A Report
to the
Montana
Legislature

Information Systems Audit

SABHRS Security Assessment

Department of Administration

March 2023

Legislative Audit
Division

22DP-01

Information Systems Audits

Information Systems (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS 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 IS 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 IS audit staff hold degrees in disciplines appropriate to the audit process.

IS audits are performed as stand-alone audits of IS 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.

Audit Staff

Miki Cestnik
Tyler J. Julian

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

LEGISLATIVE AUDIT DIVISION

Angus Maciver, Legislative Auditor
Deborah F. Butler, Legal Counsel

Deputy Legislative Auditors:
Cindy Jorgenson
William Soller

March 2023

The Legislative Audit Committee
of the Montana State Legislature:

This is our information systems compliance audit of the Statewide Accounting Budgeting and Human Resources System (SABHRS) managed by the State Financial Services Division and State Human Resources Division of the Department of Administration (DOA).

This report provides the legislature information about SABHRS IT management and security controls. This report includes recommendations for addressing an IT security staffing issue and improving the SABHRS security program at DOA. A written response from the department is included at the end of the report.

We thank department personnel for their cooperation and assistance during the audit.

Respectfully submitted,

/s/ Angus Maciver

Angus Maciver
Legislative Auditor

Room 160 • State Capitol Building • PO Box 201705 • Helena, MT • 59620-1705
Phone (406) 444-3122 • FAX (406) 444-9784 • E-mail lad@legmt.gov

Table of Contents

Figures and Tables

Tables

Appointed and Administrative Officials

Department of Administration

Misty Giles, Director, Department of Administration

Kevin Gilbertson, Chief Information Officer, State Information Technology Services Division

Cheryl Grey, Administrator, State Financial Services Division

Anjenette Schafer, Administrator, State Human Resources Division

Colter Schilling, Bureau Chief, Financial Services Technology Bureau

Martha Watson, Human Resources Information Systems Manager, State Human Resources Division

Montana Legislative Audit Division

Information Systems Audit
SABHRS Security Assessment
Department of Administration

A report to the Montana Legislature

Background

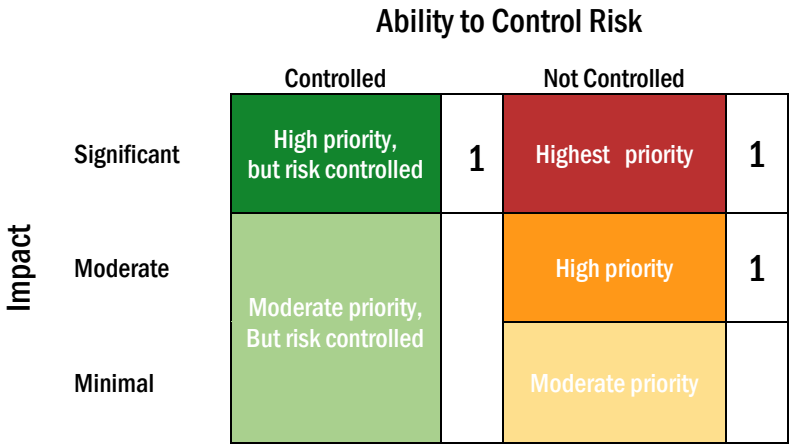
The Statewide Accounting, Budgeting, and Human Resources System (SABHRS) is a state-wide system with applications used by agencies to report disposition, use, and receipt of public resources, along with assisting in the administration of state human resource information and practices. Security audits of SABHRS are performed regularly due to the importance of the system to the State's operations.

SABHRS contains all state financial transactions and data for over 15,000 state employees. SABHRS is managed by two separate divisions within the Department – the State Financial Services Division and the State Human Resources Division.

Agency:
Department of Administration

Director:
Misty Giles

Department of Administration (DOA) has effective controls and maintains appropriate staff to ensure SABHRS application-level security. However, general security management responsibilities have not been established and DOA needs to perform the duties necessary for SABHRS to meet state security requirements.



The figure above summarizes the nature and extent of the audit findings. Findings are categorized by priority that is based on impact and whether the agency has effective controls to mitigate the risk associated with the finding. Impact is the effect a risk could have on an agency's system, security, business process, or operation. Each priority category contains the number of relevant findings in this report.

