COMBINED HEALTH INFORMATION AND MONTANA ELIGIBILITY SYSTEM

DEPARTMENT OF PUBLIC HEALTH AND HUMAN SERVICES

MAY 2025

24DP-02

System Security and Reliability Audit

Fraud Hotline
(Statewide)
1-800-222-4446
(in Helena)
444-4446
LADHotline@legmt.gov
www.montanafraud.gov

Information Technology Audits

Information Technology (IT) audits conducted by the Legislative Audit Division are designed to assess controls in an IT environment. IT controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. We conducted this IT audit in accordance with generally accepted government auditing standards. 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 finding and conclusions based on our audit objectives. Members of the IT audit staff hold degrees in disciplines appropriate to the audit process.

IT audits are performed as stand-alone audits of IT controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee, which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

Respectfully submitted,

/s/ Angus Maciver

Angus Maciver, Legislative Auditor

Audit Staff

Miki Cestnik, CISA CRISC Shaina Geubtner, SSCP

Reports can be found in electronic format at:
https://leg.mt.gov/lad/audit-reports

Montana Legislative Audit Division

Security and Reliability Audit

A report to the Montana Legislature

Angus Maciver, Legislative Auditor

Background

CHIMES manages eligibility for Medicaid, Healthy Montana Kids, SNAP, TANF, and LIHEAP, serving about 300,000 recipients with $15 million in monthly benefits. Operated by the DPHHS Human and Community Services Division, CHIMES centralizes client data and automates eligibility decisions, supporting over 400 employees in 19 offices. Given the sensitive personal data it handles, strong security is essential.

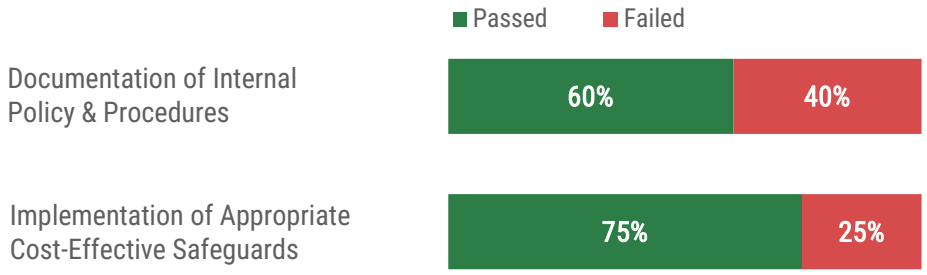
CHIMES is a commercial off-the-shelf (COTS) product provided by a vendor, configured to fit the department's needs. The State Information Technology Services Division (SITSD) provides infrastructure support for CHIMES while the vendor performs system maintenance, necessitating shared security responsibilities. The DPHHS is also overseen by the Centers for Medicare and Medicaid Services (CMS), so CHIMES must comply with Medicaid Management Information System (MMIS) regulations.

Combined Health Information and Montana Eligibility System

The Department of Public Health and Human Services (DPHHS, department) is responsible for the control environment of the Combined Health Information and Montana Eligibility System (CHIMES). While they are managing the environment well, we identified some opportunities for improvement. To improve, the department needs to formalize and adopt internal IT control policy and procedures and develop documentation to support effective control activity. The figure below summarizes testing across two key areas that form the foundation of the control environment, encompassing the standards, structures, and processes essential for effective internal control.

Figure 1

The Department needs to formalize and adopt internal IT control policy and procedures and develop documentation to support effective control activity.



Source: Compiled by the Legislative Audit Division.

What We Did

The objective of security and reliability audits is to evaluate whether systems operate within a controlled environment that enhances their security and reliability. Our assessment was based on the data security responsibilities outlined in §2-15-114, MCA, and the IT security policy established by SITSD with the Department of Administration (DOA). CHIMES must also comply with MMIS regulations enforced by the CMS. These regulations and state IT policy are based on industry standards. However, state policy has some minor differences.

Because of the extensive number of standards for CHIMES, not all of them were reviewed during our audit. The system handles sensitive data and complex processes, with control responsibilities shared between the DPHHS, SITSD, and the vendor. As a result, the highest-risk areas involve foundational security and ensuring the reliability of data used for eligibility decisions. Other control areas may be assessed in future audits through our risk-based approach. The specific control areas within the scope of our audit are further defined in Table 1.

