MONTANA UNEMPLOYMENT SERVICES ENVIRONMENT (MUSE)

DEPARTMENT OF LABOR & INDUSTRY

OCTOBER 2025

25DP-02

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, CISA, CRISC Gonzalo Nefi Lazalde

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

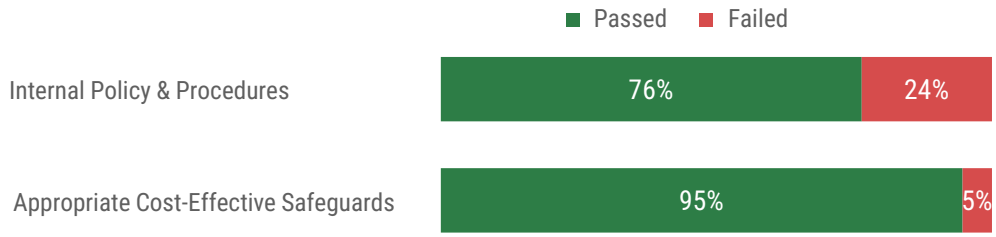
MUSE is the state's unemployment system, which manages unemployment claims, unemployment payments, tax calculations, tax contributions, and employer payments. MUSE is a commercial off-the-shelf solution that is highly configurable to the agency's needs. During the time of the audit, MUSE was hosted on the State Information Technology Services Division's (SITSD) infrastructure. However, towards the end of the audit, DLI was performing a cloud migration and is now fully on the cloud.

MUSE holds valuable information and shares data with 29 federal and state entities. In the 2024 fiscal year, $126,821,578 was paid out in benefits from the system, affecting 40,713 claimants and 54,848 employers. This system contains both federal tax information (FTI) and personally identifiable information (PII). Therefore, MUSE needs to be compliant with the Social Security Administration and IRS guidelines as well as state security requirements.

Montana Unemployment Services Environment

Over the past year, the Department of Labor & Industry (DLI, agency) has successfully maintained a strong control environment for the Montana Unemployment Services Environment (MUSE), even amid significant changes. The figure below highlights our testing across core areas—standards, structures, and processes that are critical to sustaining effective internal controls.

Figure 1



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. Our assessment was based on the data security responsibilities outlined in §2-15-114, MCA, and IT security policy established by the SITSD with the Department of Administration. State IT policy is based on industry standards; however, there are some minor differences.

Due to the extensive number of standards for MUSE, not all security standards were reviewed. Our risk-based approach identified that the system contained various types of sensitive information, including personally identifiable information and federal tax information. Due to the sensitive data and amount of money issued based on decisions managed by the system, high-risk control areas for MUSE relate to foundational security controls, data reliability, and vendor control assurance practices. If necessary, other system areas and control areas may be assessed in future audits through a similar approach. The specific control areas within the scope of our audit are defined in Table 1 (page 2).

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 and Accountability	AU	Log review, log updating, creating and retaining system logs and records, and providing individual system actions of users.
Configuration Management	CM	Baseline configuration, inventories, and a security impact analysis control.
System and Services Acquisition	SA	Management of the system development life cycle and contains information about documentation, configuration, development, and security testing controls.
System and Information Integrity	SI	Flaw remediation, malicious code detection, information systems monitoring, security alerts, software, firmware integrity, and spam protection.

Source: Compiled by the Legislative Audit Division.

Our testing methods involved interviewing agency personnel, evaluating system security plans and any available agency documentation, and system observations. For this audit, we interviewed vendor staff to clarify their responsibilities in joint processes with the agency.

