirus package with an up-to-date virus signature database.

Management Response

Information Technology team will work to implement endpoint posture assessment for Operating System patches and antivirus checks on the VPN. The initiative will require planning, testing, training, and documentation to support a smooth deployment. We anticipate completing this work by November 1, 2025.

Finding #3 - Dormant Accounts Not Disabled within CIS Required Timelines

Clark County is currently disabling accounts after 60 days of inactivity. However, “CIS control 5.3: Disable Dormant Accounts”, requires the County to disable or delete dormant accounts after 45 days of inactivity.

Clark County is not compliant with CIS Controls as mandated by Nevada Revised Statues. Failing to comply with CIS Controls allow accounts to stay active for a longer period, increasing the risk of accounts being used without authorization and potentially affecting the confidentiality,

integrity, and availability of data. This failure exposes Clark County to the negative impacts of a potential data breach.

Recommendation

Update the current process to disable accounts after 45 days of inactivity.

Management Response

Information Technology team will update our current process to disable accounts after 45 days of inactivity as suggested. This will be completed by September 1st, 2025.

Finding #4 - Criteria for Automated Log Reviews Need to be Validated

VPN audit logs should be reviewed to maintain security and integrity of Clark County data. Log review is used as a tool to monitor unusual behavior; for example, logging on at unusual hours or making an excessive number of attempts to log on. This tool also allows for quick identification of possible unauthorized access or data breach.

Clark County IT uses an application to automatically review logs based on criteria set by the department. They also perform manual reviews of logs as needed. We do not believe Clark County IT included all appropriate scenarios in the automated review. IT should have identified these types of scenarios during a risk assessment, which was not completed.

Not having the correct notifications in place could potentially increase the time to identify and respond to unauthorized access.

Recommendation

Review and update the automated log review process based on risks identified in an IT risk assessment.

Management Response

Clark County Information Technology (CCIT) department has a number of tools in place that can detect anomalous login activity. The primary tool is a SIEM platform. The tool ingests a number of logs from various sources and correlates events from each log to identify anomalous behavior. This includes multiple logins from disparate geographical locations and\or times.

CCIT was already migrating to a new SIEM which offers a more robust and granular platform. During this migration, additional logs, rules and alerts will be added. There are additional tools that could also detect anomalous logins. Finally, CCIT has monitoring \ alerting engagements with both MS-ISAC and our contracted security services partner to identify and alert CCIT when anomalous behavior is detected on the network.

Completion of the migration to the new tools will ensure the appropriate logs and alerts are configured to maintain the appropriate probability that anomalous behavior is detected and the appropriate alerts are generated.

Finding #5 - Policies and Procedures Need to Be Updated

While the IT department has policies and procedures in place for many of the CIS controls, we identified areas that need improvement.

We found 2 of their end point security application procedures do not include necessary detail to continue operation of a threat response.

We also found 7 procedures that need to be updated to reflect current processes, point of contact, or application details for the applicable areas. These areas include phishing and email investigations.

Information Technology should have current policies and procedures implemented to ensure compliance with CIS controls.

Not having updated policies and procedures opens the risk of being unable to ensure consistent operations, compliance with regulations, and data security.

Recommendation

Update existing policies and procedures to ensure they reflect current processes.

Management Response

Clark County Information Technology (CCIT) has an active project to evaluate and migrate our EDR (Endpoint Detection & Response) from our current solution to another solution. We are targeting the end of September 2025 to complete this effort.

The new tool has additional features that CCIT will evaluate and implement, as appropriate, in an effort to further enhance this tool and as a regular part of the ongoing tuning and management of the platform. All appropriate and necessary policies and procedures will be developed to support the new tool.

CCIT also has an existing effort underway to significantly enhance the e-mail security platform. Updates will be made to the phishing incident response runbook. We expect to complete these efforts by September 30th, 2025.

Finding #6 – VPN Related Issues are Not Resolved In Accordance with Department Guidelines

Clark County IT prioritizes issues reported to the help desk by type and resolves them based on an established timeline. A "ticket" is opened for each issue and assigned to the responsible technician.

The tickets are assigned under one of the following priorities:

Priority 1 - Incidents should be resolved in 2 hours
Priority 2 - Incidents should be resolved in 8 hours
Priority 3 - Incidents should be resolved in 6 days, 8 hours

The Help Desk prioritizes incidents using the Incident Priority Matrix (Figure 1).

Figure 1. Incident Priority Matrix

Incident Priority Matrix				
Impact	**High**	High 2	Critical 1	Critical 1
	Medium	Medium 3	High 2	Critical 1
	Low	Medium 3	Medium 3	High 2
		Low	**Medium**	**High**
		Urgency		

Impact

High:	Department, division, of multiple priority users affected
Medium:	Small group of users (4-25) or a single priority user
Low:	1-3 users

Urgency

High:	Business-critical service is affected
Medium:	Non-business-critical service is affected
Low:	Business service is not affected

Source: Adapted from ServiceNow Knowledge *Base: Customer Self-Service | Category: IT Policies, Procedures & Directives: Incident Priority Matrix*

There were 407 incidents related to VPN services during fiscal year 2024. We sampled a total of 41 incidents and found 11 of 41 (27%) tickets related to VPN services did not meet the

target response times. (1 priority 1, 3 priority 2, and 7 priority 3).

