togetherforbetter

AUDIT REPORT

Social Services Resolved Most of the Findings from the Original ACES Audit

January 2026

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

Social Services Resolved Most of the Findings from the Original ACES Audit

Audit Executive Summary

January 2026

Background

In July 2024, we audited Social Services' Automated Case Management Systems (ACES) application.

We identified the following six findings in the original audit report:

- ACES Audit logs should be Routinely Reviewed (High Risk).
- ACES Risk Assessment Is Not Being Performed (High Risk).
- Informal User Review Process Did Not Identify Accounts Needing to be Disabled (Medium Risk).
- ACES Disaster Recovery Procedures Do Not Include Testing or Training (Medium Risk).
- Approval Forms Were Completed after Permissions Were Provided (Low Risk).
- ACES Administrators Do Not Change Passwords Every 45 Days as Required by County Technology Directive (Low Risk).

Why We Did This Audit

We conducted this audit as a follow up to the original ACES to ensure corrective actions were implemented from the original findings.

Recommendations

Continue to work on completing and implementing a comprehensive disaster recovery plan to include testing and documentation of results.

togetherforbetter

What We Found

We found that 5 of the 6 original audit findings were fully resolved. Social Services completed the following:

- Performed an annual risk assessment.
- Implemented a log review process.
- Updated policies and procedures to include account review.
- Permissions were granted only when going through standard procedures and generic accounts approved by CCIT.
- Administrator password requirements were changed to reflect Clark County Technology Directive No.1.

One finding was not resolved. Social Services is still working on completing the disaster recovery plan.

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

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/audit/Pages/AuditReports.aspx

Table of Contents

Background 4
Objective 4
Conclusions 5
Outstanding Findings 7
ACES Disaster Recovery Procedures Do Not Include Testing or Training. 7
Appendix A: Audit Scope, Methodology, and GAGAS Compliance 9

Background

In July of 2024, we audited Social Services' Automated Case Management Systems (ACES) application.

We identified the following six findings in the original audit report:

- ACES Audit logs should be Routinely Reviewed. In the original audit, we found Social Services did not generate and review ACES audit logs on a regular basis. Security audit logs were used as needed, but the department had not developed a formal review plan or strategy. (High Risk).

- ACES Risk Assessment Is Not Being Performed. Previously, a periodic security risk assessment over the ACES software application was not being performed. (High Risk).

- Informal User Review Process Did Not Identify Accounts Needing to be Disabled. In the original audit, we found Social Services was performing an informal quarterly review of the active accounts within the ACES software application. However, we were unable to obtain documentation of the process, and accounts that should have been disabled were still active. (Medium Risk).

- ACES Disaster Recovery Procedures Do Not Include Testing or Training. In the original audit, Social Services had an informal business contingency plan, however there was no formal testing or training of the plan, nor was there formal testing of the backups. (Medium Risk).

- Approval Forms Were Completed after Permissions Were Provided. In the original audit, we found that for some accounts with elevated privileges, approval forms were completed after the user was granted access (Low Risk);

- ACES Administrators Do Not Change Passwords Every 45 Days as Required by County Technology Directive. All users followed the same requirement to change passwords every 90 days. Users with administrative rights were not required to change more frequently. (Low Risk).

Objective

The objective of this audit was to determine whether corrective actions were implemented to address the finding conditions identified in the original audit.

Conclusions

Clark County Social Services corrected five out of six findings, with the remaining finding being a work in progress.

Social Services and corresponding departments implemented the following corrective actions:

- Created and performed an annual risk assessment., The risk assessment contained vulnerabilities and threats as well as corresponding mitigating controls.
- Created and implemented a log review procedure. This included the review of high-risk transaction logs.
- Updated and implemented user account and user access policies and procedures to include periodic review of users and administrator accounts.,
- Security exception forms for generic accounts were submitted and are approved annually by the Information Technology Department.
- Implemented and updated user access policies and procedures for new and departing staff. The new process ensures access permissions are approved prior to being granted.
- Password requirements were changed to reflect the requirements of Clark County Technology Directive No.1.

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.

See Appendix A for additional details on work performed.

5 of 6 Original Audit Findings Have Been Fully Resolved

2 of 2 High Risk Findings Fully Resolved

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

1 of 2 Medium Risk Findings Fully Resolved

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.

2 of 2 Low Risk Findings Fully Resolved

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.

Outstanding Findings

ACES Disaster Recovery Procedures Do Not Include Testing or Training.

Corrective Action Status: **Work in progress**

In the original audit, Social Services had an informal business contingency plan. The plan provides steps to take in the event of an unplanned incident and is centered around procedures to recover data in the event of a disaster and processes to continue serving program participants offline.

Part of the disaster recovery process includes utilizing a backup of the ACES application. The ACES application data is routinely backed up and retained for several weeks. Although the data is backed up, there is no formal testing of the backup image.

As of the time of our follow up work, Social Services is in the process of creating a Business Contingency Plan. They met with Finance to understand the requirements needed from them in the event that ACES is unavailable.

The Information Technology Department is in the process of developing one for enterprise-wide applications. As part of this effort, a form disaster recovery plan. They will conduct a risk analysis and review and update the backup and recovery protocols for the ACES application. This will include implementing periodic backup testing in alignment with CIS Control 11.5, with documented results.

The HIPAA Security Rule addresses disaster and contingency plans. Administrative Safeguards of the HIPAA Security Rule, 45 CFR 164.308(A)(7)(i) states:

§ 164.308 Administrative safeguards.
(a) A covered entity or business associate must, in accordance with § 164.306:

> (7) (i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

Lack of written documentation on all facets of the business contingency plan could result in increased time to reestablish essential business functions during an unplanned disaster.

Lack of training and testing of the business contingency plan could result in staff not knowing their roles and responsibilities

in the event of a disaster. Both of these could result in violations to HIPAA and civil monetary penalties.

Recommendation

Continue to work on completing and implementing a comprehensive disaster recovery plan to include testing and documentation of results.

Appendix A: Audit Scope, Methodology, and GAGAS Compliance

Scope

The follow up audit covered the period from October 1, 2024, through October 31, 2025. The last day of field work was November 21, 2025.

Methodology

To accomplish our objectives, we interviewed staff and management from Social Services to obtain the status of the findings included in the original audit. We then performed the following procedures:

- Obtained and reviewed their risk assessment questionnaire as well as the completed risk assessment to ensure it is adequately addressing various threat scenarios, risk scoring and mitigating controls.
- Obtained and reviewed procedures provided related to reviewing logged security related events.
- Obtained Social Services monthly high risk reports from October 2024 to October 2025 and cross referenced the monthly reports to the department completed review workpapers ensure all high risk transactions were reviewed.
- Obtained user access policies and procedures and verified that periodic review of active accounts requirement was added.
- Confirmed that monthly administrative user access reviews were performed and an periodic review of active user was done.
- Obtained a list of active accounts, identified generic users, and ensured related security forms for those generic user accounts were submitted and approved by Information Technology.
- Obtained and reviewed the user rights dictionary and list of active users with their current permissions. We tested access for a judgmental sample of 25 of the current active users.
- We discussed and obtained evidence of change to the password change requirement to 45 days submitted by Social Services and completion of the request by Information Technology.

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.