A Report
to the
Montana
Legislature

Information Systems

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

Department of Administration

June 2010

Legislative Audit
Division

10DP-03

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. Areas of expertise include business, accounting, education, computer science, mathematics, political science, and public administration.

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.

Direct comments or inquiries to:
Legislative Audit Division
Room 160, State Capitol
P.O. Box 201705
Helena, MT 59620-1705
(406) 444-3122

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

LEGISLATIVE AUDIT DIVISION

Tori Hunthausen, Legislative Auditor
Monica Huyg, Legal Counsel

Deputy Legislative Auditors
James Gillett
Angie Grove

June 2010

The Legislative Audit Committee
of the Montana State Legislature:

We conducted an Information Systems audit of the Statewide Accounting, Budgeting, and Human Resources System maintained and operated by the Department of Administration to assist in the administration of financial and human resource records within state government. The focus of the audit was to ensure specific controls are in place and processes are working as intended.

This report contains two recommendations for strengthening controls over user access and segregation of duties.

We wish to express our appreciation to department personnel for their cooperation and assistance.

Respectfully submitted,

/s/ Tori Hunthausen

Tori Hunthausen, CPA
Legislative Auditor

Table of Contents

Appointed and Administrative Officials

Department of Administration

Janet R. Kelly, Director

Sheryl Olson, Deputy Director

Paul Christofferson, Administrator, State Accounting Division

Paula Stoll, Administrator, State Human Resource Division

Cheryl Grey, Chief, SABHRS Finance and Budget Bureau

Randy Morris, Chief, HR Information Services Bureau

Dominick Speranza, DBA Manager, IT Services Division

Report Summary

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

SABHRS is an enterprise computer application implemented by the State of Montana to assist state agencies in recording the disposition, use, and receipt of public money and property in accordance with state law. SABHRS also assists in the administration of human resource information, including the generation of a biweekly payroll. The responsibilities for all SABHRS maintenance and support are divided among three Department of Administration entities:

- SABHRS Finance and Budget Bureau, responsible for managing the financial subsystem.
- Human Resources Information Services Bureau, responsible for the human resources subsystem.
- Information Technology Services Division, responsible for providing technical support.

On an annual basis an Information Systems audit is conducted to identify and test key controls over the application to ensure the system is operating as intended to maintain the integrity of business processes and data. This audit focused on modifications to SABHRS, system access and reviews, and segregation of duties.

Overall, SABHRS has controls in place to help ensure the system operates as intended; however, we did identify areas where controls could be strengthened. This report includes two recommendations:

1. Strengthening user access approval and review procedures – Human Resources Information Services Bureau personnel have excessive access (not limited to individuals with a business need) and assignment and review of access does not include all Bureau section managers and may not identify all excessive access.
2. Segregating duties between vendor management and voucher creation – State Accounting Division personnel have the ability to create and pay a vendor without secondary approval.

Chapter I – Introduction

Introduction

On an annual basis, an Information Systems audit is conducted of controls within the Statewide Accounting, Budgeting and Human Resources System (SABHRS), including a review of modifications made to SABHRS functionality. The intent of the SABHRS audit is to identify and test key controls over the application to ensure the system continues to operate as intended. Based on our work, we provide a limited distribution memorandum detailing the SABHRS control environment to Legislative Audit Division staff for consideration during their audits. This report presents the findings of our review and includes recommendations for strengthening controls.

Background

SABHRS is an enterprise computer application implemented by the State of Montana to assist state agencies in reporting the disposition, use, and receipt of public resources. (§17-1-102, MCA). SABHRS also assists in the administration of human resource information, including the generation of a biweekly payroll. The responsibilities for all SABHRS maintenance and support are divided among three Department of Administration (DOA) entities:

- SABHRS Finance and Budget Bureau, responsible for managing the financial system
- Human Resources Information Services Bureau, responsible for the human resources system
- Information Technology Services Division, responsible for providing technical support

SABHRS includes subsystems: Financials, Human Resources Management, and a budget development component. This audit focused on specific controls within the Human Resources and Financials subsystems, and does not include the budget development component. Within each of these subsystems are modules providing different functionality to users.

The Financials subsystem includes seven modules:

- General Ledger (GL) – a single repository of all financial transaction records entered into SABHRS, including payables and receivables. When a transaction is entered, a journal line is generated. The journal line is then posted to the GL, where it can be used in a number of accounting functions including reconciliations, trial balances, and maintenance.
- Accounts Payable (AP) – responsible for processing vouchers and payment to state vendors. The AP also transmits voucher data through interfaces with the GL and Warrant Writer.

