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

Audit Department
January 2026

togetherforbetter

Background

In July 2024, we audited Social Services' Automated Case Management System (ACES) application. We identified the following six findings:

- 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).

Objectives

We conducted this audit to determine whether Social Services implemented corrective actions to resolve the original audit findings.

Conclusion

5 out of the 6 findings from the original audit were fully resolved, with the remaining finding being a work in progress.

To address the findings, Social Services completed the following:

- Performed an annual risk assessment.
- Implemented a log review process.
- Updated policies and procedures to include account review.
- Granted access permissions only when going through standard procedures and obtained IT approval for generic accounts.
- Changed administrator password requirements to reflect Clark County Technology Directive No.1.

Corrective Action Status

Original Audit Finding	Status
ACES Audit logs should be Routinely Reviewed. (High Risk) 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.	**Fully Resolved** – Social Services created and implemented a log review procedure. This includes the review of high-risk transaction logs.

Corrective Action Status

Original Audit Finding	Status
ACES Risk Assessment Is Not Being Performed. (High Risk) In the original audit, we found a periodic security risk assessment over the ACES software application was not being performed.	**Fully Resolved** – Social Services created and performed an annual risk assessment. The risk assessment contained vulnerabilities and threats as well as corresponding mitigating controls

Corrective Action Status

Original Audit Finding	Status
Informal User Review Process Did Not Identify Accounts Needing to be Disabled. (Medium Risk). 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 account review process, and accounts that should have been disabled were still active.	**Fully Resolved** – Social Services updated and implemented user account and user access policies and procedures to include a periodic review of users and administrator accounts. Security exception forms for generic accounts were submitted and are approved annually by the Information Technology Department

Corrective Action Status

Original Audit Finding	Status
ACES Disaster Recovery Procedures Do Not Include Testing or Training. (Medium Risk) 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.	**Work in Progress** – Social Services is in the process of creating a Business Contingency Plan. The Information Technology Department currently does not have a formal disaster recovery plan and is in the process of developing one for enterprise-wide applications. As part of this effort, 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.

Corrective Action Status

Original Audit Finding	Status
Approval Forms Were Completed after Permissions Were Provided. (Low Risk) In the original audit, we found that for some accounts with elevated privileges, approval forms were completed after the user was granted access	**Fully Resolved** – Social Services 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

Corrective Action Status

Original Audit Finding	Status
ACES Administrators Do Not Change Passwords Every 45 Days as Required by County Technology Directive. (Low Risk) All users followed the same requirement to change passwords every 90 days. Users with administrative rights were not required to change more frequently	**Fully Resolved** – Password requirements were changed to reflect the requirements of Clark County Technology Directive No.1

togetherforbetter