MEDICAID ENTERPRISE SYSTEM

DEPARTMENT OF PUBLIC HEALTH AND HUMAN SERVICES

JANUARY 2025

24DP-03

System Security and Reliability Audit

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
Hunter McClure
Shaina Geubtner

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

MONTANA LEGISLATIVE AUDIT DIVISION

SYSTEM SECURITY AND RELIABILITY AUDIT

A report to the Montana Legislature

Angus Maciver, Legislative Auditor

Background

Medicaid is a joint federal and state program that provides healthcare coverage to eligible low-income individuals and families, ensuring access to essential medical services.

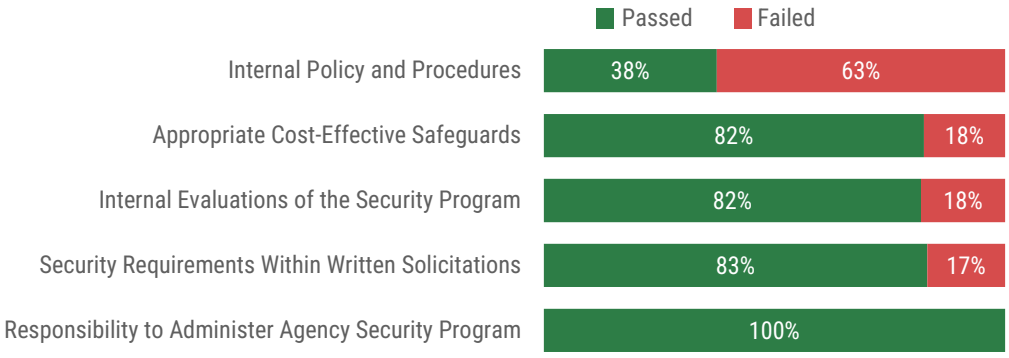
Montana's Medicaid Enterprise System (MES) administers $2 billion annually for various related programs, like Medicaid and Children's Health Insurance Program (CHIP). DPHHS's Medicaid and Health Services Branch (MHSB) oversees the enrollment process, manages the distribution of benefits, and works closely with healthcare providers to deliver a range of medical services to over 200,000 Montana citizens. MES consists of 10 modules, of which two were included in the scope of this audit.

Medicaid Enterprise System

The Department of Public Health and Human Services (DPHHS) is improving the control environment for the Medicaid Enterprise System (MES). The figure below summarizes testing across five key areas that form the foundation of the control environment, encompassing the standards, structures, and processes essential for effective internal control.

Figure 1

DPHHS needs to formalize and adopt internal IT control policy and procedures and finish implementing their risk management process.



Source: Compiled by the Legislative Audit Division.

What We Did

The objective of security and reliability audits is to evaluate whether systems are operating 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 IT security policy established by the State Information Technology Services Division (SITSD) with the Department of Administration (DOA). State IT policy is based on industry standards; however, there are some minor differences.

Due to the extensive number of standards and various control environments for each module in MES, not all modules or security standards were reviewed. Our risk-based approach identified Medicaid Management Information Systems (MMIS) and FlexRx due to critical services and the majority of Medicaid activity. MMIS manages services for medical claims processing, while the FlexRx module manages pharmacy services.

Other modules not included:

- Financial Services
- Customer Care Services
- Care Management
- Claims Processing and Management Services
- Provider Services
- Data Warehouse
- Data Analytics
- Systems Integrator

Due to the personal information and important processes within these modules, high-risk control areas for these modules relate to foundational security controls, data reliability, and vendor control assurance practices. Other modules and control areas may be assessed in future audits through this 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.
Awareness & Training	AT	Security training, procedures, and training records.
Security Assessment & Authorization	CA	Cybersecurity assessments, authorizations, continuous monitoring, plan of actions and milestones, and system interconnections.
Configuration Management	CM	Baseline configuration, inventories, and a security impact analysis control.
Contingency Planning	CP	Contingency plan testing, updating, training, backups, and system reconstitution.
Identification & Authentication*	IA	Identification and authentication of system users.
Planning	PL	Security planning policies that address the purpose, scope, roles, responsibilities, management commitment, coordination among entities, and organizational compliance.
Risk Assessment	RA	Risk Assessment policies and vulnerability scanning capabilities.
System & Services Acquisition	SA	Management of the system development life cycle and contains information about documentation, configuration, development, and security testing controls.

* IA was only evaluated for MMIS. FlexRx controls in this area are the responsibility of the vendor, which is discussed in general as part of the agencies risk management program.

Source: Compiled by the Legislative Audit Division.