- Accounts Receivable (AR) – processes incoming payments and supplies billing statements. AR data is transferred and posted to the GL.
- Purchasing – stores vendor information, purchase orders, recurring contracts, and procurement card information for all state agencies. Purchasing functionality includes processing purchase order information into the AP module. Purchasing transaction data is posted to the GL in the form of journals.
- Asset Management – stores assets and calculates depreciation, gains, losses, trade-in values, etc.
- eBill – allows agency customers to pay fines and fees through a web interface.
- Billing – manages customer billing.

The Human Resources Management subsystem includes five modules:

- Human Resources – all personnel, job position, and employment records are entered and maintained here.
- Time and Labor – employee's time is entered, validated, and approved within this module, resulting in compensation for employees.
- Benefits Administration – responsible for defining benefits (medical, retirement, leave, etc.) for which an employee is eligible.
- Payroll – responsible for calculating earnings, deductions, and net pay based on information entered within the previous three Human Resources modules.
- Workforce Management – responsible for signup and attendance for training events, conferences, etc. Records are maintained to monitor the development of employees as they progress through their careers.

All of these modules include functionality relied on by agency users in the management of financial and human resources.

Audit Objective

Based on audit planning, the overall objective was to determine if specific controls within SABHRS operate as intended.

Audit Scope and Methodology

To help identify key controls, we reviewed system processes and changes, and considered prior audit testing and SABHRS delivered functionality.

Methodology included interviews of staff, query and analysis of SABHRS data, and observation of SABHRS operations. We evaluated the control environment using state policies, SABHRS security policies, and criteria established by the IT Governance Institute and National Institute of Standards and Technology. The audit was conducted in accordance with Government Auditing Standards published by the United States Government Accountability Office.

Prior Audit Follow-up

In the previous SABHRS audit report (09DP-03), we made two recommendations to DOA. We recommended DOA establish a level of protection in SABHRS regarding identification of duplicate payments and reconcile potential duplicate payments identified during our audit. The department made changes to system settings in SABHRS requiring every payment to be checked for duplication. If an exception is identified, the payment can be saved, but not processed. The previous audit compiled a list of potential duplicates and submitted it to DOA for reconciliation; this audit determined all transactions were reconciled.

DOA reorganized SABHRS Support Services Bureau. The previous audit determined a communications mechanism regarding decision-making and dispute resolution was not in place between the newly formed entities, and recommended DOA develop a formal methodology. We reviewed two service level agreements in place and both contained language addressing our recommendation.

Chapter II – System Controls

Introduction

System controls are a combination of automated and manual processes and activities which help ensure data confidentiality, integrity, and availability. Although there can be thousands of systems controls, some have more impact on system performance than others. For this audit of the Statewide Accounting, Budgeting, and Human Resources System (SABHRS), we focused on system controls related to user access and segregation of duties to ensure specific controls operate as intended.

SABHRS is a commercial-off-the-shelf system. When a system such as SABHRS is implemented, system functionality is considered delivered, or baseline. However, the system may not perform as expected or needed by the implementing organization, thus requiring system modification. We reviewed SABHRS modifications occurring since last year's audit. Overall, the Human Resources subsystem had 48 modifications and the Financials subsystem had 19. We reviewed each to determine if baseline functionality was affected and ascertained modifications did not affect baseline SABHRS processing. Our audit work then focused on areas requiring continual review, such as user access and segregation of duties.

User Access

In order for agency personnel to use SABHRS, they must be granted access to the application. SABHRS security documentation requires agency security officers to determine if employees need access and what level of access should be allowed. Access roles have been created to implement user access. Each access role relies on supporting permissions delineating which SABHRS screens users can access and dictates if users can view, change, or delete SABHRS information. In many instances, a single user can be assigned multiple access roles with supporting permissions. Any permission can be assigned to multiple roles, potentially creating incompatible access and allowing users to exploit or damage the system or view data they should not see. Because excess user access can present considerable risk, we reviewed specific access in both the Human Resources (HR) and Financials subsystems as follows:

1. Interface Files – Agencies use interface files to transfer data from subsystems to SABHRS. We determined access to critical interface file data is limited to individuals with a business need.
2. Automated Processing – Much of SABHRS functionality occurs through automated processing. We determined controls prevent users from making unauthorized changes to automated processing files.
3. Warrants – Warrants are created based on payment data residing in SABHRS. We reviewed access to the payment data as well as the warrant print files and determined access to be limited to individuals with a business need.

