



Susan Montee, JD, CPA
Missouri State Auditor

ADMINISTRATION

Statewide Accounting System Internal Controls

December 2010
Report No. 2010-160



auditor.mo.gov



Susan Montee, JD, CPA
Missouri State Auditor

YELLOW SHEET

Findings in the audit of Statewide Accounting System Internal Controls

Terminated Users

Office of Administration (OA) management had not fully established policies and procedures to ensure user accounts with access to the Statewide Advantage for Missouri (SAM II) system were removed timely upon a user's employment termination or transfer. We found at least 100 former state employees still had access to the system after terminating employment from the agencies for which the users had been granted access. SAM II policies and procedures place the responsibility for determining who is given access to the system, including identification of accounts belonging to terminated and transferred users, with the agency employing the users. Although agencies are responsible for submitting requests to add, change, or remove user access rights, OA management is ultimately responsible for security of the system.

User Account Controls

The SAM II system is vulnerable to the risk of unauthorized transactions being processed or unauthorized actions being performed on user accounts. Current management practices do not always prevent users from approving their own transactions in the Financial system without approval by another party. In addition, security administrators of the Financial and Human Resources systems were able to create, modify, or remove user accounts from the systems without supervisory review.

Change Management

OA management had not fully established policies and procedures to segregate access to SAM II software libraries or to ensure software libraries were fully protected from unauthorized changes. In addition, OA management had not fully established or documented policies and procedures for several other key change management functions.

All reports are available on our Web site: auditor.mo.gov

Statewide Accounting System Internal Controls

Table of Contents

State Auditor's Report	2
------------------------	---

Introduction	
Background	4
Scope and Methodology	4

Management Advisory	
Report - State Auditor's	
Findings	
1. Terminated Users	6
2. User Account Controls	7
3. Change Management	9



SUSAN MONTEE, JD, CPA
Missouri State Auditor

Honorable Jeremiah W. (Jay) Nixon, Governor
and
Kelvin L. Simmons, Commissioner
Office of Administration
Jefferson City, Missouri

We have audited certain internal controls, including security controls, designed to protect data and information maintained by the Statewide Advantage for Missouri (SAM II) system. Our audit was conducted to evaluate the internal controls in the SAM II system designed to ensure the security and the materially accurate processing and reporting of financial data and information.

The objectives of our audit were to:

1. Evaluate the security controls designed to ensure the confidentiality, integrity, and availability of data and information maintained by the SAM II system.
2. Evaluate the internal controls in the SAM II system designed to ensure the materially accurate processing and reporting of financial data and information.
3. Evaluate the economy and efficiency of certain management practices and information system control activities.

We determined Office of Administration management established many of the critical internal controls necessary for protecting data and information maintained by the SAM II system. However, management needs to further strengthen controls over user accounts to ensure the confidentiality, integrity, and availability of data and information maintained in the SAM II system. We determined internal controls in the SAM II system, designed to ensure the materially accurate processing and reporting of financial data and information, were functioning as designed. We also determined certain weaknesses exist in management practices and operations, which increase the risk of unauthorized changes being made to the system.

We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform our 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 such a basis.



Susan Montee, JD, CPA
State Auditor

The following auditors participated in the preparation of this report:

Director of Audits:	John Luetkemeyer, CPA
Audit Manager:	Jeffrey Thelen, CPA
In-Charge Auditor:	Lori Melton, M.Acct., CPA
Audit Staff:	Patrick M. Pullins, M.Acct. Erica Joannes

Statewide Accounting System Internal Controls

Introduction

Background

The Statewide Advantage for Missouri (SAM II) system is the state's integrated financial and human resource management system, providing accounting, budgeting, procurement, inventory, and payroll and personnel capabilities for state departments and agencies. The SAM II system processes revenue, expenditure, payroll, transfer, and adjusting transactions.

Our audit work focused on the SAM II Financial system and the SAM II Human Resources (HR) system. The Financial system, used for purchasing, payment, and revenue processing, was implemented in July 1999. The HR system, used to maintain and process employment and payroll information, was implemented in phases between November 2000 and June 2001. Users are granted access rights to these systems to add or change data or to have inquiry-only access. As of December 2009, there were 5,122 Financial system user accounts and 5,740 HR system user accounts.

