A Report
to the
Montana
Legislature

Information Systems Audit

Statewide Accounting, Budgeting, and Human Resources System (SABHRS) Governance and Security Management

Department of Administration

June 2018

Legislative Audit
Division

17DP-03 & 17DP-04

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

Aubrey J. Curtis
Hunter McClure
Diedra Murray

Reports can be found in electronic format at:
http://leg.mt.gov/audit

LEGISLATIVE AUDIT DIVISION

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

Deputy Legislative Auditors
Cindy Jorgenson
Joe Murray

June 2018

The Legislative Audit Committee
of the Montana State Legislature:

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

This report provides the Legislature information about security management and governance practices associated with SABHRS. The scope of the audit was limited to SABHRS Financials (FS) and Human Resources (HR) applications. This report includes recommendations for improving data security and governance practices of SABHRS at the Department of Administration. A written response from the Department of Administration is included at the end of the report.

We wish to express our appreciation to the Department of Administration 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@mt.gov

Table of Contents

Figures and Tables

Figures

Tables

Appointed and Administrative Officials

Department of Administration

John Lewis, Director

Mike Manion, Deputy Director and Chief Legal Counsel

Matt Van Syckle, Chief Information Officer (interim), State Information Technology Services Division

Cheryl Grey, Administrator, State Financial Services Division

Anjenette Schafer, Administrator, State Human Resources Division

Matt Pugh, Deputy Administrator, State Financial Services Division

Dean Mack, Deputy Administrator, State Human Resources Division

Montana Legislative Audit Division

Information Systems Audit

Statewide Accounting, Budgeting, and Human Resources System (SABHRS) Governance and Security Management

Department of Administration

June 2018 17DP-03 & 17DP-04 Report Summary

All state financial transactions and data for over 15,000 state employees are contained within the SABHRS information system, which is managed by separate divisions within the Department of Administration–the State Financial Services Division and the State Human Resources Division. The security management and information technology governance practices of SABHRS could be improved through better definition of strategy, policies, and plans, along with further examination of internal business relationships.

Context

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. In addition to the Financials (FS) and Human Resources (HR) applications, there are the Internet Budget and Reporting System (IBARS) and the Montana Budget Analysis and Reporting System (MBARS) applications that provide platforms for agencies to create and submit their budgets. SABHRS FS and SABHRS HR applications were the focus of this audit. Specifically, we determined an examination of other application general control areas was appropriate, such as application security management, along with information technology governance structure and practices that are applied to SABHRS.

Results

In the past decade, the Department of Administration (DOA) has transitioned SABHRS from centralized management, under the State Information Technology Services Division, to a more decentralized model that segregates the applications and their respective oversight among the function or process owners. There were efficiencies gained from the reorganization, such as information technology (IT) responsiveness to the function owners; however, there are also drawbacks that currently affect security management and governance of SABHRS that may not have been anticipated at that time.

The Department of Administration has well-documented policies and procedures with regards to access controls for SABHRS. We determined that the department is deficient in documenting the other 17 information security control categories that are required by state policy and should be included within a comprehensive System Security Plan (SSP) for SABHRS. The State Information Technology Services Division within DOA is currently working with the State Financial Services Division on completing an SSP for SABHRS FS, with the intention of assisting the State Human Resources Division in developing an SSP for SABHRS HR. Once the SSP is created, we recommend that the department assign a security officer to continually monitor and update as necessary. In addition, the

(continued on back)

agency staff that create SABHRS accounts and request user access roles are not required to complete training that is consistent or tracked by SABHRS staff. Since these individuals are responsible for signing off on privileged access to the system, we recommend SABHRS staff ensure agency staff receive consistent training, as well as track who has completed the training.

Risk assessment is another information security control family that is a common best-industry practice and helps staff determine whether business process or system controls are working as intended. We determined that the department has begun an agency-wide internal controls and risk assessment based on information provided by the divisions. They currently predict that an audit of these controls will occur in fiscal year 2019. The recommendation is that management closely monitor the process and make every effort to meet this goal. The information obtained from an objective risk assessment could provide necessary information for the risk management framework included in the SABHRS System Security Plan.

Finally, the governance structure of SABHRS at the department was examined. We determined there is no single governing entity for SABHRS, and through reorganizations within the last decade, the roles and responsibilities between the divisions are not clearly defined and distinguishable. We recommend the department reevaluate SABHRS support organizational structure to identify areas where efficiencies can be made and ensure proper IT governance is in place for information systems not managed by the State Information Technology Services Division.

Recommendation Concurrence	
Concur	4
Partially Concur	0
Do Not Concur	1

Source: Agency audit response included in final report.

For a complete copy of the report (17DP-03 & 17DP-04) or for further information, contact the Legislative Audit Division at 406-444-3122; e-mail to **lad@mt.gov**; or check the web site at **http://leg.mt.gov/audit**
Report Fraud, Waste, and Abuse to the Legislative Auditor's FRAUD HOTLINE
Call toll-free 1-800-222-4446, or e-mail **lad@mt.gov.**

Chapter I – Introduction

Introduction

The Statewide Accounting, Budgeting and Human Resources System (SABHRS) is a statewide computer application implemented by the State of Montana and managed by the Department of Administration (DOA) to assist state agencies in reporting the disposition, use, and receipt of public resources (§17-1-102(2), MCA). SABHRS also assists in the administration of human resource information, including the generation of a biweekly payroll.

Each year, Legislative Audit information systems staff conduct assurance work on certain controls in support of the statewide and individual agencies' financial compliance audits. Based on this work, we provide a limited distribution memorandum to financial compliance staff detailing the SABHRS control environment specific to their requirements and generally focused on access.

This audit focused on information systems general control areas for SABHRS applications. During initial audit work we identified controls relating to security management and information technology governance practices that could be strengthened. This report will present our findings along with our recommendations to the agency.

Background

While SABHRS is referred to as one system, there are actually several separate applications that are running on top of a database platform. These applications are SABHRS Financials (FS), SABHRS Human Capital Management, also referred to as Human Resources (HR), and a budget development component referred to as the (IBARS/MBARS). All applications are used by accounting and human resource staff at all state agencies to assist in the management of financial and human resource business operations. The data generated in the system is also used by legislators and other stakeholder groups to assist in policy and budget decisions. The general public is able to review data generated by the system via the State of Montana's checkbook (transparency) website.

Each application serves a different function, and for the scope of this audit we focused on the FS and HR. DOA manages them independently between the State Financial Services Division (SFSD) and the State Human Resources Division (SHRD). Within each application, modules provide different data processing to end users.

The FS application modules are used for the following:

- Process vouchers and payments to vendors.
- Process incoming payments and billing statements.
- Generate journal entries for each transaction and post to the General Ledger.
- Manage purchase order transactions and records.
- Record state assets and calculate depreciation.