Table 1
Control Areas Within Scope

Control Areas	Abbreviation	Description
Access Control	AC	Determines when and how users can access the system and their level of access.
Audit & Accountability	AU	Comprises controls related to department and system audit capabilities for user accountability.
Configuration Management	CM	Determines baseline configurations and controls future changes to the system.
Contingency Planning	CP	Develops a plan in the event that an incident that disrupts services should occur.

Source: Compiled by the Legislative Audit Division.

Our testing methods included interviewing department personnel, reviewing system security plans, policy and procedure, and evaluating supporting evidence of processes. Our review for this audit also included a detailed review of user access lists and audit log information to verify the processes are effective.

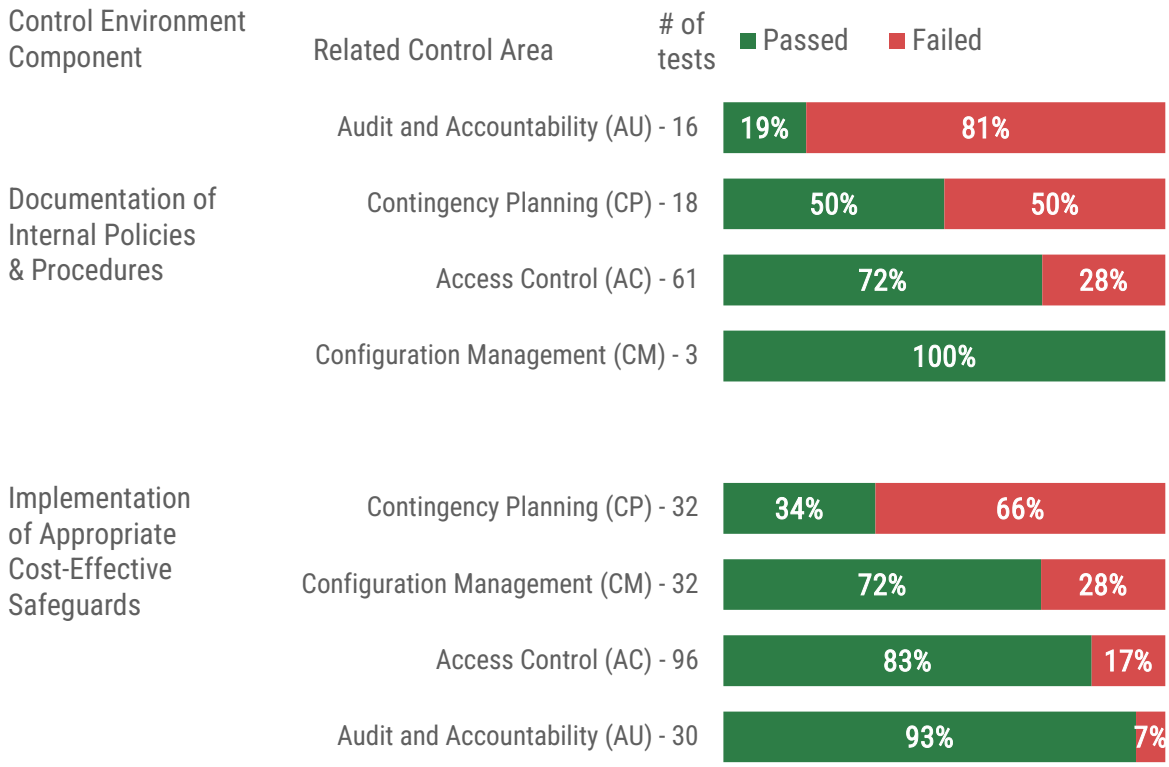
What We Found

Each of the four safeguard areas we tested for effective control design and internal policy and procedure present opportunities for improvement. Figure 2 (page 3) summarizes our audit testing across each area of the control environment.

Figure 2

Report Card:

While the Department implements most safeguards, there is an opportunity to improve the supporting documentation for safeguards and related internal policies and procedures.



Source: Compiled by the Legislative Audit Division.