(continued on back)

For the full report or more information, contact the Legislative Audit Division.

leg.mt.gov/lad

Room 160, State Capitol
PO Box 201705
Helena, MT 59620-1705
(406) 444-3122

The mission of the Legislative Audit Division is to increase public trust in state government by reporting timely and accurate information about agency operations, technology, and finances to the Legislature and the citizens of Montana.

To report fraud, waste, or abuse:

Online
www.Montanafraud.gov

Email
LADHotline@legmt.gov

Call
(Statewide)
(800) 222-4446 or
(Helena)
(406) 444-4446

Text
(704) 430-3930

RECOMMENDATIONS:

Highest Priority

Recommendation #1 (page 8):

Management and operational effectiveness

The Department of Administration needs to formally document and fulfill SABHRS information security responsibilities for both divisions.

Department response: Concur

High Priority

Recommendation #2 (page 11):

State compliance

The Department of Administration must improve management of the SABHRS audit logs and implement the State's Continuous Monitoring Plan as part of SABHRS system security planning and security program.

Department response: Concur

High Priority But Controlled

No Recommendation

Due to IT staff assuming multiple roles, the Department of Administration cannot separate critical processes. However, we identified compensating controls in place to mitigate the risk of fraud or unauthorized actions.

Chapter I – Introduction, Scope, and Objectives

Introduction

The Department of Administration (DOA) serves state government by providing business services to other state agencies, including accounting and human resources. The Statewide Accounting, Budgeting, and Human Resources System (SABHRS) is a state-wide system with applications used by agencies to report disposition, use, and receipt of public resources, along with assisting in the administration of state human resource information and practices.

SABHRS comprises several separate applications that operate on a database platform. This audit focuses on the SABHRS Financials (FS) and SABHRS Human Capital Management, also referred to as Human Resources (HR), applications. All state agencies use these applications for the management of financial and human resource business operations.

The technical operation and maintenance responsibilities for SABHRS are managed by three divisions at DOA:

- State Human Resources Division (SHRD) manages the HR application.
- Financial Services Technology Bureau (FSTB) within the State Financial Services Division (SFSD) manages the FS application and the database administrators that manage the database platform for both HR and FS applications.
- State Information Technology Services Division (SITSD) is responsible for hosting the SABHRS FS and HR application servers.

Audit Scope and Objectives

The two audit objectives were to:

- Determine if the IT management of SABHRS impacts DOA's ability to meet State information security requirements; and
- Determine if Database and System Administrator accounts are appropriately managed and that compensating controls exist to eliminate security risks or potential fraud.

The objectives are based on two key risks. Adequate human resources may not be allocated for SABHRS security. There is also a potential conflict of interest by the placement of key SABHRS personnel within only one division. These key personnel possess administrative privileges that increase risk for inappropriate access to SABHRS audit logs which are designed to enforce user and administrator accountability.

Our audit focused on the Information Technology (IT) management of SABHRS and its IT personnel within both divisions that support SABHRS. The scope of this audit includes the following:

- Human resource considerations for each division.
- The roles, responsibilities, and privileges of key IT personnel.
- The controls that enforce IT personnel accountability and separation of duty.
- SABHRS application security reviews relative to the duties performed by key IT staff and how their activity is monitored.

What We Did

Our IT audit methodologies focused on reviewing process components to identify the capability of controlling risks. Risks to the agency are identified in planning. Fieldwork reviews the processes used to prevent or mitigate risk. Methodologies include:

- Identifying the individuals responsible and accountable for processes.
- Documenting a thorough understanding of control processes through interviews, observations, and document reviews.
- Reviewing any work products (reports, documents, decisions) or information sources related to reviewed processes.
- Identifying if there are metrics used for determining effectiveness.
- Assessing how the culture and behavior of staff involved in the control process influence their effectiveness.

As part of the audit, we determined how capable each control process is at meeting its intended goal and reducing risk to the agency. The following table summarizes the control areas reviewed during this audit and our overall determination. The control processes reviewed for each control area are discussed in greater detail in subsequent chapters.

Table 1
SABHRS Control Areas

Control Area	Determination
Application Security Services Management	3
Application Change Management	3
Application IT Management Framework	3
Application IT Human Resources Management	3
Security Management Framework	2
Security Human Resources Management	1
Database IT Security Services Management	2
Database Managed Business Process Controls	2
Legend	
Activities are organized and the process is well-defined	3
Basic activities are performed and are complete	2
Some activity occurs, yet not organized or incomplete	1
Incomplete or incapable process	0

Source: Compiled by the Legislative Audit Division.

