STATEWIDE ACCOUNTING, BUDGETING, AND HUMAN RESOURCES SYSTEM (SABHRS)

DEPARTMENT OF ADMINISTRATION

MARCH 2026

25DP-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, CISA, CRISC Shaina Geubtner, SSCP

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

Montana Legislative Audit Division

Security and Reliability Audit

A report to the Montana Legislature

Angus Maciver, Legislative Auditor

Background

The Statewide Accounting, Budgeting, and Human Resources System (SABHRS) is used by state agencies to report the disposition, use, and receipt of public resources and to assist in the administration of state human resource information. The Department of Administration's (DOA's) State Human Resources Division, State Financial Services Division, and State Information Technology Services Division (SITSD) share technical system operation and maintenance responsibilities. The system comprises various modules, including Financial (FS) and Human Resources (HR) applications, which work together closely. All state financial transactions and data for over 15,000 state employees flow through these applications.

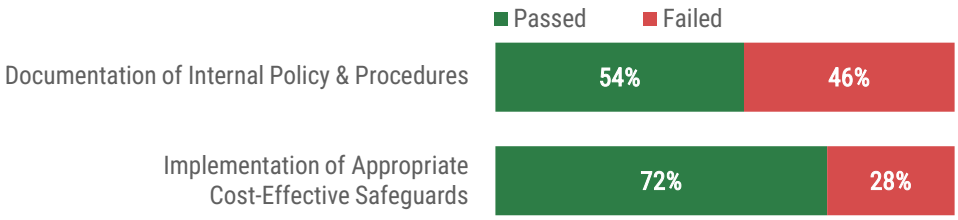
SABHRS utilizes a commercial product developed by a vendor and managed by the department for its operational needs. State Information Technology Services Division (SITSD) supports SABHRS infrastructure. This necessitates shared security responsibilities between SITSD and DOA.

Statewide Accounting, Budgeting, and Human Resources System (SABHRS)

The Department of Administration (DOA, department) manages the control environment for the Statewide Accounting, Budgeting, and Human Resources System, known as (SABHRS). While statewide centralization efforts are designed to streamline and strengthen operations, the department cannot lose sight of SABHRS' security and compliance requirements. Any lapse could disrupt daily functions and undermine confidence in the system, which serves nearly every state agency. The figure below summarizes testing across key areas that form the foundation of the control environment, highlighting 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 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 SITSD with the DOA. State IT policy is based on industry standards; however, there are some minor differences.

Due to the large number of standards for SABHRS, not all security standards were reviewed. SABHRS handles a large volume of state financial and employee data that is subject to financial audits. We determined that the highest-risk control areas for SABHRS involve foundational security controls and ensuring data reliability for stakeholders. Other 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.
Configuration Management	CM	Determines baseline configurations and controls future changes to the system.

Source: Compiled by the Legislative Audit Division.

Our testing methods involved interviewing agency personnel, reviewing security plans, policies, and procedures, and evaluating supporting evidence for processes. Our review for this audit also included a detailed review of user access and change management procedures.

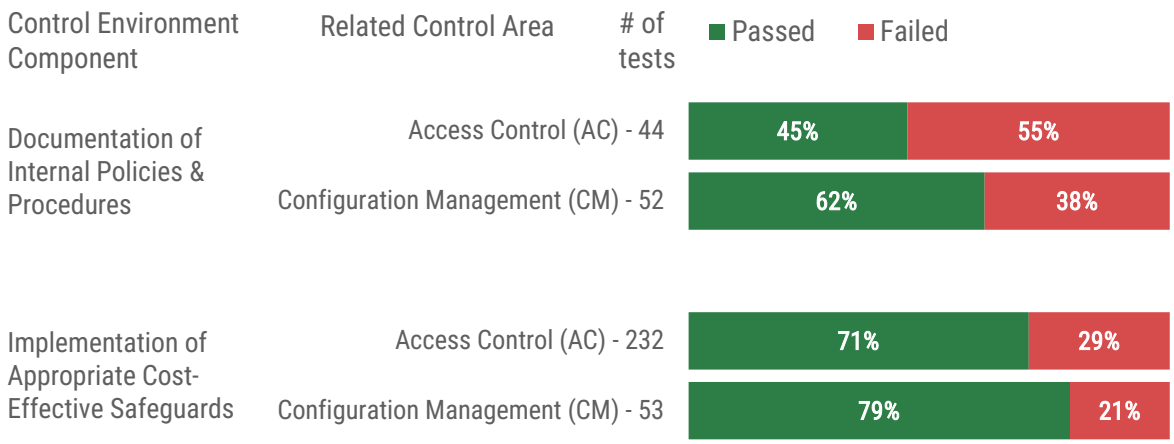
What We Found

The table below provides a more granular summary of our audit testing within the control environment, highlighting results for each control area tested.

Figure 2

Report Card:

The Department implements most appropriate cost-effective safeguards, but improvements in documentation of internal policies and procedures are needed.



Source: Compiled by the Legislative Audit Division.