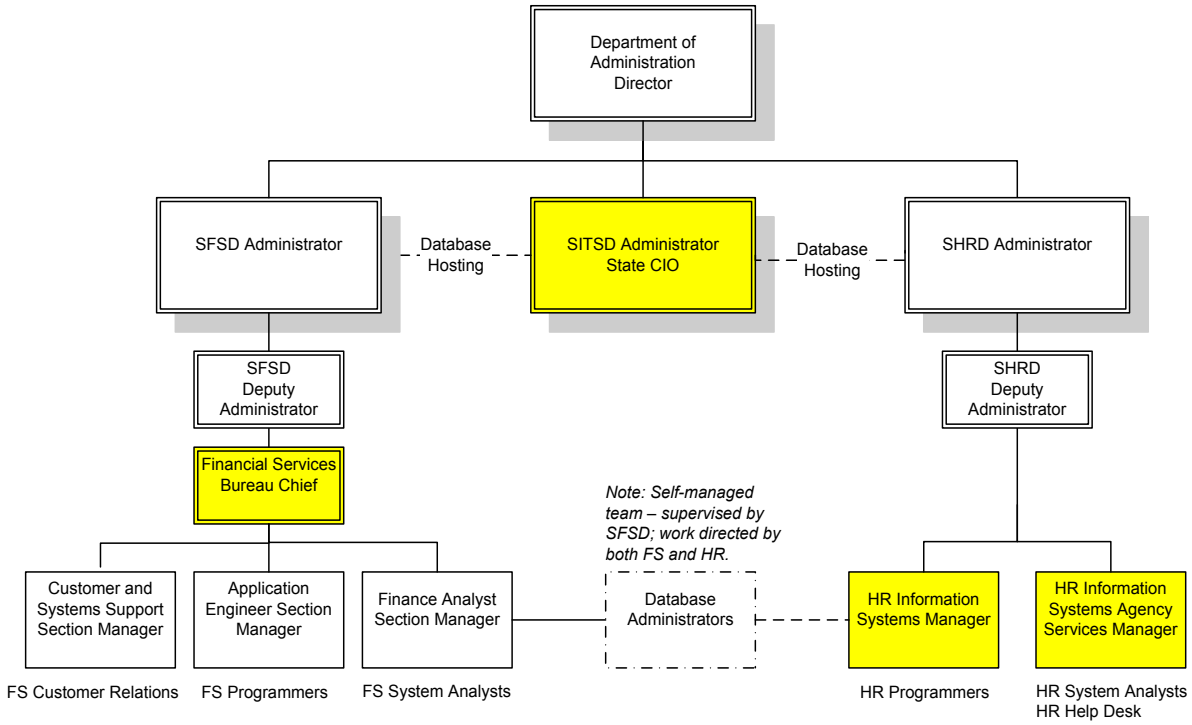
The HR application modules are used for the following:

- Record and maintain employment records for state employees.
- Record, validate, and approve employee time.
- Record and calculate benefits for state employees.
- Calculate individual employee payroll.

The responsibilities for the operation and maintenance of SABHRS are divided among four entities at DOA (these are highlighted in yellow in the figure on page 3).

- Financial Services Technology Bureau (FSTB) within the State Financial Services Division is responsible for managing the FS application.
- Human Resources Information Systems (HRIS) Technical Support Section within the State Human Resources Division is responsible for assigning technical programming and database support to resolve HR application issues.
- HRIS Agency Services Section is responsible for staffing HR Help Desk, coordinating HR application improvements, and providing professional training to division and agency personnel.
- State Information Technology Services Division (SITSD) is responsible for hosting FS and HR application servers and databases at the State of Montana Data Center.

Figure 1
Current Organizational Chart of DOA SABHRS Support



Source: Compiled by the Legislative Audit Division from information obtained from the Department of Administration.

Note: Yellow indicates primary technology providers, system management, and system administrators.

Audit Scope and Objectives

From the audit planning work we conducted, we determined that the scope should be limited to the two applications mentioned above (FS and HR) and should focus on primarily application level general controls, specifically security management. In addition, based on risk areas identified during annual assurance work, we decided that a review of IT governance practices used by the department over SABHRS would be pertinent. Proper governance ensures that the enterprise objectives are achieved by evaluating agency needs, setting direction through prioritization and decision making, and monitoring performance compliance and progress against agreed-on direction and objectives.

Our objectives during the audit were to:

1. Determine if SABHRS Financials and Human Resources application-level security management effectively safeguards data and protects application modules.

2. Determine whether Department of Administration's IT governance structure and procedures for providing oversight of SABHRS Financials and Human Resources applications are in line with industry best practices.

Audit Methodology

The following is a general list of the procedures followed in order to meet the audit objectives:

- Interviewed SABHRS technical staff, including individuals involved with programming and database management.
- Interviewed SABHRS managerial staff, including Financial Services Technology Bureau Chief, Human Resources Information Systems (HRIS) Manager, and HRIS Agency Services Manager.
- Interviewed SITSD staff, including state Chief Information Officer (CIO), the Enterprise Security Manager, and an Enterprise Risk Management Analyst.
- Communicated with DOA Human Resource Manager and reviewed current and historical organizational charts and position descriptions for key personnel.
- Surveyed 100 SABHRS agency account managers with a 53 percent response rate.
- Reviewed prior audit reports, work papers, and interviews.
- Reviewed fraud, waste, and abuse hotline calls for the agency.
- Queried all state employees and analyzed SABHRS access, roles, and training.
- Reviewed documented internal policies and procedures provided by the agency.
- Reviewed relevant statute and state policy.
- Reviewed industry best practices including ITIL Information Technology Service Management.
- Conducted meetings with the administrators of both the State Human Resources Division and the State Financial Services Division to discuss preliminary audit findings.

Audit Criteria

In addition to statute and state policy, the resources used throughout the planning and fieldwork of the audit were the Federal Information System Audit Control Manual from the Government Accountability Office, and publications from the National Institute of Standards and Technology (NIST), specifically NIST 800-53 regarding security and privacy controls of federal systems and NIST 800-39 for managing information security risk at the organization, mission, and information system level. NIST has

been designated by SITSD as the standard for IT security policy development for the entire state. For the first objective, DOA provided the Information Technology Infrastructure Library (ITIL) IT Service Management as the standard used internally for IT governance, which was also taken into account as we conducted audit work. ITIL provides a set of processes and procedures that are efficient, reliable, and adaptable to organizations of all sizes, and ensures that IT solutions are clearly aligned with business requirements. ITIL was initiated in the United Kingdom, and is now globally recognized as a best-practice framework.

Chapter II – SABHRS Security Management Practices

Introduction

This chapter will address the first objective of the audit, security management of the Statewide Accounting, Budgeting, and Human Resources System (SABHRS), and will discuss how the Department of Administration (DOA) integrates information security responsibilities of SABHRS into its organizational structure and processes. We determined the responsibility for the overall SABHRS information security program, including policies and procedures, is shared among three divisions at DOA with no single designated administrator.

Responsibility of DOA Information Security Program Is Unclear

The SABHRS applications support most state agencies; however, the system and its applications are considered specific to the missions of the State Financial Services Division (SFSD) and the State Human Resources Division (SHRD) and are therefore managed by these divisions.

According to §2-15-114, MCA, each director is responsible for ensuring a level of security for all data within their department. Included within this responsibility is a list of requirements, such as developing and maintaining written internal policies and procedures, designation of an Information Security Manager (ISM) to administer the agency's security program, and ensuring internal evaluations of the security program for data are conducted. Within state policy, an ISM may designate an Information Security Officer (ISO), also known as Information Systems Security Officer, to ensure appropriate security posture is maintained for each information system. The ISM and ISO may be combined into one position based on the size of the agency. Specific duties of the ISO listed within state policy are as follows:

- Develop agency policies, standards, and procedures in evaluating and referring to other qualified entities.
- Evaluate real or suspected information security incidents within the agency.
- Provide resolution recommendations to agency head, any attached agencies, and division administrators.

SITSD Responsible for Facilitating Security Planning for All State Agencies

Currently, the State Information Technology Services Division (SITSD) within DOA serves the following two separate missions:

- Enterprise IT planning/coordination/oversight
- Enterprise service delivery

Examples of enterprise services provided by SITSD include network connectivity (data, voice, video, and internet), phones, e-mail, and application/database hosting at the data center for most state agencies. The current intention of SITSD is to deliver generic enterprise-wide IT services that do not encompass specific agency applications. While SABHRS is used by most state agencies, it is an application and therefore managed within the divisions, in this case SFSD and SHRD.