The Department Relies on the Limited Policy and Procedures Established in State Policy by SITSD

The DPHHS has limited policies and procedures related to the control areas tested. Instead, it relies on state security policy and other standards required by the state. It had some policies and procedures specific to Access Control (AC). However, these only applied to a few safeguards within the AC area.

In 2022, state policy security requirements were updated. The updated language in state policy provides some guidance and understanding but does not identify system-specific aspects important for agencies to manage their systems properly. State policy indicates that agencies can develop policies and procedures for individual systems. Therefore, the department should address the decisions and procedures specific to its systems through its own policy and procedure documentation.

The Department Requires Supporting Documentation and Improved Management for Control Areas

CHIMES is missing supporting documentation and a complete internal assessment with specific state standards. Supporting documentation refers to additional details of how to operate or monitor the system and comprehensive management processes related to the system, like an Accounts Matrix, an Auditable Events Matrix, and a Contingency Plan. Each of these documents are intended to be used by department staff to complete duties such as comprehensive access reviews, event monitoring activities, and contingency plan training. We also identified that while CHIMES uses a CMS-provided template for its system security plan (SSP) to maintain federal compliance, it fails to identify and address state-specific requirements as part of internal system assessments.

Impact

Policies and procedures are essential to ensure organizational systems function effectively, regardless of staff changes. They provide clear, consistent instructions for implementing safeguards, reducing reliance on institutional knowledge and mitigating the risk of losing critical expertise due to staff turnover.

Without a policy tailored to the department's environment, system-level requirements cannot be met. These policy requirements include identifying roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding the system. Each of these aspects are important to the CHIMES environment and the following were identified throughout our testing:

1. Identification of roles and responsibilities: There are various roles supporting CHIMES, and some procedures are responsibilities shared with SITSD and the vendor. It was difficult to clearly understand procedures and responsibilities throughout the audit because there was no clear understanding or documentation. With security consolidation on the horizon, this is even more important with more responsibility moving to SITSD, but accountability still stays with the system owner—the DPHHS.

2. Coordination among organizational entities: As mentioned above, significant coordination is necessary for procedures between the DPHHS offices, SITSD, the vendor, and the CMS.

3. Compliance: CHIMES has to comply with multiple standards. CMS requirements for federal funding and federal marketplace access, as well as state policy requirements, need to both be documented to identify gaps in compliance when implementing controls to meet either standard. With federal requirements being priority for security staff, we identified some state safeguards that are not part of the DPHHS's internal assessment throughout all control areas. This was most notable in the configuration management area. Without being part of this assessment, these state-required safeguards are not managed appropriately.

The absence of robust policies and procedures presents a challenge to staff understanding and implementing safeguards effectively. During our review, we found that a review of user privileges is not included in periodic access reviews, auditable event types for the system are not documented and reviewed annually for appropriateness, and contingency plan evidence for the system is not mature enough to adequately train staff charged with responsibility in this area. While the majority of safeguards tested passed, reducing the risk of security concerns, the issues we identified can become significant if left unaddressed.

Improvement Opportunity

The DPHHS has experienced ongoing challenges in maintaining sufficient staffing to manage all components of a comprehensive security program for its many systems. Although the department has budgeted for three dedicated positions, it has not been able to fill all of them consistently. Since June 2024, some of these positions have been intentionally kept vacant to support consolidation efforts with SITSD. As a result, one or two staff members have been responsible for handling security tasks across multiple systems.

In response to limited resources and ongoing changes in state policy, agency staff have focused on the implementation of safeguards. These safeguards are documented and managed using system security plan templates provided by CMS, with quarterly reporting to CMS to ensure continued federal compliance. Therefore, the department still relies on security policy developed by SITSD.

At the time of our audit, SITSD was updating state security policy, and the DPHHS was participating in workshops to prepare for a consolidation of responsibilities with SITSD. The goal of this initiative is to improve overall security by centralizing resources within SITSD. However, the transition is still underway, and key details about roles and responsibilities have yet to be finalized.