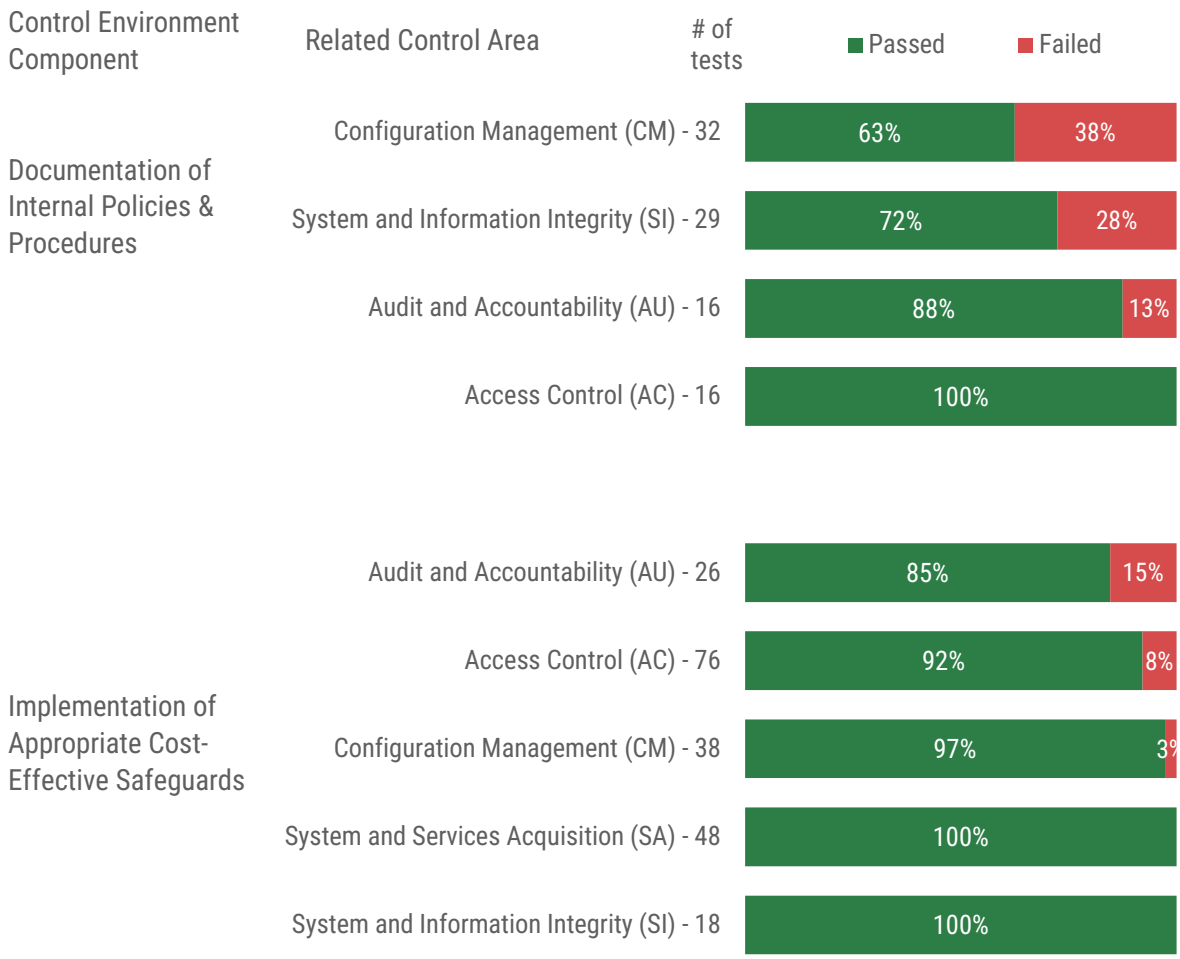
What We Found

Figure 2 (page 3) provides a summary of our audit testing across each area of the control environment.

Figure 2

Report Card:

Test results highlight notable progress and opportunity.



Source: Compiled by the Legislative Audit Division.

The Department of Labor & Industry Has Minor Improvements To Make

While the agency has system-specific policy and procedure, documentation was not standardized, and the criteria in each document varied greatly per document. Some documents were well thought out with all components necessary, while others were a collection of related procedures or missed certain aspects of the procedure. For example, Access Control met all criteria standards established by SITSD, but Configuration Management documentation was missing information on how the agency reviews and approves its setup each year.