The SAM II system is managed by the Office of Administration (OA). The OA Division of Accounting is responsible for the Financial and HR systems, including maintaining policies and procedures for use of the systems. Technical support is provided by the systems development and programming staff under the OA Information Technology Services Division (ITSD) and the software vendor that customized the SAM II system for the state. ITSD security administrators are responsible for processing security requests to add, change, or remove user access to the Financial and HR systems.

Changes to the functionality of the SAM II system are processed by ITSD programmers with access to software libraries that maintain source code. Source code is the written programming code used to produce an executable program in the SAM II system. Software libraries are maintained in separate environments for programs being developed or modified, programs being tested by users, and programs approved for use.

According to accepted standards, security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Confidentiality refers to preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information. Integrity relates to guarding against improper information modification or destruction, and availability ensures timely and reliable access to and use of information.

Scope and Methodology

The scope of our audit included internal controls established and managed by the OA, policies and procedures, and other management functions and compliance issues in place during the year ended June 30, 2010. Our scope



Statewide Accounting System Internal Controls Introduction

did not include internal controls that are the responsibility of the management of agencies using the SAM II system.

Our methodology included conducting interviews with appropriate officials and staff; obtaining and reviewing available policies and procedures, federal laws, and other applicable information; and performing testing.

We obtained data files from the SAM II system of user accounts having access to the HR system as of December 2009 and to the Financial system as of December 2009 and June 2010. To ensure completeness of the data, we grouped the accounts by agency and compared the results to a separate list of state agencies whose users should have access to the systems. We reviewed the approval rights of the Financial system user accounts to determine if each user was restricted from approving transactions the user had also entered in the system. We gave OA officials a list of all user accounts we found that could approve transactions the user had also entered in the system. Although we used computer-processed data from the SAM II system to identify user accounts and related information, we did not rely on the results of any processes performed by this system in arriving at our conclusions. Our conclusions were based on our review of the controls over user accounts.

We obtained the employment records of all state employees for fiscal years 2001 to 2010 from the HR system. We matched these records to user accounts with SAM II system access to determine if any terminated employees had active user accounts. We gave OA officials a list of all terminated employees we found who had active access to the SAM II system. Although we used computer-processed data from the HR system for our audit work, we did not rely on the results of any processes performed by this system in arriving at our conclusions. Our conclusions were based on our review of the issues specific to the audit objectives.

We based our evaluation on accepted state, federal, and international standards and best practices related to information technology security controls from the following sources:

- Missouri Adaptive Enterprise Architecture (MAEA)
- National Institute of Standards and Technology (NIST)
- Government Accountability Office (GAO)
- IT Governance Institute Control Objectives for Information and related Technology (COBIT)

Statewide Accounting System Internal Controls

Management Advisory Report

State Auditor's Findings

1. Terminated Users

Office of Administration (OA) management had not fully established policies and procedures to ensure user accounts with access to the Statewide Advantage for Missouri (SAM II) system were removed timely upon a user's employment termination or transfer. We found at least 100 former state employees still had access to the system after terminating employment from the agencies for which the users had been granted access.

According to the Missouri Adaptive Enterprise Architecture (MAEA), agencies must have a procedure in place for administrators to be notified of the departure of users in a timely manner. SAM II policies and procedures place the responsibility for identification of accounts belonging to terminated and transferred users with the agency employing the users. Agencies are responsible for determining who is given access to the system and for ensuring that all individuals who have access still need the access. Once a user no longer needs access, the agency is supposed to submit a form to the security administrators requesting the user's access to the system be removed.

To help agencies ensure access rights are removed promptly, the security administrators perform additional tasks including reviewing SAM II accounts for inactivity. Human Resources (HR) system security administrators also compared the list of users with active SAM II HR accounts to employment records and notified agency security personnel of accounts belonging to terminated or transferred employees. Agency security personnel were then responsible for initiating the process to remove user accounts.

In November 2009, a new automated method was developed to provide reports to agency security personnel of HR accounts assigned to terminated employees. The automated reporting method was implemented in phases, with the final agencies granted access in May 2010. However, during this interim period, security administrators did not continue to notify agency security personnel of the HR accounts assigned to terminated or transferred employees. We found 16 HR system user accounts active as of December 31, 2009, for which the employee had terminated state employment.

Financial system security administrators had not reviewed the employment records for terminated or transferred employees. According to an OA official, Financial system security administrators had not been granted access to the employment records to identify terminated or transferred employees. As a result, Financial system security administrators had to rely on security personnel at each agency to identify user accounts that should be removed. We found 88 Financial system user accounts active as of December 31, 2009, for former employees who had terminated employment or transferred to another agency.