During testing, we found that in some cases, the ticket was put on hold. This may have been a result of IT requiring additional time to resolve the issue or waiting for a response from the user that opened the ticket. For tickets that were put on hold, we found instances where the assigned technician did not receive alerts that the ticket was still open. In other cases, the assigned technician received inactivity alerts, but failed to investigate whether the ticket needed resolution. In one instance, the system sent 238 inactivity alerts before the ticket was closed, with no indication that action was taken to fix the issue.

We believe the volume of alerts and lack of supervision allow tickets to remain outstanding for extended periods of time.

VPN incidents should be resolved in a timely manner to reduce potential security issues, including unsecure user work arounds and lost work time while waiting for an issue to be fixed.

Recommendations

- Create a written policy or procedure that provide directions to Clark County IT employees for actions to take when tickets are assigned to them. Include inactivity alerts to ensure that the tickets are addressed according to target response times.
- Review the target response times to ensure they meet current business needs.
- Create an additional priority for items that are low priority and require longer than the current priority 3 response time to minimize inactivity alert fatigue.

Management Response

CCIT is reviewing and will update processes related to incident and problem management. An additional priority level for lowest-level priority incidents will be created. Training and ongoing monitoring of incident response will be provided to all employees that are assigned incident tickets.

Finding #7 - Backup Data for VPN Applications Should be Tested Periodically

During our testing, we found that while Clark County IT has a detailed recovery process for recovering and restoring a server, they do not have a process in place to test the backup.

The IT department does not feel additional testing is necessary, as they occasionally need to restore from the backups and have not had any issues doing this in the past. They also regularly use the files in the backup application to

restore other non-VPN servers and have a redundant server in place.

CIS Control 11.5 requires organizations to test backup and recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.

If VPN services have issues and require restoration from backup files, and the backup fails, then the VPN service would be interrupted for an extended period.

Recommendation

Implement a procedure to ensure backups are tested or used for recovery at least quarterly or conduct a risk analysis to determine that it is not needed.

Management Response

CCIT will conduct a risk analysis and review and update the backup and recovery protocols for the VPN service and services / appliances and include testing of the backups on a basis that conforms to CIS Control 11.5.

Appendix A: Audit Scope, Methodology, and GAGAS Compliance

Scope

The audit covered the period from July 1, 2023, through June 30, 2024. We considered processes in place as of May 1, 2025. The last day of field work was May 5, 2025.

Methodology

To accomplish our objectives, we performed the following procedures:

- Completed a walkthrough of the VPN application and obtained information from creating to disabling of a user.
- Obtained evidence of the encryption used for the VPN application.
- Reviewed the authentication process of users when connecting to the VPN.
- Reviewed access control of the VPN account by comparing active accounts with deactivation reports.
- Reviewed policies and procedures that are applicable to VPN application.
- Discussed and obtained evidence of security controls that are used for the VPN application.
- Discussed and obtained information regarding VPN logs used by Clark County.
- Reviewed overall governance of the VPN programs.
- Sampled service desk tickets to ensure VPN related tickets are resolved within the established timeframe.
- Compared existing client controls of the VPN client to industry standards.
- Interviewed and held meetings with staff of the VPN application for clarification.

While some samples selected were not statistically relevant, we believe they are sufficient to provide findings for the population as a whole.

Our review included an assessment of internal controls in the audited areas. Any significant findings related to internal control are included in the detailed results.

Standards Statement

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Our department is independent per the GAGAS requirements for internal auditors.

[i] per NRS 603A.210. NRS 603A.210 states, "If a data collector is a governmental agency and maintains records which contain personal information of a resident of this State, the data collector shall, to the extent practicable,

with respect to the collection, dissemination and maintenance of those records, comply with the current version of the CIS Controls as published by the Center for Internet Security, Inc. or its successor organization, or corresponding standards adopted by the National Institute of Standards and Technology of the United States Department of Commerce."

[ii] per NRS 603A.210. NRS 603A.210 states, "If a data collector is a governmental agency and maintains records which contain personal information of a resident of this State, the data collector shall, to the extent practicable, with respect to the collection, dissemination and maintenance of those records, comply with the current version of the CIS Controls as published by the Center for Internet Security, Inc. or its successor organization, or corresponding standards adopted by the National Institute of Standards and Technology of the United States Department of Commerce."

[iii] Federal regulations for the performance of a risk assessment are outlined in the Administrative Safeguards of the HIPAA Security Rule, 45 CFR 164.308(a)(1)(ii)(A) which states:

§ 164.308 Administrative safeguards.
(a) A covered entity or business associate must, in accordance with § 164.306:
(ii) Implementation specifications:
(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.