The safeguard testing revealed issues within the MUSE environment. These shortcomings exposed vulnerabilities in key security areas, prompting the need for improvements in Access Control, Audit and Accountability, and Configuration Management. The following findings detail those gaps and the agency's initial steps toward resolution:

Access Control: Automation can be used by a system to send out alerts for user access changes to the system, increasing the likelihood of discovering anomalies. Automation for user management was not initially set up for MUSE. As the audit progressed, the agency set up automated monitoring alerts. However, conflicts of interest still need to be addressed. Additionally, DLI did not have a monthly review of information that was posted on a public-facing website.

Audit and Accountability: Initially, documentation for auditable events was vague, and did not fully incorporate the separate duties of the agency and vendor. As fieldwork progressed, documentation was expanded to reflect the necessary duties of the parties involved in managing MUSE.

Configuration Management: As discussed earlier, documentation of the review process was missing within procedures.

Impact

Internal safeguards and documentation are needed by systems to mitigate risk. These controls vary greatly from decisions and procedures to system configurations. While most of these controls were in place for the new system, the following two deficiencies are still significant to the MUSE environment.

Automated Account Monitoring: While user account audits do occur, not having automated notifications for account management can cause delays in investigations if an account is altered inappropriately.

Standardized Policy and Procedure: Without standardization, inconsistencies with requirements occur, which can ultimately lead to a degradation of controls and changes not being reflected in policy. The details required in policy and procedure are important to MUSE and DLI's operations, specifically for:

- Management of the MUSE system involves multiple entities—SITSD, DLI, and the vendor—each with distinct roles and responsibilities. Clearly defining and communicating these roles in a formal policy helps ensure all parties understand their obligations. This clarity is essential for consistent system oversight and accurate guidance for staff to follow.

- The Department of Labor & Industry must comply with control standards set by state requirements, IRS guidelines, and the Social Security Administration. The agency's policies and procedures should explicitly state which regulations apply and how existing controls meet these requirements. Without clear compliance guidance, DLI risks overlooking critical regulatory obligations, which could result in legal, financial, or reputational harm.

- The Montana Unemployment Services Environment has undergone several major changes, with responsibilities shifting among managing entities. When policies are not reviewed and updated in step with these changes, control gaps can emerge. To prevent such vulnerabilities, timely policy revisions must align with system updates and changes in oversight responsibilities.

Improvement Opportunity

The Department of Labor & Industry has undergone various changes with the transition to MUSE and the organizational changes to consolidate with SITSD. MUSE went live in October 2023. While the new system has brought new upgrades to the antiquated systems, major system updates require significant resources to ensure that a smooth transition occurs. With this upgrade, documentation referencing the older systems also needs to be updated to reflect changes to the environment.

The department has consolidated its security operations with the State Information Technology Services Division. As part of this transition, the department transferred its security staff to the state technology division. However, it still needed personnel to handle system-specific responsibilities, leading to the creation of a Security Coordinator position within the agency. This role is tasked with maintaining documentation and ensuring compliance with the multiple security standards under which the MUSE system is audited. As a result, the department has found itself in a fast-paced, reactive environment, continually adjusting to meet the demands of various auditing entities.

Standardization Will Improve DLI's Ability to Manage Change

Towards the end of our work, DLI was dealing with additional changes to the control environment. MUSE was in the process of being migrated into the cloud. While DLI did not have a standardized template at the beginning of the audit, a template was created and used by DLI for updating policies and procedures we reviewed in our work. These new documents do have the criteria that state policy requires. While the new documentation has followed the template, older internal policy and procedures still need to be reviewed and updated with the new template, and all documentation will need review to ensure the cloud environment changes are reflected in a timely manner.

Recommendation #1

We recommend the Department of Labor & Industry use a template when updating, creating, or reviewing their internal policies and procedures.