Criteria Used

State law outlines the responsibilities of all agencies to develop and manage security programs and conduct IT resources in an organized, deliberative, and cost-effective manner. IT governance and management practices are necessary to successfully implement these requirements. Therefore, both industry best practices and state requirements were used as criteria for this audit:

- The State Information Security Policy (and appendices) implements sections of Montana Code Annotated (MCA) that apply to information security. This policy defines the roles and responsibilities, technical controls, and IT standards adopted by the State. These standards align with the National Institute of Standards and Technology (NIST) standards which also served as criteria during this audit engagement.
- The Control Objectives for Information and Related Technology (COBIT) framework guides on common IT management and governance practices to reduce technical issues and business risks. While DOA is not required to use this standard, the practices identified incorporate industry best practices that support and align with NIST and State security requirements. COBIT was used to evaluate the Human Resource considerations and IT management practices.
- Policies and procedures specific to SABHRS provided the criteria for evaluating SABHRS application security and compliance with internal requirements.

Chapter II – SABHRS Application Security

The security of the SABHRS FS and HR applications depend on successful IT management. We determined the State Financial Services Division (SFSD) and the State Human Resources Division (SHRD) appropriately manage SABHRS application security and application controls. The following table summarizes the application-specific control processes reviewed in making this determination.

Table 2
SABHRS Application Security Control Processes

Control Process	Determination*
Application IT Security Services Management	
Manage user identity and logical access	Pass
Application IT Change Management	
Evaluate, prioritize, and authorize change requests	Pass
Manage emergency changes	Pass
Track and report change status	Pass
Close and document changes	Pass
Application IT Management Framework	
Establish roles and responsibilities	Pass
Optimize the placement of the IT function	Pass
Define information and system ownership	Pass
Define target skills and competencies	Pass
Application IT Human Resources Management	
Acquire and maintain adequate and appropriate staffing	Pass
Identify key IT personnel	Pass
Maintain the skills and competencies of personnel	Pass

Source: Compiled by the Legislative Audit Division.

* A pass/fail determination indicates whether process activities need improvement to meet the intention of the control area.

Access Control: SABHRS has mature access control to manage user identity and logical access to the system. This process regulates who can access the data in SABHRS and what actions can be performed within the system. SABHRS has well-defined roles and clear procedures for assigning, changing, and reviewing user access. Privileged roles for configuring SABHRS and its security are appropriately controlled.

Change Control:. SABHRS has a mature change management control process to prevent and identify unauthorized changes to the system. This process ensures that changes to SABHRS data, programming, or configuration are deliberate and follow evaluation and authorization procedures–this includes considerations for emergency changes. DOA maintains a detailed record of all SABHRS changes and access to this record is appropriately controlled.

IT Management Framework: DOA has a mature framework to ensure adequate management of SABHRS application security. Application management roles and responsibilities are defined, consider segregation of duty in their design, and skills and competency requirements for all SABHRS support positions are defined.

IT Human Resources Management: DOA maintains adequate and appropriate staffing for SABHRS application security. Key IT personnel are identified, their duties align with the roles and responsibilities defined in the IT management framework, and they must past appropriate security and qualification screening. Adequate controls exist to address unforeseen changes to key IT personnel.

Conclusion

SABHRS has the necessary control structure to ensure effective application security and the Department of Administration maintains adequate and appropriate staff to enact these controls.

Chapter III – Insufficient IT Security Personnel

The security posture of SABHRS is not defined by application security alone. While the controls that enforce application security are appropriate and effective, security governance and management that address agency strategy and supporting activities for overall security must also be considered. While the State Information Technology Services Division (SITSD) provides direction in State IT policy and procedures, DOA does not have an individual responsible for the day-to-day management of the agency's information security and to coordinate security-related interactions. This role is critical for effectively maintaining and executing a security program for agency systems. A security program goes beyond application security and includes the assessment of all controls and maintaining current policies, thorough system documentation, and ensuring compliance with State information security requirements.

The following table summarizes the review of the IT and human resources management control processes relevant to general security responsibilities for SABHRS.

Table 3
SABHRS Security Management Control Processes

Control Process	Determination*
Security Management Framework	
Establish roles and responsibilities	Fail
Security Human Resources Management	
Acquire and maintain adequate and appropriate staffing	Fail
Identify key IT personnel	Fail

Source: Compiled by the Legislative Audit Division.