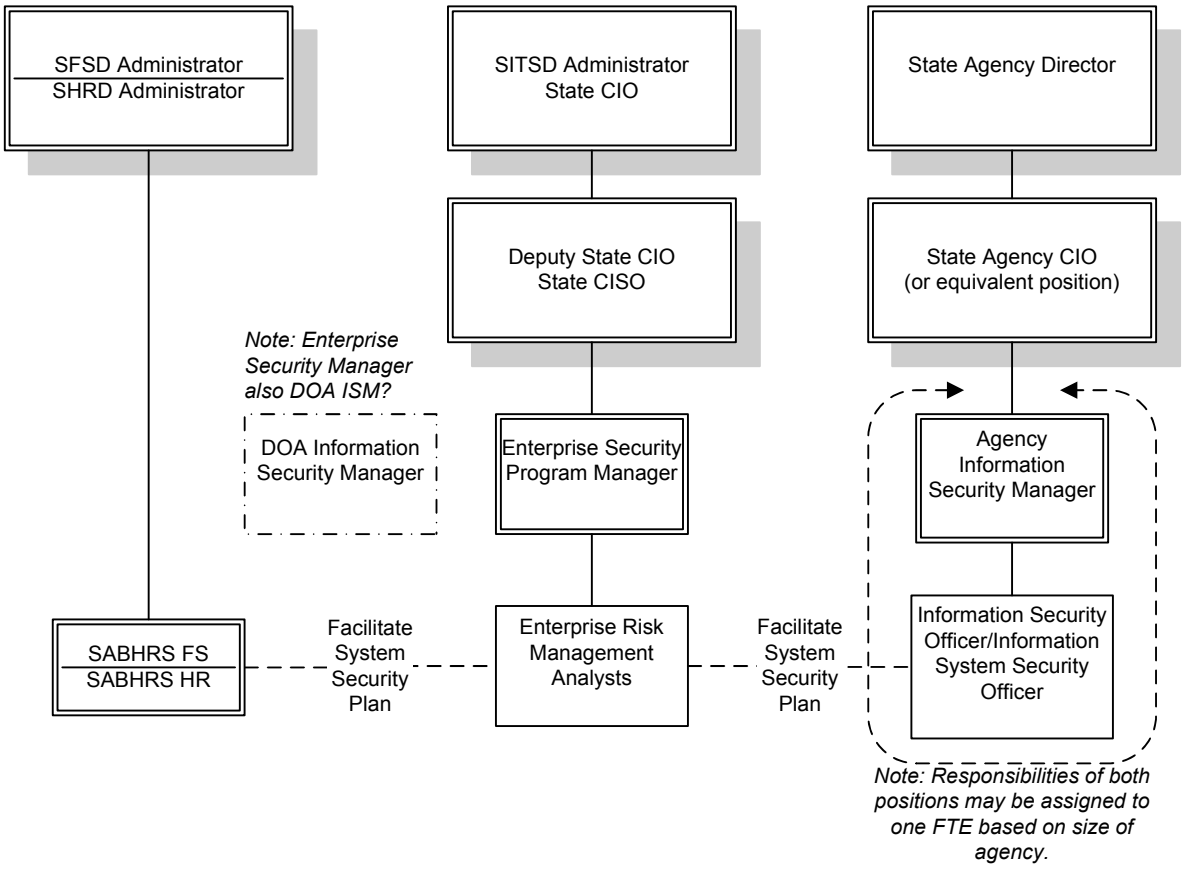
Within SITSD, the Enterprise Security Program Manager reports to the Chief Information Security Officer and is responsible for managing a statewide Information Security Program. This individual has oversight of all security programs in each state agency, and facilitates systems security planning for assigned agencies.

SABHRS Security Is Decentralized

The state CIO asserts that the relationship between SITSD and the other divisions within DOA is no different than any other agency or customer within state government. Hence, the responsibility of securing SABHRS, or any other system within DOA, would fall upon the Director of DOA. Since DOA's IT management (outside of SITSD) is generally decentralized, this responsibility is ultimately delegated to the specific division administrators, specifically SFSD and SHRD administrators with regards to SABHRS.

As for an agency [DOA] ISM, there is no documented designated party assigned these responsibilities over SABHRS, nor is it noted in DOA's IT Strategic Plan for 2016. However, during interviews it was inferred by some staff within DOA that the Enterprise Security Program Manager has assumed this role regardless of whether SABHRS is an SITSD managed system or not. The diagram on page 9 helps illustrate the interpretation of how SITSD interfaces with the other divisions within DOA, along with how other state agencies structure information security management.

Figure 2
Information Security Program Support From SITSD to SFSD and SHRD



Source: Compiled by the Legislative Audit Division from information obtained from the Department of Administration.

SABHRS System Security Plans Not Completed

The System Security Plan (SSP) is the first step in determining what controls are in place, along with what controls need to be implemented and how. While the SSP is not essential to the day-to-day functionality of SABHRS, it is essential with respect to information security of the organization, which would include any data repository such as SABHRS. For instance, SABHRS stores personally identifiable information on over 15,000 state employees. If unauthorized access is granted to SABHRS, and data is used for malicious purposes, the state may be held accountable for the information security breach. Since SABHRS security no longer falls under the purview of SITSD, there is a heavy burden placed on the other divisions to fulfill the responsibilities of the ISO for SABHRS, in addition to their other enterprise responsibilities.

SITSD Currently Facilitating SABHRS Security Plans

Similar to other agencies, the Enterprise Security Program Manager at SITSD is currently working with the Administrator of SFSD on developing an SSP for SABHRS FS, which would include information technology risk management framework based on the National Institute of Standards and Technology (NIST) Special Publication 800-39, as directed in state policy regarding information security. To summarize the purpose of the SSP, it provides a comprehensive blueprint for addressing the cybersecurity core requirements – identify risk, protect data, detect security weaknesses, respond to security weaknesses, and recover data during emergencies. Specific details for each requirement are explained in the state policy. SITSD is working in conjunction with other state agencies on their security plans. Agencies have three to five years to document plans and implement controls listed within the information security policy, effective 2015. Nonetheless, NIST information security controls have been the standard for the state since before 2015.

While SITSD is facilitating the development of the plan, the expectation would be that SFSD would be responsible for implementation and monitoring of the controls once the plan is complete. In addition, staff would need to update the plan when needed. At the time of the audit, the projection provided by SITSD for completing the SSP was January 2018. This goal was not achieved based on some supporting documentation that had to be created, and SFSD continues to work alongside the SITSD Enterprise Security Program Manager to complete the plan. While we recognize the efforts of DOA to complete the SABHRS security plan, we also note that the best practice is not a new concept. In a 2004 Information Systems audit, we addressed the necessity of a comprehensive SABHRS security plan and recommended the department update its plan to include a process that addressed risks and potential threats, along with continual evaluation of new vulnerabilities.

At this time, there have only been discussions between SHRD and SITSD on the SSP for the SABHRS HR application. The intention of the SITSD Enterprise Security Program Manager is to complete the process of developing the SSP with SABHRS FS before approaching SHRD to begin the process with SABHRS HR. The Enterprise Security Program Manager predicts that efficiencies could be achieved by eventually combining both applications into one SABHRS SSP.