The Department Lacks Effective System Documentation of the Design of Security Controls

While SABHRS HR and SABHRS FS operate within a single system, they are managed independently in certain areas due to distinct underlying processes. This separation has resulted in gaps in internal policies, procedures, and system documentation. Notably, SABHRS lacks a formal access control policy that covers both modules. In general, the policies and procedures governing these modules lack effective oversight, particularly regarding the responsibility of documentation and compliance with review frequency requirements.

Our audit testing identified notable deficiencies in Access Control and Configuration Management within the system:

- Gaps in system documentation defining account management, enforcement of least privilege, and system access controls.
- SABHRS HR requires the most improvement, with a less robust system security plan.
- Although staff perform key configuration management activities, they rely on institutional knowledge rather than documented procedures within a configuration management plan.

Impact

Well-defined policies, procedures, and system security documentation help ensure systems continue to operate effectively during personnel changes. Clear guidance on applying safeguards reduces reliance on individual expertise and preserves critical knowledge within the organization.

Assigning responsibility for each policy and procedure ensures proper development, documentation, dissemination, and regular review that aligns with state standards and best practices. Without this structure, organizations risk relying on outdated guidance that may not reflect current requirements. Incomplete or informal documentation increases dependence on institutional knowledge, which can be lost when key staff depart. This lack of formal documentation also raises the risk of process deterioration and unclear roles. Although our configuration management testing did not reveal immediate impacts from these issues, we did observe related concerns in account management.

For example, agency security account managers are responsible for ensuring appropriate user access within SABHRS, but the requirement that they perform regular reviews of roles assigned to agency-managed accounts is not documented. While the process for granting access is documented, account managers must also review whether users' roles remain necessary for their current business needs. Without this oversight, users may retain excessive access to certain functions and sensitive information, which violates the principle of least privilege.

As symptoms of these broader issues, our audit work found the following:

1. Nine users hold conflicting roles, allowing them to create and pay a vendor as well as create and approve vouchers. We also found that five users held conflicting travel and expense roles, giving them varying access levels to travel authorizations and expense reports, despite SABHRS FS documentation requiring separation of duties. Separation of duties must be in place to enforce accountability and maintain a system of checks and balances. Without this, the risk of fraud, errors, and misuse of the system increases. When reviewing these users' activity within the system, we did not find any evidence that users inappropriately used these roles.
2. A terminated employee still had access to privileged roles within the system. Effective user termination processes must be appropriately enforced to restrict unnecessary access to the system. Even though we verified that this user account had not been used after the termination date, the system is at risk of unauthorized access and misuse of dormant accounts without these measures.

These foundational security concepts limit access to only what is required for assigned responsibilities. Allowing unnecessary access increases the risk of unauthorized activity and the potential for misuse of critical system functions or sensitive information. Ultimately, without comprehensive and consistent system documentation that encompasses the entire SABHRS system, such gaps in security and accountability are much more likely to occur.

Improvement Opportunity

Prior audit work dating back to 2018 has shown that the Department has historically struggled with organizational challenges and frequent shifts in responsibilities affecting the management of system security and compliance for SABHRS. These issues have led to unclear accountability for maintaining system documentation and internal policies and procedures. The agency noted that a dedicated individual previously managed much of this documentation. However, after this individual's departure, the management and maintenance of system documentation stalled, and significant improvements have only begun recently.

For nearly ten years, audits have identified competing priorities and frequent changes in responsibilities hindering the agency's progress in integrating and enhancing internal policies and procedures for both SABHRS modules. However, ongoing consolidation efforts have increased coordination between DOA and SITSD, leading to recent improvements.

Internal Policy and Procedure Show Signs of Improvements

The department is working to improve its internal policies and procedures. However, documentation has become complex because the system was managed as two separate parts. Consolidating this material and fully understanding the control environment of a single system will require significant effort.

Much of this work is ongoing. The Department of Administration must further standardize its approach to strengthen internal controls and ensure consistent policies and procedures.

Recommendation #1

We recommend the Department of Administration:

A. Update and formalize the policies and procedures governing both SABHRS HR and FS to ensure comprehensive and consistent documentation across both systems; and

B. Clearly assign and document responsibility for the ongoing management, maintenance, and review within each system policy and procedure, ensuring system-wide control design consistency in compliance with state standards.

Improvements Are Necessary for Access Control Design and Implementation

System security documentation that is intended to design effective access control lacked several requirements. This misalignment with state requirements and best practices increases SABHRS's vulnerability to security threats, especially when documented controls and processes are outdated.

Both SABHRS HR and FS would benefit from updating their system security documentation and requirements for regular role reviews. This type of documentation is a critical component of effective management, particularly in areas such as financial reporting, compliance, risk, and internal controls. Without this documentation and understanding, it is harder to maintain consistency and manage controls. Additionally, security tools and functions within the system may be underutilized, such as data masking. While FS uses data masking for a specific field, HR does not use the functionality for sensitive information. Thorough control documentation would provide a better basis to analyze whether this functionality should be used in addition to role-based access to limit access to information.