* A pass/fail determination indicates whether process activities need improvement to meet the intention of the control area.

Significant Findings

DOA is not compliant with §2-15-114, MCA, which requires each agency to designate an individual to manage the agency's security program. DOA has not identified or established personnel responsible for SABHRS security. As a result, certain security-related duties for SABHRS are not being managed; these include:

- Maintenance and assessment of general IT controls for SABHRS.
- Maintenance of System Security Plans and associated documentation.
- Development of a SABHRS security program that aligns with State requirements for a system to operate on the State network.

Impact

SITSD has established a review and approval process to ensure systems meet State security requirements to operate. This process requires all systems have a System Security Plan (SSP) that adheres to the State of Montana Risk Management Framework (RMF). The RMF requires a review and update of the SSPs every two years. Both SABHRS applications are approaching operational renewal approval and SITSD review. The previous review process, completed in 2020, indicated that the following requirements must be met for re-approval in 2023:

- Implement (and document) required continuous monitoring activities
- Mitigate all deficiencies identified in the previous review

While progress toward the above requirements continues, neither of these conditions have been met. Therefore, SABHRS, a system critical to State operations, is at risk of not receiving approval to operate. While this is unlikely, this circumstance nonetheless highlights that SABHRS is not meeting State security requirements and should be a model for other agencies that must meet the same requirements.

Improvement Opportunity

Effective security management is a full-time position. Current SABHRS personnel have absorbed additional security responsibilities in addition to work in their primary function. While policy defines responsibilities for key SABHRS IT personnel, the department has not established responsibility for that role or maintained the personnel to support general IT security activities. In response to a 2017 audit recommendation, DOA stated SITSD would fill this role and assume security responsibilities for DOA. Despite their response, this has not occurred, and SABHRS lacks effective security management.

The State Financial Services Division (SFSD) has an open full-time equivalent (FTE) which previously performed general IT security duties for SABHRS. During this period, SFSD made significant improvements in overall security and documentation. SABHRS HR was able to leverage some of this work for their own security, though the lack of dedicated FTE impeded HR's level of progress.

DOA recognizes that general security duties for SABHRS is a full-time position and not manageable under the current support structure. This open FTE was not compensated at a rate expected of a security officer supporting both SABHRS divisions. The department indicated they have been unsuccessful filling this role due to the current classification and the competitive market for security skills. However, DOA stated filling this position at a more competitive rate is within their current personnel budget. With security consolidation plans unfolding across the state, DOA needs to determine the best way to secure SABHRS in the long-term. This will likely need to include some form of coordination with SITSD and the IT staff responsible for SABHRS. If DOA decides to assign security duties to the open FTE within SFSD, the department would need to properly reclassify the FTE and increase future personnel budgets.

RECOMMENDATION #1

We recommend the Department of Administration formally document and fulfill SABHRS information security responsibilities for both divisions.

Chapter IV – Audit Trail Protection and Monitoring

A key component of an effective IT security program is identifying, logging, and monitoring auditable events related to security and critical business processes. Recording these events in an audit log provides the forensic data necessary to investigate security incidents or business discrepancies and is a means to enforce accountability within the system. The Department of Administration (DOA) maintains these audit logs, but the audit logs are not controlled to prevent manipulation by the administrative personnel held accountable by these logs.

The following table summarizes the review of the control processes designed to enforce administrative accountability and the integrity of SABHRS audit data.

Table 4
SABHRS Database Management Control Processes

Control Process	Determination*
Database IT Security Services Management	
Maintain an audit trail of access to information	Pass
Define risks associated with business and security events	Fail
Log critical business and security events	Fail
Continually monitor business and security events	Fail
Database Managed Business Process Controls	
Ensure administrative privileges are monitored	Fail
Capture and secure source information of transactions	Fail

Source: Compiled by the Legislative Audit Division.

* A pass/fail determination indicates whether process activities need improvement to meet the intention of the control area.

Significant Findings

The SABHRS audit logs are not adequately controlled to ensure administrative accountability is enforced:

- The SABHRS database administrators have unrestricted access to the SABHRS audit logs.
- Certain key auditable events related to security are not identified or recorded.
- The audit logs are not actively monitored.