We identified excess access within HR as follows:

1. Employee Benefits and Deductions – Benefit and deduction rates in SABHRS must be regularly updated. We reviewed access of individuals able to modify benefits and deduction rates and determined access is not limited to individuals with a business need.
2. Garnishments – Garnishments can be set, removed, or changed during the payroll process. We queried SABHRS for individuals who can perform garnishment activity and determined access is not limited to individuals with a business need.
3. Line Item Changes – Line item changes allow payroll errors to be corrected during the payroll process. We queried SABHRS for users with the ability to create line item changes and determined access is not limited to individuals with a business need.
4. Unconfirm Process – The unconfirm process is used to reverse the payroll process if it fails prior to completion of payroll. We queried SABHRS for users who can run unconfirm and determined access is not limited to individuals with a business need.

Our review covered access by all agencies including SABHRS personnel. Each instance of excessive access noted above involved SABHRS Human Resources Information Services Bureau (HRIS) personnel, and increases the risk of intentional or unintentional changes to state employee benefits and payroll data. When we approached HRIS section management with our results, they agreed access was not limited to the need for job duties and should be reduced. Management also noted in some cases, HRIS personnel had authorized access for a job position; however, when personnel moved to a new position, authorized access for the original position was not removed. We also determined the process used to assign HRIS personnel access does not always include HRIS section management. Assignment of specific SABHRS access only requires approval from the requesting section and the SABHRS security officer. As a result, access to specific SABHRS sections can be granted without the knowledge of that section's management.

In addition to the process used to gain access, reviews are another method of controlling user access. We determined user access reviews are performed by specific SABHRS personnel; however, we noted the following:

- The reviews are performed by personnel not in the section for which access is being reviewed. For example, payroll staff access is not reviewed by anyone in the Payroll section.
- The reviews are based on SABHRS roles, not supporting permissions. Without reviewing permissions, which can be assigned to multiple roles, users could have more access than needed to perform their job duties.
- The results are not always provided to the SABHRS section management for which the review is being performed.

When considering user access, it is important for program managers to control system access. As such, program managers should be involved in assignment and review of access requests.

Recommendation #1

We recommend the Department of Administration ensure:

A. *SABHRS section management approve SABHRS Human Resources Information Services personnel access requests.*

B. *Human Resources Information Services user access reviews are based on permissions, not just roles, and involve Human Resources section management.*

Segregation of Duties

Another consideration during the assignment of user access roles is segregation of duties. Industry standards require a segregation of duties between roles preventing an individual from performing incompatible activities. SABHRS security documentation also requires individuals only be assigned the minimum level of access needed to perform job duties. We reviewed segregation of duties controls within the Payroll, Accounts Receivable, Accounts Payable, and General Ledger modules of SABHRS. Generally, SABHRS enforces a segregation of duties by not allowing transactions to be processed unless an individual other than a transaction's creator approves the transaction. We determined this is true within Payroll and Accounts Receivable; however, we identified exceptions within both Accounts Payable and General Ledger.

Accounts Payable

When payment vouchers are created in the Accounts Payable module of the Financials subsystem, SABHRS functionality includes a segregation of duties preventing a user from both entering and approving their own vouchers. However, we determined a process exists which bypasses the existing control. Some agencies, including the Montana University System, account for activity in a separate system and transfer the information into SABHRS using interface files. To allow interface files to be automatically processed, without having to provide a separate approval for every transaction in the file, preapprovals were created. However, we determined individuals were also using preapprovals to directly enter transactions into SABHRS. As a result, when an individual creates a payment voucher using preapprovals, they could create and approve their own voucher increasing the risk of an unauthorized payment. We queried SABHRS to determine how many transactions using preapprovals were created between March 1, 2009, and March 12, 2010. The query returned 19,955 transactions, excluding interface file transactions, indicating regular use of preapprovals. Of these, 205 were payments and the rest were either payment corrections or reversals.

We spoke with accounting management at the three agencies with the largest number of transactions processed using preapprovals. We determined the agencies generally use preapprovals to make corrections, adjustments, etc., to transactions processed through the interface files. This is necessary for tracking purposes; since interface files are created and processed using preapprovals, any subsequent changes to transactions in an interface file must occur using preapprovals or tracking would be incorrect. Preventing use of preapprovals, although beneficial in protecting against unauthorized transactions, would inhibit agency personnel in performing required job duties. To compensate, DOA relies on each agency to have its own system of controls to ensure unauthorized payments are not created when using preapprovals.