Statewide Accounting System Internal Controls
Management Advisory Report - State Auditor's Findings

Although agencies are responsible for submitting requests to add, change, or remove user access rights, OA management is ultimately responsible for security of the system. Without effective procedures to remove access, terminated employees could continue to have access to critical or sensitive resources or have opportunities to sabotage or otherwise impair entity operations or assets, according to the GAO.

Recommendation

The OA periodically review user accounts to ensure access of terminated or transferred employees is removed.

Auditee's Response

The OA will continue to provide security audit reports to the agencies who are responsible for determining who is given access to the system and for ensuring that all individuals who have access still need access. In addition, the OA provides reports to all agencies showing employees in termination status that still have access to the Human Resources system, to assist agencies with their responsibility to submit requests to remove access for terminated employees. It is not appropriate for the OA to automatically remove access for employees in termination status, because at times, agencies perform a termination action as a part of a position transfer, rather than complete termination of employment.

2. User Account Controls

The SAM II system is vulnerable to the risk of unauthorized transactions being processed or unauthorized actions being performed on user accounts. Current management practices do not always prevent users from approving their own transactions in the Financial system. In addition, security administrators of the Financial and HR systems were able to create, modify, or remove user accounts from the systems without supervisory review.

2.1 Transaction approvals

A weakness in the Financial system security settings allows users to create a transaction and then apply approval to the same transaction without review or additional approval from another party. While OA management had taken steps to limit this risk, we found 50 Financial system user accounts that had authority to enter and approve their own expenditure transactions as of June 30, 2010.

Each user account in the Financial system is assigned certain rights and privileges from a list of available options. Among these rights and privileges are creating and approving transactions. Each agency is also able to assign rules to transactions to specify approvals necessary based on dollar value and transaction type. If a user is allowed rights to both create and approve a transaction, and these rights satisfy the rules established for the transaction, the user would be able to create and approve the same transaction without review or additional approval from an independent party.

The Financial system does have a control to restrict a user from approving their own transaction. According to OA management, not all agencies want to fully implement this additional control because some agencies allow data



Statewide Accounting System Internal Controls
Management Advisory Report - State Auditor's Findings

entry users to apply the first approval to their own transactions before an additional approval is later applied by another user.

By allowing users to approve their own transactions without another approval, there is an increased risk that inappropriate or unauthorized transactions may be processed.

2.2 Review of security administrator actions

OA management did not require supervisory review of system logged user account actions performed by security administrators of the Financial or HR systems. As part of job responsibilities, security administrators have the ability to create and modify user accounts. OA policy requires a security request form to be approved by agency personnel before a user account is created. The security administrators are responsible for ensuring the security request forms received had been approved by appropriate agency personnel. However, a reconciliation of the approved security request forms received to user account changes was not performed. Changes made by the security administrators were logged, but OA officials said the logs were not reviewed regularly. Routinely monitoring security administrator actions can help identify significant problems and deter employees from inappropriate activities.

Recommendations

The OA should:

- 2.1 Continue to work with agencies to limit the risk of users approving their own transactions and establish policies to ensure future users are not granted this right.
- 2.2 Perform periodic supervisory reviews of defined actions performed by security administrators.

Auditee's Response

- 2.1 *The OA will continue our regular review of individual security settings and continue working with the agencies to prevent users from approving their own transactions. The OA will further review the default security settings of document types to ensure appropriate approval is required on all transactions.*
- 2.2 *The OA maintains the system logs produced by the statewide accounting system. These logs show all security actions taken and would be the source of information for supervisory reviews of the actions performed by security administrators. Given the actual size of the logs the OA will evaluate alternative approaches to assess random samples and investigate other alternatives to perform a more robust review of system security controls.*



3. Change Management

OA management had not fully established or documented a change management methodology or the policies and procedures for guiding the software modification process. According to the MAEA, change management defines the roles, processes, standards, and deployment of software through the development, test, and production environments. Change management is necessary to control versions, scope, and development of software and provides accountability and responsibility for changes. Good change management provides strict control over the implementation of system changes and thus minimizes corruption to information systems, according to the GAO.

3.1 Programmer access to production code

OA management had not fully established policies and procedures to segregate access to the SAM II Financial or HR system software libraries or to ensure software libraries were fully protected from unauthorized changes. Any change to an information system can potentially have significant effects on the overall security of the system, according to accepted standards. As a result, organizations should define, document, approve, and enforce access restrictions associated with changes to the information system.