Access Controls Exist, But Overall Security Management Lacking

The SFSD and the SHRD administration have established policies and procedures regarding accessing SABHRS. Their efforts to implement access controls around

SABHRS, as well as maintain system functionality, should not be diminished. However, security policy documentation provided by SABHRS staff primarily focuses on access controls only, and leaves much to interpretation for the remaining 17 NIST information security control families that are required in state policy. A NIST control family is a category of controls that support core functions for the cybersecurity of information systems. Most, if not all, control families would be addressed for each system. However, not all controls within a family (or category) would need to be implemented for all systems. Selection of security controls at the information system level should be based on continual risk management activities performed throughout the life cycle of the system–this process is referred to as a Risk Management Framework. The state has provided guidance on baseline controls for systems considered to be at the moderate level for data security. The table below lists the various security control families that are established by NIST, along with the core cybersecurity functions they support, and is included within state policy.

Table 1

NIST Control Families and Core Functions for Cybersecurity

Family	Core Function
Access Control	Identify, Protect, Detect
Awareness and Training	Protect
Audit and Accountability	Protect, Detect, Respond
Security Assessment and Authorization	Identify, Protect, Detect, Respond
Configuration Management	Identify, Protect, Detect
Contingency Planning	Identify, Protect, Detect, Respond, Recover
Identification and Authentication	Protect
Incident Response	Protect, Detect, Respond, Recover
Maintenance	Protect
Media Protection	Protect
Physical and Environmental Protection	Identify, Protect, Detect, Respond
Planning	Identify, Protect, Detect
Personnel Security	Identify, Protect, Detect
Risk Assessment	Identify, Protect, Detect, Respond
System and Services Acquisition	Identify, Protect, Detect
System and Communications Protection	Protect, Detect
System and Information Integrity	Identify, Protect, Detect, Respond
Program Management	Identify, Protect, Detect, Respond

Source: Montana Operations Manual Policy-Information Security Policy-Appendix A (Baseline Security Controls).

It is the responsibility of the agency to evaluate and categorize information systems to determine the appropriate controls based on the criticality and classification of the information managed by each system. Currently, a Risk Management Framework for SABHRS FS is being developed with assistance from SITSD. This Risk Management Framework will be incorporated in the SABHRS FS SSP, and can very likely be used for SABHRS HR SSP development as well. It is not clear whether the responsibility of performing risk assessments of SABHRS on a recurring basis falls under SITSD or the business owner. Documented designation of ISM authority for the department would help identify areas of responsibility.

State Policy Recommends Designating an Information Security Officer

As stated above, state policy recommends designating an ISO for larger organizations to help support the security program by maintaining security for specific information systems. Some specific ISO tasks are to evaluate information security incidents, provide resolution recommendations to the agency head, develop policies and procedures, assessment of common security controls, and carry out ISM responsibilities for system security planning. The responsibilities outside of developing an SSP are enough to consider a designated position who would work with the SITSD Enterprise Security Program Manager.

Under previous administrations, there were "security analyst" or "security administrator" positions under both SABHRS FS and SABHRS HR. Currently, there is a vacant security analyst position under Human Resources Information Systems (HRIS). The explanation given by the agency for this vacancy is that new account authentication software being implemented throughout the enterprise would automate a multitude of the duties done by this individual. We agree that this software will generate efficiencies with creating SABHRS accounts and the department deserves credit for pursuing this initiative, but this proposed software solution does not cover all information security protocols. After reviewing the position description of the security analyst, there are major duties and responsibilities assigned that, if accomplished, would be beneficial to DOA and can not be automated. Additionally, some align with the responsibilities of the ISO, for instance:

- Develop and maintain extensive knowledge of IT application security concepts and best practices.
- Document technical security set up and configuration, and related operational procedures. Maintain applicable components of SABHRS Security Plan. Provide recommendations and technical expertise of security related audit compliance and issues.

- Support the development and implementation of reporting tools and other procedures that facilitate the validation and verification that the security environment is enforcing established policies and management guidelines.

The supervisor of this vacant position, with the help of SABHRS HR developers, was fulfilling these duties at the time of the audit. Information security for a system as diverse and interconnected as SABHRS demands the attention of one full-time equivalent. Also, based on industry best practices, a separation between security and the business owner should exist in terms of the organization's reporting structure as well as job responsibilities. For example, the security analyst should not report to those responsible for the operational management of the applications. Since the technical staff report to the division administrators, or business owners, the security analyst falls under the supervision of the business owner, which presents a conflict of interest. Separating ISO responsibilities from the division administrators responsible for SABHRS will ensure the administrators' ability to effectively assess the use of common security controls by these individuals and their staff without undue influence.

To summarize, both business owners and information security managers work together to ensure that information systems and underlying applications are properly secured. Since DOA has segregated information technology resources within the department, it is critical to delineate responsibilities in order to ensure that state policies regarding information security, which are enforced by the department for other agencies, are also followed internally.

RECOMMENDATION #1

We recommend the Department of Administration:

A. *Formally designate and document the Information Security Manager for the department;*

B. *Finalize and implement a SABHRS system security plan that addresses all the National Institute of Standards and Technology (NIST) security control families and incorporates the NIST Risk Management Framework; and*

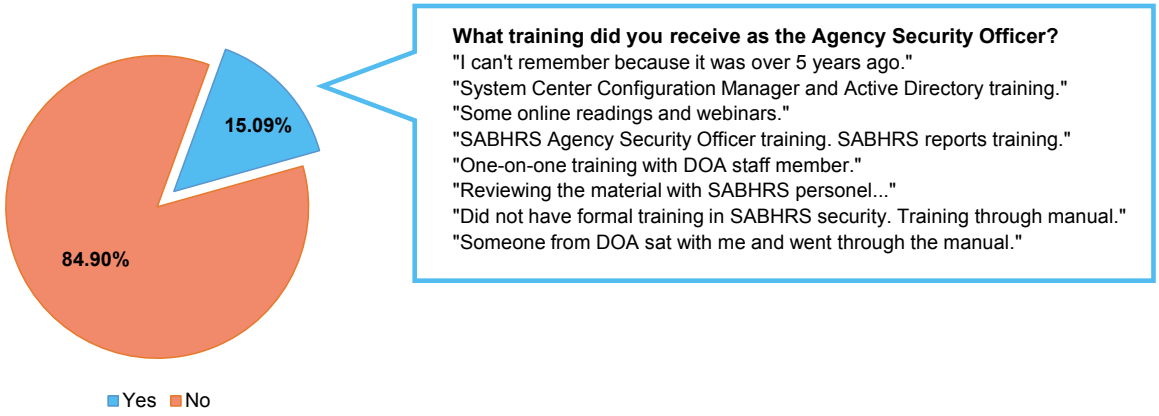
C. *Establish an information security officer with the responsibility to develop and maintain security policies and procedures, periodically assess security controls, and work with business owners to determine resolutions to security weaknesses for data and information systems not managed by the State Information Technology Services Division.*

Training for Agency SABHRS Account Managers

Another critical security control family included in NIST is awareness and training. Every state employee has general access to SABHRS, which allows the capability to perform basic tasks such as view and edit personal information, enroll in benefits, or enter time sheets. Depending on your position in state government, you may require elevated access to either SABHRS FS or SABHRS HR. Specific to position responsibility, each user account is assigned a role or combination of roles. Roles define what pages a user can access, how the information is displayed and what actions can be applied to the data by the user. Both SABHRS FS and SABHRS HR have roles that are unique to the application. Certain user roles must meet detailed criteria before they can be assigned to an account. For example, the employee requesting elevated access must have job-related tasks requiring such, and also may be required to complete training from SABHRS staff. Training records are kept on employees within SABHRS. In addition, it is necessary when assigning roles to ensure that employees do not possess conflicting roles. These best practices are also known as least privilege and proper segregation of duties.