Impact

The database administrators (DBAs) are responsible for maintaining and securing the State's personnel and financial data contained within SABHRS. The level of access granted to the DBAs to effectively perform their duties also grants unrestricted access to all data in the system. The audit logs maintained

by SABHRS not only enforce the State's financial accountability they also enforce user and DBA accountability for changes made to the data in (and configuration of) SABHRS. Uncontrolled access to the audit logs presents the DBAs with the opportunity to perpetrate and conceal errors or fraud in the system. The deficiencies identified in SABHRS audit logging presents different issues that need to be addressed to mitigate this risk:

Database Log Integrity: Best practices state audit logs should be sent to a centralized logging repository where the DBAs do not have any access or authority. SITSD offers a centralized logging service, and the department has implemented the baseline configuration of this service for SABHRS. The current implementation, however, only records high-level commands issued to the system and database and does not include the audit logs created and maintained by the database. Capturing and forwarding all SABHRS auditable events, including the audit logs maintained in the database, would ensure the integrity of all audit log data and further enforce accountability in the system.

Historical Security Events: SABHRS maintains application security configuration and user privilege data in the system. This data, however, only represents the current state of the system and contains little to no historical information on changes made to this configuration – this introduces a potential gap in the data that would be used to investigate security incidents. Handling changes to the SABHRS security data as auditable events (and ultimately recording these changes to the audit trail as described above) would provide additional information for enforcing user accountability and the data necessary to implement active security monitoring of SABHRS.

Audit Log Monitoring: The department reviews changes associated with SABHRS auditable security and business events regularly, ensuring security configurations align with management-approved changes and the system records business transactions correctly. Events with greater potential impact are reviewed more frequently. This review process, however, is a reactive approach to security as it introduces a period between an event's occurrence and its detection. Reviews should be coupled with active monitoring as a proactive/preventative approach to overall security. Active monitoring would allow DOA to detect security and business events as they happen and respond to potential threats before any harm is done.

Improvement Opportunity

The identification and documentation of auditable events, securing the audit logs, and the monitoring of these logs for auditable events are common requirements among standards pertaining to the storage of sensitive data. To meet evolving compliance requirements, the State has adopted these standards as part of the State of Montana Risk Management Framework (RMF) and Continuous Monitoring Plan. The department has not implemented aspects of this plan for SABHRS due, in part, to the lack of dedicated security personnel discussed in the previous chapter. DOA captures auditable events and has implemented the foundational mechanisms for monitoring but the intention of these two activities is not yet aligned to ensure full compliance with the State's information security requirements.

RECOMMENDATION #2

We recommend the Department of Administration improve management of the SABHRS audit logs and implement the State's Continuous Monitoring Plan as part of SABHRS system security planning and security program.

Department of Administration

Department Response

MONTANA DEPARTMENT OF ADMINISTRATION

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

March 17, 2023

Angus Maciver, Legislative Auditor
Legislative Audit Division
P.O. Box 201705
Helena, MT 59620

RE: SABHRS Information Security Audit 22DP-01: Department of Administration

Dear Mr. Maciver,

The Department of Administration (DOA), specifically State Financial Services Division (SFSD), State Human Resources Division (SHRD), and State Information Technology Services Division (SITSD), appreciates the opportunity to respond to the SABHRS Information Security Audit 22DP-01. Thank you to you and your staff for your work and professionalism during this process. All parties conducted a thorough review of the audit, and a response on behalf of the Department is included below.

Recommendation #1: We recommend the Department of Administration formally document and fulfill SABHRS information security responsibilities for both divisions.

Department Response: Concur
The Department divisions (SITSD, SHRD, SFSD) will collaborate to fulfill the required SABHRS information security responsibilities as well as document associated roles and responsibilities by December 2023.

Recommendation #2: We recommend the Department of Administration improve management of the SABHRS audit logs and implement the State's Continuous Monitoring Plan as part of the SABHRS system security planning and security program.

Department Response: Concur
The Department will implement the State's Continuous Monitoring Plan by allocating appropriate resources to manage system security and monitor audit logs by September 2023.

125 North Roberts, Rm 155, Mitchell Building
P.O. Box 200101
Helena, MT 59620-0101
406-444-2032
doadirector@mt.gov
doa.mt.gov

The Department divisions will also collaborate to leverage the existing centralized logging repository to ensure the audit logs record all relevant auditable events.

We look forward to implementing the corrective measures on the recommendations provided in this audit.

Sincerely,

Misty Ann Giles, Director

cc: Kristin Reynolds, Chief Financial Officer
Kevin Gilbertson, Chief Information Officer
Anjenette Schafer, Administrator
Cheryl Grey, Administrator