For the DPHHS, the transition involves a broader range of security functions than other agencies that are consolidating risk management tasks. At the time of our review, it was unclear who would be responsible for specific activities and documentation. However, as the system owner, the DPHHS will remain accountable for certain parts of its security program. Our recommendations highlight the need for clear coordination with SITSD to ensure successful implementation.

The Department Needs To Identify and Develop Department and System-Specific Documentation

The department must define roles and responsibilities through system-specific policies and procedures and document system safeguards. System-specific policies and procedures facilitate the implementation of cost-effective safeguards. This clarity will make controls more effective as well as ensure compliance with CMS and state policy requirements. Often when multiple compliance requirements exist, policy needs to be supplemented with a compliance matrix or some type of comparison of various requirements to ensure that there is an awareness and intentional decision about gaps in compliance when implementing controls.

Recommendation #1

We recommend the Department of Public Health and Human Services coordinate with the State Information Technology Services Division to ensure:

A. A review of CMS and state policy is completed to identify additional standards required by state policy and document, through internal policy, the decisions about which standard to implement, and

B. Areas where system-specific policies and procedures are identified, developed, and implemented, where necessary.

The Department Has Implemented Most of the Cost-Effective Safeguards We Tested

The DPHHS has successfully met 142 of 190 applicable safeguard test requirements, achieving an overall pass rate of 75 percent. The Access Control, Audit and Accountability, Configuration Management, and Contingency Planning control areas had findings regarding area-specific supporting documentation and related process requirements. The findings within the Configuration Management control area were largely due to limited control documentation that did not recognize state standards. They can be addressed through a review of CMS and state policy, discussed in Recommendation 1.

The Department Needs To Complete the Development of an Accounts Matrix and Include the Review of User Privileges in Access Reviews

While the department conducts routine access reviews, they do not ensure users have appropriate access and privileges. This is hard to do without a clear picture of these attributes outlined within a defined Accounts Matrix. User access reviews are intended to ensure a separation of duties between users and enforce the principle of least privilege. Separation of duties is the concept that no user has enough permissions to misuse the system on their own. At the same time, the principle of least privilege ensures that users have minimal access to complete their duties as assigned.

Audit work found that some privileged business users had elevated security permissions and that some staff who had moved into new roles still retained access that no longer aligned with their current responsibilities. These findings highlight an opportunity for improvement by incorporating user privilege reviews as part of the regular user access review process.

An Accounts Matrix would ideally incorporate the business decisions and safeguards related to least privilege and separation of duties. It can be used to verify which user permissions are appropriate during review.

Recommendation #2

We recommend the Department of Public Health and Human Services:

A. Complete the formal development of an Accounts Matrix for CHIMES, and

B. Include the review of user permissions to improve routine access reviews.

The Department Needs To Develop an Auditable Events Matrix and Implement a Review Process for Event Types

An Auditable Events Matrix helps organizations identify key system events and set up alerts and notifications supporting effective risk management and security controls. While the department has a process for monitoring alerts and notifications, it lacks a fully developed matrix outlining all details for auditable events.

To be effective, the matrix should include justifications for why specific events are logged and describe how each event is audited. Although some audit alerts are documented, they are not consistently reviewed to ensure they remain appropriate as the system evolves.

Without a complete Auditable Events Matrix and regular reviews of event types, the department risks maintaining consistent oversight of system activities. As systems are updated or changed, this matrix must be updated to ensure new events are identified and current events are still logged in a manner that ensures integrity.

Recommendation #3

We recommend the Department of Public Health and Human Services:

A. Coordinate with SITSD to identify and document responsibilities for maintaining the Auditable Events Matrix and activities related to audit and accountability, and

B. Ensure the development of an Auditable Events Matrix for CHIMES is completed and a process to review event types, alerts, and notifications for appropriateness annually is implemented.

The Department Needs To Complete the Development of an Information System Contingency Plan and Implement Appropriate Contingency Plan Training

A system-specific contingency plan is designed to guide the efficient restoration of critical services in the event of disruption. While the department provided some evidence of core contingency planning activities, the current process lacks the detail needed to support effective recovery, coordination, and clarity around roles, responsibilities, and required resources. For example, staff must understand which events would trigger the contingency plan and know how to reach key recovery personnel. Without this information clearly outlined in a system-specific plan, staff may not recognize when to take action. This uncertainty can lead to delayed incident response, extended downtime, and greater disruption to business operations.