In order to apply the proper roles, each agency designates a representative as its agency security officer (ASO). This would be the first line of approval for the creation of a new user in any of the SABHRS applications. The ASO and managers, according to the ASO Manual, are ultimately responsible for their users having appropriate access, and must be familiar with SABHRS Financial/HR Roles and Responsibilities Manuals. These manuals are just a few of the documents DOA has provided online via the Montana Information Network for Employees (MINE) to help educate agencies on SABHRS. During audit fieldwork, we surveyed 100 primary and alternate ASOs and inquired about the level of training they had obtained before they assumed the responsibilities of ASO. Of the 53 respondents to our question of whether they were required to take any training, 84.9 percent answered “no.” Of the 8 individuals who responded that they were required to take some training, the descriptions of this training were inconsistent and are included in Figure 3 (see page 15).

Figure 3
Survey Question on Required Training for Agency Security Officers



Source: Compiled by the Legislative Audit Division from the survey of SABHRS agency security officers.

Responses ranged from "online readings and webinars" to "one-on-one training with DOA staff member." The ASO Manual does not suggest anything different than what the survey presented stating that ASOs are "generally trained by an agency's existing ASO on security request procedures." Any new ASO can receive guidance, if requested, from SABHRS staff.

The ASO position provides SFSD and SHRD a point-of-contact at the agency to determine the least privilege for employees' SABHRS access. The SABHRS staff provide another layer of control through ensuring proper segregation of duties by determining if there are conflicting roles being requested, and also verifying required training for certain roles. It is our interpretation that the ASO responsibilities focus primarily on access, and using the term "security" within the title gives the impression that the position is accountable for all aspects of information security. In the Agency Security Officer Manual that is distributed by DOA, the primary responsibilities revolve around managing SABHRS accounts at their respective agencies. The duties of the ASOs are described as the following:

- Request creation of new users in SABHRS applications.
- Request assignment of Row or Data Level security. Row or Data Level security defines the data to which a user has access. [User Roles]
- Notify SABHRS security staff when an employee transfers or terminates employment by deactivating the user's access to SABHRS applications.
- Be aware of the state procedures and policies pertaining to security.

Through survey work and interviews with agency staff, it was noted that ASOs were not always aware of or clear that the above bullets were part of their responsibility. The job duties that appeared to be less clear to ASOs included deactivation of user access and awareness of state procedures and policies pertaining to security.

As the system owner, the department should require all assigned ASOs to complete a short training course that explains the roles and responsibilities, along with the security policies they need to be aware of. Training is provided by DOA if the agency requests it, but as the survey shows this is not a requirement. While the agencies are the data owners and designate account managers for requesting access to SABHRS, DOA is ultimately responsible for the security of the data contained therein and should take a vested interest in the competency of the ASOs. The ASOs are essentially on the front line for providing user roles, that at times can have access to sensitive information and elevated privileges to modify information. In addition, this step could help with limiting the number of requests for conflicting user roles, and ultimately the probability of DOA inadvertently approving conflicting roles.

RECOMMENDATION #2

We recommend the Department of Administration:

A. *Administer uniform training for all SABHRS agency security officers, and*

B. *Change the title of agency security officers to better reflect their role as SABHRS agency account managers.*

Internal Business Controls and Risk Assessment

DOA is currently establishing an entity-wide risk assessment program of internal business controls for the whole department. To date, this process has involved meeting with DOA divisions to gather information on their internal controls with self-selected risk values assigned. The next step would be writing a plan to complete an internal audit of these controls and determine whether the risks associated are accurate. The intent is to conduct an internal audit by fiscal year 2019.

According to NIST 800-39, risk assessments should consider threats and vulnerabilities at the entity-wide level, system level, and application level. As discussed earlier in this chapter, Risk Management Framework should be applied when selecting security controls from each of the NIST control families for applications or systems. Entity-wide risk assessments take into account personnel policies and procedures, training, and

security awareness activities for all information systems within the organization. These internal evaluations not only comply with statute regarding department responsibilities for data security, they support risk-based decisions by leadership that will ultimately affect the business process or system/application controls.

Through these assessments, the department can identify areas that need direct attention, and effectively prioritize allocated resources. This is especially critical during times where appropriations are limited. While DOA staff have collected information from all divisions regarding internal controls, the crux of the assessment lies with the audit of these controls to determine how effective they are. Therefore, the agency currently does not have an objective valuation of its internal controls. In addition, the process needs to be cyclical with the ever-changing landscape of data security within the agency.

RECOMMENDATION #3

We recommend the Department of Administration finalize the agency's internal controls and risk assessment and complete an audit on these controls, to include SABHRS business process controls.

Chapter III – SABHRS Governance

Introduction

In this chapter, information technology (IT) governance within Department of Administration (DOA) will be discussed, specifically surrounding SABHRS. This was the second objective of the audit, and from our review of security management there were potential correlations that could be drawn between the first objective and the agency IT governance practices from both the past and the present.

IT Governance

Governance is a common term used within IT best management practices. It is recommended that every organization with IT adopt a governance model to assist in service or system management. The State Information Technology Services Division (SITSD) under the Department of Administration (DOA) has stated that its IT governance model is the Information Technology Infrastructure Library (ITIL). ITIL provides a portfolio of publications aimed at helping organizations and individuals manage programs or projects that incorporate IT. The core of ITIL resides in five publications – Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement. ITIL was referenced for criteria purposes when examining governance practices over SABHRS.

Governance, as defined by ITIL, is the single overarching area that ties IT and the business together. Governance is what defines the common directions, policies and rules that both the business and IT use to perform the mission. Proper governance allows organizations to evaluate, direct, and monitor strategy, policies and plans. Proper management plans, builds, runs and monitors business activities to ensure they are in alignment with the direction or strategy defined by the governing entity.

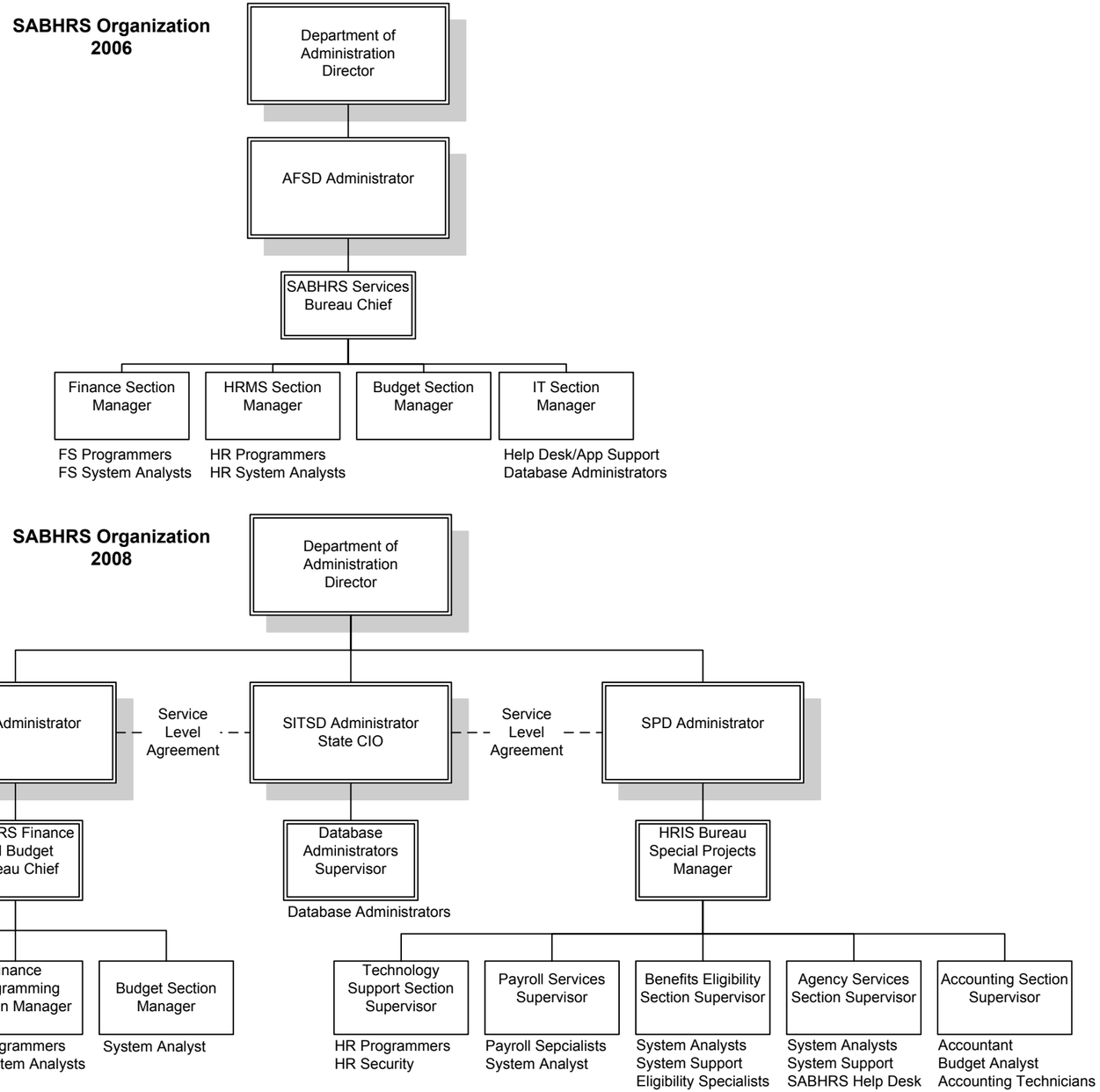
Multiple Reorganizations of SABHRS Services Bureau