State Vendor Management

Vendor management is the responsibility of the State Accounting Division (SAD). To prevent SAD employees from creating and potentially making an unauthorized payment to a vendor, duties must be segregated. SAD personnel with the ability to create a vendor should not be able to create and authorize a payment voucher to the same vendor. We queried SABHRS and identified five SAD staff with this access. Although SABHRS delivered functionality normally prevents a user from creating and approving their own payment vouchers, all five SAD staff can do both when using preapprovals. We reviewed transactions performed by all five staff and determined they did not perform any transactions using preapprovals; however, the potential exists.

Recommendation #2

We recommend the Department of Administration segregate user access roles to prevent State Accounting Division personnel from creating a vendor, as well as creating and approving payment vouchers.

Department of Administration

Department Response

DEPARTMENT OF ADMINISTRATION
DIRECTOR'S OFFICE

BRIAN SCHWEITZER, GOVERNOR

JANET R. KELLY, DIRECTOR

STATE OF MONTANA

(406) 444-2032
FAX (406) 444-6194

MITCHELL BUILDING
125 N. ROBERTS, RM 155
PO BOX 200101
HELENA, MONTANA 59620-0101

June 4, 2010

Ms. Tori Hunthausen
Legislative Auditor
Legislative Audit Division
PO Box 201705
Helena, MT 59620-1705

RE: Information Systems Audit #10DP-03: Statewide Accounting, Budgeting, and Human Resources System (SABHRS)

Dear Ms. Hunthausen:

The Department of Administration has reviewed the Information Systems Audit of the Statewide Accounting, Budgeting, and Human Resources System (SABHRS) and the recommendations contained therein. Our response to the recommendations appears below:

Recommendation #1:

We recommend the Department of Administration (DOA) ensure:

A. SABHRS section management approve SABHRS Human Resources Information Services (HRIS) personnel access requests.

B. Human Resources Information Services user access reviews are based on permissions, not just roles, and involve Human Resources section management.

Response:

A. Concur. HRIS section supervisors will approve access requests based upon business need.

B. Concur. The HRIS Bureau management will perform an annual review of each employee's user access and ensure access is based

"AN EQUAL OPPORTUNITY EMPLOYER"

upon a business need and approved by the appropriate HRIS section supervisor.

Recommendation #2:

We recommend the Department of Administration segregate user access roles to prevent State Accounting Division personnel from creating a vendor, as well as creating and approving payment vouchers.

Response: Conditionally Concur. Currently, DOA's State Accounting Division's (SAD's) user access roles segregate the creation and approval of vouchers. The underlying cause of the audit recommendation is the use of preapproved payment transactions. SAD plans to eliminate the preapproval process.

The one exception will be in the Department of Revenue's (DOR's) Business and Income Taxes Division. The division's personnel are carefully monitored. Further, SAD's internal monitoring and manual approval process reduces risks to an acceptable level.

My staff and I appreciated the courtesy and professionalism of the legislative audit staff in conducting this audit. The Department always views the audit process as an opportunity for improvement and welcomes your input.

The Department's Corrective Action Plan (CAP) is attached.

Sincerely,

Janet R Kelly

Janet R. Kelly, Director

Attachment

Preliminary Response
Corrective Action Plan (CAP): Audit Report #10DP-03
Statewide Accounting, Budgeting, and Human Resources System (SABHRS)
Department of Administration
June 4, 2010

Agency	Recommendation #	Does this affect a federal program?	CFDA # (if previous YES)	Management View	CAP – Corrective Action Plan	Person responsible for CAP	Target Date
61010 DOA	**Recommendation #1** We recommend the Department of Administration (DOA) ensure:						
	A. SABHRS section management approve SABHRS Human Resources Information Services (HRIS) personnel access requests.	No		Concur	HRIS section supervisors will approve access requests based upon business need.	Randy Morris	9/1/2010
	B. Human Resources Information Services user access reviews are based on permissions, not just roles, and involve Human Resources section management.	No		Concur	The HRIS Bureau management will perform an annual review of each employee's user access and ensure access is based upon a business need and approved by the appropriate HRIS section supervisor.	Randy Morris	9/1/2010
61010 DOA	**Recommendation #2** We recommend the Department of Administration segregate user access roles to prevent State Accounting Division personnel from creating a vendor, as well as creating and approving payment vouchers.	No		Conditionally Concur	Currently, DOA's State Accounting Division's (SAD's) user access roles segregate the creation and approval of vouchers. The underlying cause of the audit recommendation is the use of preapproved payment transactions. SAD plans to eliminate the preapproval process. The one exception will be in the Department of Revenue's (DOR's) Business and Income Taxes Division. The division's personnel are carefully monitored. Further, SAD's internal monitoring and manual approval process reduces risks to an acceptable level.	Paul Christofferson	8/1/10