Improving Oversight and Accountability in Automated Alert Systems

During the audit process, the department responded constructively to feedback, initiating updates to safeguard controls as issues were identified. This proactive approach led to revisions in the Audit and Accountability documentation, ensuring it now reflects the full scope of implemented controls. The Configuration Management finding is addressed through recommendation one. With that addressed, account automation remains the primary opportunity for improving the department's control environment.

Currently, the MUSE system generates automated alerts that are delivered to staff via email. While these notifications serve a useful purpose, they are routed to the same personnel who manage user accounts. This overlap creates a potential conflict of interest, as those responsible for Access Control also monitor the alerts intended to flag suspicious activity. Although these individuals possess the necessary access and technical knowledge to manage the controls effectively, the absence of independent verification introduces a significant risk.

For example, a compromised security manager account could modify its own access or that of another user, receive the corresponding alert email, and delete it without oversight. This loophole mirrors tactics used by malicious actors, who often exploit email systems by creating rules that reroute automated alerts to trash folders or otherwise hide them from detection. To safeguard the integrity of the system, impartial oversight is essential. Implementing a layer of independent review ensures that alert notifications are received, preserved, and acted upon appropriately, strengthening accountability and reducing the risk of misuse. Without such checks, even well-intentioned systems remain vulnerable to manipulation. Independent oversight is not just a best practice—it is a necessary guardrail.

Recommendation #2

We recommend the Department of Labor & Industry identify and implement a process that reduces conflicts of interest in generated alerts from the system.

DEPARTMENT RESPONSE

DEPARTMENT OF LABOR & INDUSTRY

Montana Department of
LABOR & INDUSTRY

September 19, 2025

Angus Maciver, Legislative Auditor
Legislative Audit Division
Room, 160, State Capital
PO Box 201075
Helena, MT 59620-1705

RECEIVED
September 19, 2025
LEGISLATIVE AUDIT DIV.

Re: Department of Labor & Industry Response to Legislative Audit Division's *Montana Unemployment System Environment (MUSE) System Security and Reliability Audit (25DP-02).*

Dear Mr. Maciver;

The Department of Labor & Industry has reviewed the Montana Unemployment System Environment (MUSE) System Security and Reliability Audit and would like to thank your audit staff for their review. We welcome collaborative opportunities to improve the effectiveness of our programs in providing quality services to all Montanans. Our responses to the recommendations are as follows:

Recommendation #1

We recommend the Department of Labor & Industry use a template when updating, creating, or reviewing their internal policies and procedures.

DLI Response: Concur

Information security and data privacy remain top priorities for the Department. Following the partial merger of Information Security with the State Information Technology Services Division (SITSD), all security resources staff were transferred to SITSD. DLI leadership has since identified the need for additional resources to strengthen security. We hired an Information Security Coordinator into a new position. This new hire provides greater visibility into our systems, enables us to identify and address opportunities for improvement, and enhances collaboration with SITSD, vendors, and agency personnel to ensure identified needs for security enhancements are addressed and safeguards are implemented.

The Department recognized prior to this audit, the importance of policy standardization and timely updates. We remain committed to refining, aligning, and updating our policies with the Montana Baseline Security Standards (MT-BASE) and adapting them to the evolving risk landscape.

Montana Department of
LABOR & INDUSTRY

Recommendation #2

We recommend the Department of Labor & Industry identify and implement a process that reduces conflicts of interest in generated alerts from the system.

DLI Response: Concur

In working with our vendor, FAST Industries, the Department has implemented a new control to generate independent MUSE system alerts. Alerts which are sent to separate distribution groups which exclude initiators of system access control requests. These alerts are reviewed by the Information Security Coordinator, who does not have access to the MUSE environment, thereby ensuring impartial oversight. A formal Audit and Accountability Procedure for MUSE documents and governs this review process.

Respectfully,

Sarah Swanson, Commissioner
Montana Department of Labor and Industry