Prior to 2006, the Statewide Accounting, Budgeting, and Human Resources System (SABHRS) was under the oversight of the Information Technology Services Division (ITSD) at the Department of Administration. The SABHRS Services Bureau (SSB) was managed by a single bureau chief, and four subordinate section managers. There was a Finance Section, a Human Resource Management System Section, Budget Section, and IT Section. Personnel within these sections consisted of programmers, system analysts, database administrators, and help desk staff for both the Financials (FS) and Human Resources (HR) applications. In August of 2006, a reorganization was implemented that moved SSB from under ITSD to the Accounting and Financial Services Division (AFSD).

According to department staff, the purpose of the reorganization was to foster a better line of communication between data owners, process owners, and technical staff. However, after some research on practices in other states, it was proposed that there be another reorganization to separate SABHRS into the two main applications (FS and HR) and place each under the respective business process owner. In January of 2008, another reorganization was implemented to move the SABHRS HR programmers and analysts to a newly established HRIS Bureau in the State Personnel Division. The SABHRS FS staff would remain under the SABHRS Finance and Budget Bureau (SFABB) in AFSD. The database administrators and technical support staff would move back to ITSD. To ensure the same level of database support would still be provided by ITSD, service-level agreements were created between ITSD and AFSD, as well as ITSD and SPD. The following diagram depicts the organizational structure supporting SABHRS and how it has evolved from the 2006 and 2008 reorganizations.

Figure 4

Evolution of SABHRS Support Organization From 2006 to 2008



Source: Compiled by the Legislative Audit Division from information obtained from DOA.

In January of 2009, the Legislative Audit Division (LAD) communicated with DOA regarding the reorganizations at DOA, specifically those affecting SABHRS. The purpose was to bring to light some concerns with the reorganization of SSB, and provide a suggestion that could possibly improve operations. The concerns focused on the decentralization of responsibility over the enterprise-level system, SABHRS. Due to the extensiveness of the reorganization and the potential impact to service, LAD suggested that DOA develop and implement a process to measure the effectiveness of the reorganization. In the SABHRS information systems audit report of that same year, a recommendation was presented regarding the decentralization of SABHRS into three divisions and for DOA to develop a formal mechanism for department personnel to make decisions and resolve disputes regarding SABHRS. During the audit, we recognized the ability of seasoned employees within the department and their adaptability to different governing models, as well as managers who have developed working relationships that accommodate the current organizational structure.

The current overall SABHRS management structure remains as it was in 2009, with some additional personnel moves. The database administrators that were moved in 2008 were once again brought back to what is now the State Financial Services Division (SFSD) in 2013, six months after a new Chief Information Officer (CIO) at SITSD was appointed. The SLAs that were established in 2009 are no longer valid. While there has not been a major SABHRS reorganization since 2009, there have been some modifications to the organizational structure from the diagram above.

Organizational Changes Based on Division Needs

Changes to the organization of DOA within the last 10-12 years have influenced how IT is governed in the department today. After reviewing organizational charts and position descriptions of personnel who are associated with SABHRS, interviewing current and prior employees, reviewing previous audit work papers, and creating a timeline of events dating back to 2006, it appears that decisions regarding SABHRS personnel are made solely based on the needs of each individual division and not on any specific strategic guidance from the director's office. This is especially concerning when it involves positions that support enterprise-level systems. For instance, during our review of organizational charts, we discovered a recently created position that was being filled without any position description on record. In addition, while there are general business goals and objectives for each division, new processes and procedures that are part of reorganization efforts are not evaluated to determine whether objectives for an organizational change, such as improving customer service or communication, are ever met. According to the ITIL Continual Service Improvement standard, transforming from a system-management-based organization to a more service-management-based organization will be more proactive in nature and better

align IT with business. Regardless of whether IT does implement continual service improvement around services or service management, it is critical that governance is addressed from a strategic view.

Currently, the SABHRS support organization has taken a system- or application-based management approach with respect to decentralizing into SABHRS FS and SABHRS HR. Industry best practices state there is no single-best way to organize, and each agency must tailor according to its resources and size. Nonetheless, organizational changes made in haste without clear objectives and input from all staff is an inefficient use of limited state resources that can lead to misunderstandings regarding working relationships and potentially feed a culture of mistrust between staff and leadership.

As discussed in the previous chapter, it was not clearly apparent who was responsible for overall security of SABHRS. Any misunderstanding of roles and responsibilities can not only lead to inefficiencies within the department, it can potentially create security weaknesses that are overlooked. To date, there is a wealth of institutional knowledge of SABHRS from tenured employees that have remained with DOA. These individuals are fully capable of maintaining the day-to-day operations of SABHRS. However, as senior staff attrition eventually occurs, coupled with unclear roles and responsibilities embedded within a management structure that is decentralized, there is a high probability of future complications. This warrants a re-evaluation of the department's organizational structure and practices over SABHRS.

