LEGISLATIVE AUDIT DIVISION

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

Deputy Legislative Auditors:
Cindy Jorgenson
Joe Murray

MEMORANDUM

TO: Legislative Audit Committee Members

FROM: Amanda Sayler, Senior Information Systems Auditor

CC: Department of Administration
John Lewis, Director
Mike Manion, Deputy Director and Chief Legal Counsel
Tim Bottenfield, Chief Information Officer
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

DATE: January 2020

RE: Information Systems Audit Follow-Up (20SP-01): Statewide Accounting, Budgeting, and Human Resources System (SABHRS) Governance and Security Management (17DP-03 and 17DP-04)

ATTACHMENT: Original Information Systems Audit Summary

Introduction

Our Information Systems audit report titled *Statewide Accounting, Budgeting, and Human Resources System (SABHRS) Governance and Security Management (17DP-03 and 17DP-04)* was issued to the Legislative Audit Committee in June 2018. The audit included five recommendations to the Department of Administration (DOA). We conducted follow-up work to assess implementation of the report recommendations. This memorandum summarizes the results of our follow-up work.

Overview

Our audit presented information about the governance and security management of the SABHRS Human Resources and Financial Services. SABHRS is a statewide system with applications used by agencies to report disposition, use, and receipt of public resources. Additionally, it assists in the administration of state human resource information and practices. DOA defines the application as separate systems with oversight split between two divisions: State Human Resources Division (SHRD) and State Financial Services Division (SFSD). The audit found that the decentralization of the applications increased the risk of security weaknesses. Although the agency maintains some policies and procedures regarding access management controls, it lacked documentation and audit of several security controls required by state policy.

Our audit contained five recommendations to DOA. DOA concurred with four recommendations and did not concur with one. The agency reported one recommendation complete, one being implemented, and two partially implemented. Based on follow-up work, we found DOA implemented one recommendation, partially implemented three recommendations, and did not implement one recommendation.

Background

All SABHRS applications are used by accounting 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 public is able to review data generated by the system via the State of Montana's website.

SABHRS has transitioned from a centralized management under State Information Technology Services Division (SITSD) to a more decentralized model that segregates SABHRS Human Resources (HR) and SABHRS Financial Services (FS). This means each application serves a different function and is managed independently between SHRD and SFSD. The responsibilities for operation and maintenance of SABHRS are divided among four areas at DOA.

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

Due to the decentralized nature of management, our audit reviewed security management, oversight procedures, and the efficiency of the decentralized structure. Our audit work determined DOA was missing controls needed to properly ensure security over SABHRS. Although the department maintained some access control policies and procedures, the department lacked management and oversight of key security controls including security training, risk assessments, and security plans. Our work also identified several inefficiencies in the current organizational structure and found the agency did not have defined roles and responsibilities for key information technology (IT) support staff. The recommendations in the report included defining security controls such as implementing security plans, clearly identifying security and support roles, administering security training, and completing an audit of internal controls. We also recommended DOA reevaluate current organizational structure to identify efficiencies that can be gained, such as streamlining security and staff responsibilities concerning IT and security.

Audit Follow-Up Results

Follow-up work included discussions with the agency, reviews of position descriptions, roles and responsibilities, and available security plans. We found DOA increased some security controls including designating a formal security manager over SABHRS, developed a security plan for SFSD, and defining and updated IT support staff titles, roles, and responsibilities. However, we found DOA did not address other key security weaknesses, such as creating a security plan for SHRD, or auditing SABHRS internal controls including business process controls.

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.**

Implementation Status – *Partially Implemented*

The purpose of this recommendation was to ensure SABHRS is properly secured. At the time of the audit, information security duties such as technical security set up and configuration, were being fulfilled by a supervisor of a vacant security analyst position and SHRD developers. Information security duties demands the attention of at least one full-time staff and requires separation from business ownership and responsibilities. SABHRS maintains and processes some the state's most important data and therefore it is important for the agency to provide assurance there are security controls in place and that someone has dedicated responsibility over security. Since the audit, DOA has assigned information security duties to SITSD's Information Security Manager. This position develops and maintains security policies, controls, and identifies resolutions for security weaknesses. DOA has also implemented a security plan for SFSD. However, SHRD has yet to implement a security plan.

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.**

Implementation Status – *Implemented*

SABHRS is used by all state agencies and therefore each agency designates a representative as its agency security officer. This position is the first line of approval for the creation of a new user in any SABHRS applications. The purpose of this recommendation was to address the lack of awareness and training at the other agencies that use and manage SABHRS. For example, agency security officers did not have clear understanding of their responsibilities. The title of agency security officer was confusing, considering DOA is primarily responsible for security of the data contained in SABHRS. Security officers manage their respective agencies' user controls for SABHRS, which is commonly known as account management. To provide clarity to agency staff, we recommended they update the title from agency security officers to account managers. Our follow-up work found the titles of the agency security officers had changed to better reflect their duties as account managers. In December 2019, the agency sent the online training to account managers. Managers had until the end of December 2019 to complete it.

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.

Implementation Status – *Being Implemented*

The purpose of recommending that DOA finalize the agency's internal controls and risk assessment and then complete an audit on the controls was to ensure the department can identify and prioritize high risk areas needing attention, such as data security and threats. At the time of the audit, we found DOA was in the process of establishing an entity-wide risk assessment program of internal business controls. They had anticipated completing a plan to audit the controls and determine if risks were assessed accurately by fiscal year 2019. During follow-up work, we found the internal business control risk assessment was completed, but risk assessments covering the system control families for HR had not yet been conducted. An audit of HR internal controls has not been completed. The agency indicated certain financial internal controls also had yet to be audited. When discussing responsibilities with the various areas of SABHRS management, it was unclear who has responsibility to conduct these internal audits and tests, related to security. It is important these are done to understand how controls are working and take this into consideration for future risk assessments.

RECOMMENDATION #4

We recommend the Department of Administration:

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

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

Implementation Status – *Partially Implemented*

The purpose of this recommendation was to address potential inefficiencies within DOA organizational structure, specific to the divisions that manage SABHRS. The agency undertook several reorganizations over the past 10 years, which changed how IT is governed across the agency and the state. When these changes occurred, clear responsibilities, especially over key control areas such as security, were not defined. During our follow-up work we found roles and responsibilities had been defined, but the agency did not reevaluate the support structure to identify efficiencies. DOA believed they implemented the recommendation because they discussed the recommendation in one meeting. However, the department could not provide evidence showing any kind of analysis was conducted to support the decision not to make changes to the support structure. We also found during follow-up work there was no coordination between SHRD, SFSD, the director's office, and SITSD. We found in areas such as development of a security plan and conducting risk assessments and audits, they did not have clear paths for completion, showing who was responsible, or coordination points between the various divisions. This indicated a lack of coordination still exists, which increases risk for inefficiency. The agency was unable to provide clear documents outlining staff workloads, coordination efforts, and clear roles and responsibilities from staff and leadership.

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 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.**

Implementation Status – *Not Implemented*

The agency did not concur with this recommendation. DOA indicated in its follow-up response it is strengthening its IT governance by continuing to incorporate industry best practices. It is evaluating other options to ensure governance is achieved. We continue to stand by the recommendation and believe implementation of one of these steps would ensure more efficient and complete governance over SABHRS.

S:\Admin\IS\Follow-up\20SP-01-SABHRS-17DP-03-04-memo.docx/ah