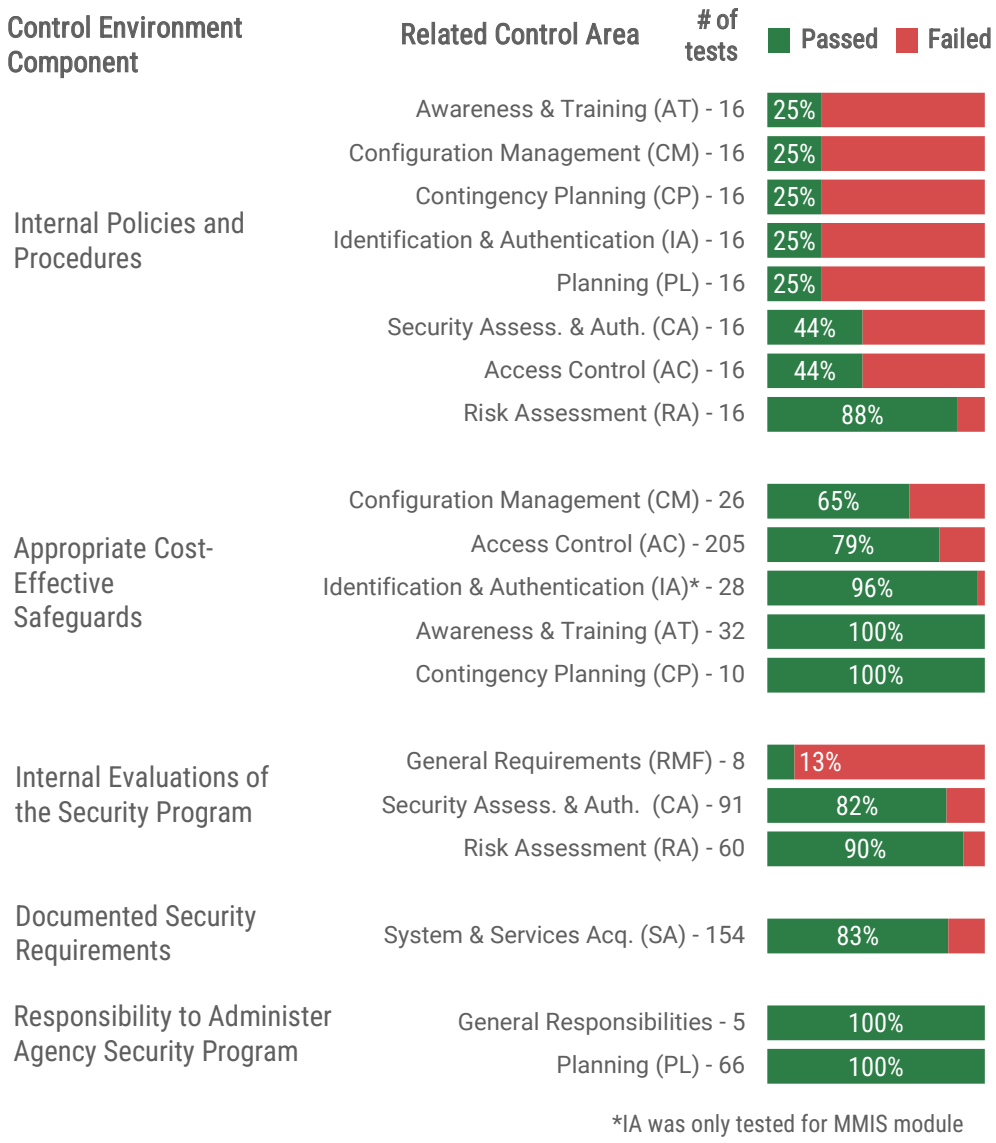
Our testing methods involved interviewing agency personnel, reviewing external audits, internal assessments, system security plans, and any available agency documentation. For this audit, we also assessed vendor system security documentation and policy to ensure it met the necessary standards for accuracy and thoroughness. Auditors also consulted with agency staff to understand how the tested standards were being implemented.

What We Found

Our audit focused on FlexRx and MMIS. The two modules have different control environments that were both assessed. There was no significant difference in results between the two modules, so testing results are combined below.

Figure 2

Report Card:
The test results highlight both notable progress and opportunities.



Source: Compiled by the Legislative Audit Division.

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

Over the course of the audit, we found that DPHHS has documentation related only to the Access Control (AC) and Risk Assessment (RA) areas. However, the agency mainly relies on the vendor and SITSD to provide all other documentation. In 2022, state policy security requirements were updated. When this occurred, SITSD replaced detailed policies with one to two sentence paragraphs describing the policy area instead. While these paragraphs provide some guidance and understanding, they are incomplete and do not meet policy requirements for individual systems at each agency. The agency needs to address the decisions and procedures specific to its systems through policy and procedure documentation.