RECOMMENDATION #4

We recommend the Department of Administration:

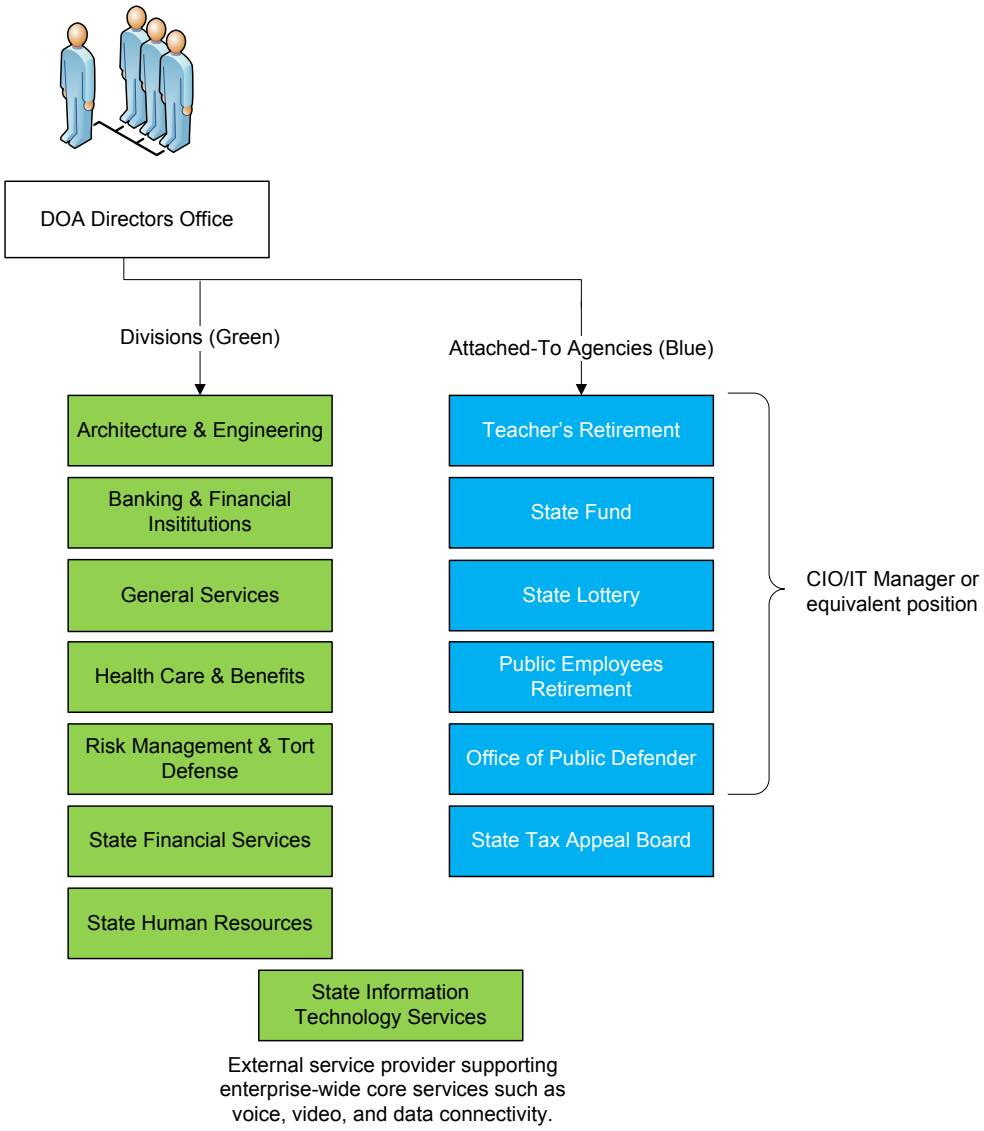
A. *Re-evaluate its current SABHRS support organizational structure to identify areas where efficiencies can be gained; and*

B. *Document and clearly communicate roles and responsibilities to personnel who support SABHRS.*

Current Governance of SABHRS Is Decentralized

DOA is a large and complex organization, with eight divisions and six attached agencies. While SITSD is a division within DOA, it consists of approximately 175 employees that support this externally-facing organization, which provides services to agencies across the state. Conversely, its mission is not focused on providing internal or shared services specific to DOA. Figure 5 (see page 25) depicts the divisions and attached-to agencies within the department.

Figure 5
DOA Divisions and Attached-To Agencies



Source: Compiled by the Legislative Audit Division from information obtained from the Department of Administration.

Former IT Manager Position for DOA

Following the 2009 Information Systems audit of SABHRS by LAD, DOA "re-established" the position of IT manager. The overall purpose of the position was to act as the executive agent for the director in the conduct of planning, managing, and coordinating IT support and reporting requirements for DOA. This was also a solution in response to the 2009 audit recommendation to create a mechanism for

making decisions and resolving division disputes in regards to SABHRS. The position description states that 50 percent of this individual's time was to be spent on staff coordination, which included reviewing divisions' actions related to IT, ensuring director's decisions and concepts regarding IT are implemented, and formulating and announcing DOA IT operating policy. The person hired into this position, along with one staff assigned as a systems analyst, helped develop an internal IT strategic plan for the agency and its services/applications outside the purview of SITSD, which included SABHRS. The goals outlined in this plan were as follows:

1. Deliver Services–Assist divisions in providing services that meet our customers' needs and support their Vision, Mission, and Goals.
2. Manage Information–Develop comprehensive information and data management strategies and associated supporting programs.
3. Establish Standards and Best Practices–Establish an IT services foundation based on standards, best practices, and fiscal sustainability.

DOA stated the internal Agency IT Strategic Plan 2014 is an active document, and the goals listed above are still priorities for the department. The DOA director's office spearheaded this effort, but during the course of this process the IT manager left the position and the state CIO committed to assuming the responsibilities of the IT manager. Conversely, the 2016 DOA Agency IT Strategic Plan (which includes SITSD) states under the heading 'IT Governance' the following:

> IT Governance is handled independently by each DOA division. In the larger division, State Human Resources Division and the State Financial Services Division, IT proposals and projects are handled by senior division management along with other division business. There are no separate IT formal processes and procedures for division with smaller IT operations: Architecture and Engineering, Banking and Financial Institutions, Office of Public Defender, Health Care and Benefits.
>
> SITSD has a large and overlapping governance structure for its two separate missions: enterprise IT planning/coordination/oversight and enterprise service delivery.

There was no documented protocol or current service-level agreement between the three divisions that clearly established this relationship. As discussed previously, service-level agreements were in place between SITSD and the other divisions in the past. While SABHRS is an enterprise-wide system, SITSD policy on Leadership Roles and Responsibilities says its area of responsibility only encompasses information systems that SITSD manages or controls, which does not include SABHRS. While there are benefits to having decentralized management of IT assets, which includes better responsiveness to the business units and direct customers, there still remains the necessity for a single governing entity that can make decisions regarding IT processes and procedures from a more global perspective.

Application-Based Management of SABHRS

As business owners, the State Financial Services Division and the State Human Resources Division have established business strategic plans, along with goals that align with these plans. A concern that arose during the audit was whether SABHRS management had decentralized to the extent that each division is solely focused on their respective application with no single entity observing how information technology processes are conducted for SABHRS or any other system not managed by SITSD. As required by statute, information technology resources in the state must be conducted in an organized, deliberative, and cost-effective manner (§2-17-505, MCA). Another guiding principle for information technology development requires similar information technology systems and data management applications to be implemented and managed in a coordinated manner to minimize unwarranted duplication. There are distinct benefits to organizing information technology assets under the business owners, such as better responsiveness and improved customer support. However, are there efficiencies that are being sacrificed, and if so, are the benefits outweighing the costs? In addition, from separating technical staff by application versus function, is there enough skill crossover capability to mitigate risk with employee turnover? The divisions that are supported by SABHRS do regularly meet and coordinate efforts related to technology, but the questions asked above should be addressed from a department-wide perspective and include systems other than SABHRS.

RECOMMENDATION #5

We recommend the Department of Administration address SABHRS IT governance by implementing one of the following corrective actions:

A. *Reestablish the IT manager position, or position of equivalent responsibility, to act as a governing agent for IT resources and processes not managed by State Information Technology Services Division, including SABHRS; or*

B. *Delegate governing authority of SABHRS to the State Information Technology Services Division and clearly define and document the roles and responsibilities associated.*

Department of Administration

Department Response

MONTANA DEPARTMENT OF ADMINISTRATION
"the backbone of state government"

Director's Office
Steve Bullock, Governor • John Lewis, Director

May 31, 2018

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

Dear Mr. Maciver:

Thank you for the opportunity to respond to the audit of the Statewide Accounting, Budgeting, and Human Resources System (SABHRS) Governance and Security Management. We appreciate the professionalism of the LAD staff throughout this comprehensive audit.