As noted with internal policy and procedure, the agency has recognized these areas of improvement and has begun taking action to correct issues, such as improving access termination processes and exploring options to protect the visibility of sensitive data. As the agency works to remediate these issues, reviewing and updating system documentation and requirements will be essential in addressing underlying access control problems.

Recommendation #2

We recommend the Department of Administration:

A. Update and formalize system security documentation applying to both SABHRS HR and FS to ensure comprehensive and consistent documentation across both systems; and

B. Formalize the review requirement for Agency Security Account Managers to review user roles bi-annually to ensure assigned access continues to be appropriate based on business needs.

Effective Configuration Management Necessitates a Formal Plan

A formalized plan documents essential processes, such as submitting change requests, obtaining approvals, testing changes, and evaluating their impact on system security and functionality. Without a formal configuration management plan, controlling and monitoring system changes becomes challenging, increasing the risk of inconsistent practices, unclear accountability, and noncompliance. Additionally, the absence of a thoroughly documented process can result in unauthorized changes and jeopardize operational continuity if key staff with essential knowledge leave the agency.

Although staff perform these activities in practice, the processes rely heavily on institutional knowledge and lack formal, high-level expectations for coordination. SABHRS should continue to carry out essential functions typically governed by a change advisory board (CAB), such as evaluating, authorizing, and prioritizing proposed changes, and maintaining thorough records, to ensure effective oversight. Implementing a comprehensive configuration management plan that clearly defines roles and responsibilities for these tasks will help promote consistency and accountability.

Recommendation #3

We recommend that the Department of Administration develop, document, and formalize a configuration management plan for SABHRS.

DEPARTMENT RESPONSE

DEPARTMENT OF ADMINISTRATION

MONTANA DEPARTMENT OF ADMINISTRATION

Director's Office
Greg Gianforte, Governor
Misty Ann Giles, Director

doa.mt.gov
406.444.2460
doadirector@mt.gov

March 13, 2026

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

RECEIVED
March 13, 2026
LEGISLATIVE AUDIT DIV.

Re: *25DP-03-Statewide Accounting, Budgeting, and Human Resources System (SABHRS) Department of Administration System Security and Reliability Audit*.

Dear Director Maciver,

The Department of Administration has reviewed the audit report titled *25DP-03-Statewide Accounting, Budgeting, and Human Resources System (SABHRS) Department of Administration System Security and Reliability Audit*. We appreciate the work of the Legislative Audit Division and agree with the audit recommendations.

Our goal is to strengthen SABHRS governance, documentation, configuration management, and user access controls in alignment with state standards and best practices. The Department recognizes security and control work is never complete and will treat these efforts as part of an ongoing cycle of review and improvement.

Recommendation #1:
We recommend the Department of Administration:

A. Update and formalize the policies and procedures governing both SABHRS HR and FS to ensure comprehensive and consistent documentation across both systems; and
B. Clearly assign and document responsibility for the ongoing management, maintenance, and review within each system-wide control design consistency in compliance with state standards.

Department Response: The Department concurs with this recommendation. The Department expects to make significant progress on the work detailed below by April 30, 2027.

- The Department will formalize and consolidate policies and procedures for SABHRS HR and FS.
- The Department will assign responsibility for each system-wide control with a focus on design consistency and compliance with state standards.

Recommendation #2:
We recommend the Department of Administration:

A. Update and formalize system security documentation applying to both SABHRS HR and FS to ensure comprehensive and consistent documentation across both systems; and
B. Formalize the review requirement for Agency Security Account Managers to review user roles bi-annually to ensure assigned access continues to be appropriate based on business needs.

Department Response: The Department concurs with this recommendation. The Department expects to make significant progress on the work detailed below by April 30, 2027.

- The Department will develop and maintain a combined system security plan with a focus on the Access Control documentation requirements, with appropriate and consistent documentation for both SABHRS HR and FS, prioritizing foundational system controls by the target date.
- The Department will adopt and enforce a policy requiring Agency Security Account Managers to review user roles on a bi-annual basis to confirm access remains appropriate for business needs.

Recommendation #3:
We recommend the Department of Administration develop, document, and formalize a configuration management plan for SABHRS.

Department Response: The Department concurs with this recommendation and will develop, document, and implement a configuration management plan for SABHRS by April 30, 2027.

The Legislative Audit Division has identified important opportunities to strengthen SABHRS security, reliability, and governance, and the Department appreciates this work. Based on the recommendations, the Department is committed to formalizing policies and procedures, enhancing system security documentation and user access review, and developing a comprehensive configuration management plan for SABHRS. Together, these actions are intended to improve the consistency, transparency, and

effectiveness of SABHRS controls in alignment with state standards and to better support agencies that rely on these core systems.

Thank you for your guidance and support. We look forward to working collaboratively to ensure the highest standards of procurement and IT services.

Sincerely,

Misty Ann Giles
Director
Department of Administration