Incomplete Risk Management Contributed to All Other Testing Failures

At the time of the audit, DPHHS had developed risk management procedures but had not implemented them. These procedures generally include the identification of risk, implementation of necessary controls, and monitoring of control effectiveness. Instead of these procedures, DPHHS relies on vendor documentation with limited verification of the information received. For example, updates to state policy and differences between state policy and the baseline industry standard were not identified in the vendor's materials and communicated to the vendor. Therefore, the control documentation provided by the vendor did not align with some areas of state policy. This means the agency does not have assurance of controls in those areas, which contributed to the failed tests in various areas.

Impact

Without policy and procedure, organizations rely on institutional knowledge to ensure foundational security practices are conducted, and more work is needed to transfer institutional knowledge as staffing changes. During the audit, we identified an inconsistent understanding of the control environment due to security staff changes. DPHHS has an increased risk of inconsistent IT application management, potentially leaving them vulnerable to security breaches.

This problem is exacerbated by an incomplete risk management process that should be identifying and monitoring controls. In MMIS and FlexRx's situation, the vendor is responsible for a majority of the controls. The risk management process should be used to help manage the vendor and gain assurance that controls are properly implemented. The vendor provided security documentation missed state policy control requirements in various areas, and after following up with the vendor, we identified the policies referenced by the vendor were out-of-date in some cases. Therefore, DPHHS does not adhere to state security requirements nor fully understand the risks and controls for FlexRx and MMIS.

Improvement Opportunity

When identifying why DPHHS has not implemented risk management for MES modules, it stated that staffing issues have impacted its ability to complete the program. Due to staffing concerns among multiple agencies, SITSD has started a security consolidation process across the enterprise to help alleviate this issue. DPHHS is currently going through workshops with SITSD and anticipates completing the risk management consolidation in 2025. However, other factors contribute to DPHHS's lack of documented policies and procedures and incomplete risk management process.

DPHHS Needs To Identify and Develop Agency and System Specific Documentation

DPHHS relies on SITSD to provide policies related to most areas we reviewed. SITSD is aware that the current policy does not meet state security requirements and is currently working to improve them. Through consolidation and updates to statewide policy, DPHHS can work with SITSD to ensure policy requirements are met, but it still needs to document its agency-specific procedures.

Recommendation #1

We recommend the Department of Public Health & Human Services:

A. Work with the State Information Technology Services Division to identify areas where system specific policy needs development,

B. Develop and implement system specific procedures, and

C. Formally adopt and supplement state IT control policy and procedures.

Changing Requirements and New Tools Require a Change to Risk Management

According to DPHHS, in the past, SITSD only required agencies to review vendor-provided audit reports as part of their risk management process. When state policy was updated in 2022, agencies were required to make significant changes and use a new tool to document and track all IT controls for a system.

With these changes in requirements occurring, DPHHS identified the need for specific procedures and additional policies in the risk management area. However, DPHHS has not reflected those changes in its contracts with the MMIS and FlexRx vendor. For example, documentation that DPHHS provided the vendor to give context to their security requirements is no longer used.

Turnover in security staff at DPHHS has slowed the implementation of the risk management procedures as well. There is currently one of three FTE filled in this area for the entire department. It is unclear how the outcome of the consolidation workshops will affect DPHHS's ability to fill these positions at this time. By working with SITSD through consolidation workshops and finishing the implementation of its risk management program, DPHHS will be able to update contract requirements and ensure that required controls are implemented by the vendor.

Recommendation #2

We recommend the Department of Public Health & Human Services:

A. Finish implementation of its risk management program and IT control management,

B. Update vendor contracts to reflect current security and risk assessment processes, and

C. Work with the State Information Technology Services to complete an evaluation of security staffing needs.

DEPARTMENT RESPONSE

DEPARTMENT OF PUBLIC HEALTH AND HUMAN SERVICES

GREG GIANFORTE
GOVERNOR

DEPARTMENT OF
PUBLIC HEALTH &
HUMAN SERVICES

CHARLIE BRERETON
DIRECTOR

January 21, 2025

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

RECEIVED
January 21, 2025
LEGISLATIVE AUDIT DIV.

Re: 24DP-03 Medicaid Enterprise System (MES) Security and Reliability Audit.

Dear Mr. Maciver,

The Department of Public Health & Human Services (DPHHS) has reviewed the MES 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:

A. Work with the State Information Technology Services Division to identify areas where system specific policy needs development,
B. Develop and implement system specific procedures, and
C. Formally adopt and supplement state IT control policy and procedures.

Response:
Concur. Efforts to remediate the recommendations are underway and will be ongoing until fully implemented. The department believes recommendations will be implemented within a year.

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

A. Finish implementation of its risk management program and IT control management,
B. Update vendor contracts to reflect current security and risk assessment processes, and
C. Work with the State Information Technology Services to complete an evaluation of security staffing needs.

Response:
Concur. The department has started to address these findings and expects to complete implementation within one year.

Sincerely,

Charles T. Brereton
Director