Given the department reliance on SITSD services and vendor partnerships, responsibility for contingency planning is shared across multiple entities. As security functions consolidate under SITSD, clearly defining who is responsible for developing and managing the contingency plan will ensure it is complete and effective.

Recommendation #4

We recommend that the Department of Public Health and Human Services coordinate with the State Information Technology Services Division to identify responsibilities and gather comprehensive information to:

A. Develop and formalize a complete information system contingency plan for CHIMES, and

B. Implement training for users assigned with contingency plan roles and responsibilities.

DEPARTMENT RESPONSE

DEPARTMENT OF PUBLIC HEALTH AND HUMAN SERVICES

GREG GIANFORTE
GOVERNOR

DEPARTMENT OF
PUBLIC HEALTH &
HUMAN SERVICES

CHARLIE BRERETON
DIRECTOR

May 21, 2025

Angus Maciver Legislative
Auditor Legislative Audit
Division PO Box 201705
Helena, MT 59620

Re: 24DP-02 Combined Health Information and Montana Eligibility System (CHIMES) Security and Reliability Audit

Dear Mr. Maciver,

The Department of Public Health & Human Services (DPHHS) has reviewed the CHIMES Security and Reliability audit report. DPHHS thanks your staff for their review. Our responses to LAD's recommendations are as follows:

Recommendation #1
We recommend the Department of Public Health & Human Services coordinate with the State Information Technology Services Division to ensure:

A. A review of CMS and state policy is completed to identify additional standards required by state policy and document, through internal policy, the decisions about which standard to implement, and
B. Areas where system specific policies and procedures are identified, developed, and implemented, where necessary.

Response:
Concur. The department will coordinate with the State Information Technology Services Division (SITSD) and believes recommendations will be implemented within the next 12 months. SITSD is still working on finalizing the adopted State Information Security Policies to be reviewed for implementation by the agency.

System-specific policies and procedures will be completed within the next 12 months, following the review of State Information Security Policies to determine agency implementation.

Recommendation #2
We recommend the Department of Public Health & Human Services:

A. Complete the formal development of an Accounts Matrix for CHIMES, and
B. Include the review of user permissions to improve routine access reviews.

Response:
Concur. The department has begun addressing these findings. The Human and Community Services Division (HCSD) Systems Security Unit is working on a CHIMES Accounts Matrix, which will include CHIMES Primary Office and Job Types mapped to CHIMES Role Names, along with the permissions (business functions) associated with each role. The Accounts Matrix is expected to be completed by September 30, 2025. The business process, CHIMES EA Quarterly User Review, will also be updated to include utilizing the Accounts Matrix to review user permissions during regular access reviews by September 30, 2025.

Recommendation #3
We recommend the Department of Public Health & Human Services:

A. Coordinate with SITSD to identify and document responsibilities for maintaining the Auditable Events Matrix and activities related to audit and accountability, and
B. Ensure the development of an Auditable Events Matrix for CHIMES is completed and a process to review event types, alerts, and notifications for appropriateness annually is implemented.

Response:
Concur. The department will coordinate with SITSD and NSU to ensure that the Auditable Events Matrix is defined in policies and procedures, with the review of the current security consolidation RACI defining responsibilities for activities related to the matrix.

A specific document for the Auditable Events Matrix will be created for CHIMES, to be reviewed annually, with an estimated implementation date in early 2026.

Recommendation #4
We recommend the Department of Public Health & Human Services coordinate with the State Information Technology Services Division to identify responsibilities and gather comprehensive information to:

A. Develop and formalize a complete information system contingency plan for CHIMES, and
B. Implement training for users assigned with contingency plan roles and responsibilities.

Response:
Concur. The department will complete a fully executable ISCP for CHIMES. This has already begun but still requires the participation of SITSD in their role within the plan.

Once the RACI review and full security consolidation have been completed to define various responsibilities related to the ISCP, the plan can be finalized, and formal testing with appropriate stakeholders can be conducted.

Sincerely,

Signed by:
Charles T. Brereton
F85D511C51B4408...

Charles T. Brereton
Director