Programmers responsible for development and maintenance of source code were allowed to move approved source code into the production environment. Management review procedures were not sufficient to ensure the source code placed in production was the approved version. As a result, a programmer could modify source code or insert new code without detection. Programmers should not be allowed to independently develop, test, and move program changes into production, according to the GAO. In addition, access to software libraries should be limited and the movement of programs and data among libraries should be controlled by personnel independent of both the user and the programming staff. Organizations should also conduct periodic audits of information system changes to determine whether unauthorized changes have occurred, according to accepted standards.

Inadequately segregated duties increase the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, or computer resources damaged or destroyed, according to the GAO.

3.2 Change management documentation

OA management had not fully documented policies and procedures for guiding modifications to the SAM II system. OA management had established procedures for some change controls; however, management had not completed the process of establishing and documenting policies and procedures for these controls. Change management policies and procedures should describe the change management process and address purpose, scope, roles, responsibilities, compliance, and implementation of security controls, according to the GAO.



Statewide Accounting System Internal Controls
Management Advisory Report - State Auditor's Findings

We found OA management had not fully established or documented policies and procedures for the following key change management functions:

- Overall change control policy
- Change control authorizations
- Testing of changes
- Reversal of changes

Overall change control
policy

OA management had not fully established the change control management policies and procedures necessary to ensure changes to the SAM II system were appropriately documented. According to the GAO, policies and procedures should be designed to reasonably assure changes to application functionality are authorized and appropriate, and unauthorized changes are detected and reported promptly.

ITSD staff use a change tracking system for managing requests related to software problems or program enhancements. OA officials said the change tracking system is used for all changes. However, there is no documented policy requiring use of the change tracking system. As a result, there is a risk that some changes made to the system could be unapproved, go undetected, or be made in manners that conflict with expected procedure.

Change control
authorizations

OA officials said every SAM II system change request is reviewed and approval obtained from business process owners prior to moving the change into production. However, a documented policy indicating who should approve changes has not been developed. Accepted standards require organizations develop a formal, documented information system maintenance policy and ensure changes are approved.

Testing of changes

OA management had not fully documented testing requirements for changes to the SAM II system. OA officials said test plans were developed for all changes. However, documentation was only maintained for tests performed, not planned tests. In addition, the tests only contained steps for testing the modifications the change was intended to make. A baseline set of tests, performed on all changes to ensure changes did not cause unexpected effects, had not been established. According to accepted standards, a test plan should define the levels and types of tests to be performed, be based on organization-wide standards, and be approved by relevant parties.

Reversal of changes

Change control procedures did not require programming staff to document procedures for the reversal of a change to the SAM II system if the implementation did not operate as intended. Accepted standards require that, as part of the implementation plan for a proposed change, consideration should be given to how the change would be reversed in the event of a system error or other unforeseen complication. Such a plan, also called a



Statewide Accounting System Internal Controls
Management Advisory Report - State Auditor's Findings

"back-out" plan, is used to help system administrators restore the information system to its state before the changes were implemented.

OA officials said if a change to the SAM II system failed, the most likely action would be to restore the prior version of the system from backups; however, the officials acknowledged the process to restore a portion of the system, including how to identify the relevant portions to recover and how to restore the relevant portion of code to the production environment, were not documented in change control procedures. As a result, there is increased risk that personnel making changes to the system would be unable to effectively and efficiently restore the system in the event of an unforeseen system error.

Recommendations

The OA should:

- 3.1 Restrict programmers from moving source code to the production environment. If resource constraints prohibit segregation of duties, sufficient supervisory review of programmer actions should be established.
- 3.2 Fully establish and document change management policies and procedures.

Auditee's Response

- 3.1 *The OA recognizes that segregation of programmer duties is highly desired. However, resource constraints prohibit complete segregation of duties. The very limited number of programmers supporting the statewide accounting system are required to have access rights to make changes and move changes into the production environment to resolve problems during critical processing periods (i.e., payroll), and at other times for on-going support purposes.*

The OA recognizes that periodic supervisory audits of system changes are a best practice. We will increase supervisory review to determine whether unauthorized changes have occurred, to the extent that resources are available.

- 3.2 *The OA will document change control policies and procedures, including change control authorizations, testing of changes, and reversal of changes.*