The staff of the State Financial Services Division (SFSD) and the State Human Resources Division (SHRD) thoroughly reviewed the content of this audit. As was shared with the Legislative Audit Division staff at the exit conference on Tuesday, April 17, 2018, this audit encompasses two separate systems—the financials system and the human resources system. The staff evaluated each system separately regarding the recommendations made in this audit.

While Department of Administration (DOA) concurs with Recommendations #1 through #4 of this report, it does not concur with Recommendation #5 and does not agree with the way that parts of this audit were written. DOA anticipated that the auditors would evaluate current business practices against current IT governance standards. A significant portion of this report, however, considers an organizational structure from 10-14 years prior. That organizational structure is not valid for today's business operations of the financial and human resources systems. In addition, the audit text contains broad, general statements that are not supported by the current organizational structure or operation of the divisions' systems.

Below are five examples extracted from the audit report that highlight our concerns:

- Page 10: "In a 2004 Information Systems audit, we addressed the necessity of a comprehensive SABHRS security plan and recommended the department update its plan to include a process that addressed risks and potential threats, along with continual evaluation of new vulnerabilities."

  Response:
  This statement does not indicate that the 2004 Information Systems audit recommendation was adequately completed by DOA. DOA expected this current governance and security management audit would evaluate how the current SFSD and SHRD systems operations align with current governance documentation.

Page 23: "Changes to the organization of DOA within the last 10-12 years have influenced how IT is governed in the department today. After reviewing organizational charts and position descriptions of personnel who are associated with SABHRS, interviewing current and **prior** [emphasis added] employees, reviewing previous audit work papers, and creating a timeline of events dating back to 2006, **it appears that decisions** [emphasis added] regarding SABHRS personnel are made **solely** [emphasis added] based on the needs of each individual division and not on any specific strategic guidance from the director's office. This is especially concerning when it involves positions that support enterprise-level systems."

Response:
No facts were identified that support this statement being included in the audit report. Because each division is responsible for its system, it is expected that each division's strategic plan would guide its personnel actions to meet business needs. The auditors interviewed "prior" employees, but when asked about which prior employees were interviewed, the lead auditor indicated that these individual(s)' names would not be released, and no details regarding the comments were shared. This lack of information makes it difficult to respond to the contention.

The statement "it appears that decisions ..." is subjective; this report is expected to be an objective audit report regarding the current systems. Supporting data and evidence that provide objective concerns are necessary to determine the issues that need to be addressed.

The word "solely" implies not involving anyone else in the decision-making process, which is incorrect regarding this matter. For example, before the database administrators' move to SFSD from SITSD, many discussions occurred among SITSD, the State CIO, SHRD management, the DOA Director, and DOA's IT Manager in the Director's Office.

- Page 24: "Nonetheless, organizational changes made in haste without clear objectives and input from all staff is [sic] an inefficient use of limited state resources that can lead to misunderstandings regarding working relationships and potentially feed a culture of mistrust between staff and leadership."

Response:
No facts support this statement. Indeed, many conversations and forethought went into each effort, including discussion of business needs and strategies. Furthermore, it is unrealistic to seek input from "all" staff when making organizational changes. Unless clear supporting data and evidence are provided, the remainder of this comment is conjectural and, given its lack of a factual foundation, does not belong in an audit.

- Page 27: "There are distinct benefits to organizing information technology assets under the business owners, such as better responsiveness and improved customer support.

However, are there efficiencies that are being sacrificed, and if so, are the benefits outweighing the costs?"

Response:
If the audit identified specific examples of efficiencies being sacrificed or benefits outweighing the costs, the audit should specifically provide examples of identified issues. Otherwise, these leading questions without factual foundation do not belong in this audit report.

- Page 27: "In addition, from separating technical staff by application versus function, is there enough skill crossover capability to mitigate risk with employee turnover?"

Response:
DOA believes it has reasonably mitigated risk. This suggestive statement, however, intimates that some risk exists, yet the audit did not provide any concrete examples to inform its statement.

RECOMMENDATIONS:

Our comments to the audit recommendations are:

Recommendation #1 *– We recommend the Department of Administration:*

A. Formally designate and document the Information Security Manager for the department;
B. Finalize and implement a SABHRS system security plan that addresses all the National Institute of Standards and Technology (NIST) security control families and incorporates the NIST Risk Management Framework; and
C. Establish an Information Security Officer position with the responsibility to develop and maintain security policies and procedures, periodically assess security controls, and work with business owners to determine resolutions to security weaknesses for data and information systems not managed by the State Information Technology Services Division.

Department Response: <u>Concur</u>

A. The Information Security Manager from SITSD will continue to fulfill the duties as the Information Security Manager for DOA. This position description will be slightly updated to clarify this information.
B. SFSD and SHRD both concur with the two separate SABHRS security plans for each division's independent system.
C. The Information Security Manager from SITSD will assume this role and its associated responsibilities.

Recommendation #2 – *We recommend the Department of Administration:*

A. Administer uniform training for all SABHRS agency security officers; and
B. Change the title of agency security officers to better reflect their role as SABHRS agency account managers.

Department Response: Concur

A. DOA will continue to administer training to agency staff.
B. DOA will update the title of agency security officer to agency security account managers.

Recommendation #3 – *We recommend the Department of Administration finalize the agency's internal controls and risk assessment and complete an audit on these controls, to include SABHRS business process controls.*

Department Response: Concur

These recommended actions are already in progress with each independent system (SFSD and SHRD).

Recommendation #4 – *We recommend the Department of Administration:*

A. Re-evaluate its current SABHRS support organizational structure to identify areas where efficiencies can be gained; and
B. Document and clearly communicate roles and responsibilities to personnel who support SABHRS.

Department Response: Concur

A. DOA will re-evaluate its SABHRS support organizational structure.
B. DOA will document and communicate roles and responsibilities to SABHRS staff.

Recommendation #5 – *We recommend the Department of Administration address SABHRS IT governance by implementing one of the following corrective actions:*

A. Re-establish the IT Manager position, or position of equivalent responsibility, to act as the governing agent for IT resources and processes not managed by State Information Technology Services Division, including SABHRS, or
B. Delegate governing authority of SABHRS to the State Information Technology Services Division and clearly define and document the roles and responsibilities associated.

Department Response: Do Not Concur

DOA does not concur with this recommendation. It is strengthening its IT governance by continuing to incorporate industry best practices including an Information Technology Service Management framework. It is evaluating other options to ensure IT governance is achieved.

SUMMARY:

As was stated, DOA does concur with most of the recommendations provided in this audit. We also appreciated the frank exchange of ideas during the exit conference and the willingness of your staff to listen to DOA's concerns. We did, however, expect that the final audit report would address more of these concerns. The matters raised during the exit conference and in this letter are important to DOA, and that is why we have made detailed comments about them in this response. We look forward to acting on the recommendations with which we concur and appreciate your consideration of our comments.

Sincerely,

John Lewis, Director

c: Mike Manion, Deputy Director and Chief Legal Counsel
Matt Van Syckle, Chief Information Officer (interim), State Information Technology Services Division
Cheryl Gray, Administrator, State Financial Services Division
Anjenette Schafer, Administrator State Human Resources Division
Matt Pugh, Deputy Administrator, State Financial Services Division
Dean Mack, Deputy Administrator, State Human Resources Division