Office of Missouri State Auditor

Nicole Galloway, CPA

Statewide Accounting System Internal Controls

Report No. 2016-133
December 2016

auditor.mo.gov

Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Findings in the audit of the Statewide Accounting System Internal Controls

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.

Terminated Users

The system is vulnerable to the risk of unauthorized or inappropriate transactions being processed because user accounts of terminated employees are not always removed timely. The audit found 18 former employees still had access to the system 30 days or more after terminating employment from the state agency that granted the user access.

Policies and Procedures

Office of Administration (OA) management has not fully established policies and procedures to segregate programmer access to the SAM II system software libraries, including the production environment, or to ensure software libraries are fully protected from unauthorized changes. OA management did not require supervisory review of system logged user actions performed by the SAM II security administrators. OA management has improved documentation of change management policies and procedures by developing test plan standards, including a baseline set of tests to be performed on all changes; however a policy for reversing changes still needs to be fully developed. While contingency planning activities have improved, OA management has not documented the formal assignment of specific responsibilities for maintaining the contingency plans. Similar conditions were noted in prior audit reports.

In the areas audited, the overall performance of this entity was **Good**.*

*****The rating(s) cover only audited areas and do not reflect an opinion on the overall operation of the entity. Within that context, the rating scale indicates the following:

Excellent: The audit results indicate this entity is very well managed. The report contains no findings. In addition, if applicable, prior recommendations have been implemented.

Good: The audit results indicate this entity is well managed. The report contains few findings, and the entity has indicated most or all recommendations have already been, or will be, implemented. In addition, if applicable, many of the prior recommendations have been implemented.

Fair: The audit results indicate this entity needs to improve operations in several areas. The report contains several findings, or one or more findings that require management's immediate attention, and/or the entity has indicated several recommendations will not be implemented. In addition, if applicable, several prior recommendations have not been implemented.

Poor: The audit results indicate this entity needs to significantly improve operations. The report contains numerous findings that require management's immediate attention, and/or the entity has indicated most recommendations will not be implemented. In addition, if applicable, most prior recommendations have not been implemented.

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

Statewide Accounting System Internal Controls
Table of Contents

NICOLE GALLOWAY, CPA
Missouri State Auditor

Honorable Jeremiah W. (Jay) Nixon, Governor
and
Douglas E. Nelson, 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. This audit was conducted in fulfillment of our duties under Chapter 29, RSMo. The objectives of our audit were to:

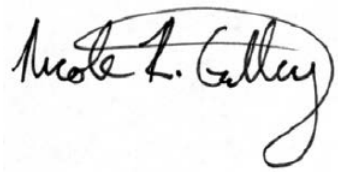
1. Evaluate the system's internal controls over significant management and financial functions.

2. Evaluate compliance with certain legal provisions.

3. Evaluate the economy and efficiency of certain management practices and information system control activities.

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.

For the areas audited, we identified (1) deficiencies in internal controls, (2) no significant noncompliance with legal provisions, and (3) the need for improvement in management policies and procedures. The accompanying Management Advisory Report presents our findings arising from our audit of the SAM II system.



Nicole R. Galloway, CPA
State Auditor

The following auditors participated in the preparation of this report:

Director of Audits:	Douglas J. Porting, CPA, CFE
Audit Manager:	Jeffrey Thelen, CPA, CISA
In-Charge Auditor:	Patrick M. Pullins, M.Acct., CISA
Audit Staff:	Marian Rader, M.Acct., CPA, CFE
	Michelle Johnson

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 process transactions or to have inquiry-only access. As of June 2016, there were 3,160 Financial system user accounts and 1,850 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. OA 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, 2016. Our scope

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

Our methodology included reviewing written policies and procedures, interviewing various OA personnel, and performing testing. We obtained an understanding of the applicable controls that are significant within the context of the audit objectives and assessed whether such controls have been properly designed and placed in operation. We tested certain of those controls to obtain evidence regarding the effectiveness of their design and operation. We also obtained an understanding of legal provisions that are significant within the context of the audit objectives, and we assessed the risk that illegal acts, including fraud, and violation of contract or other legal provisions could occur. Based on that risk assessment, we designed and performed procedures to provide reasonable assurance of detecting instances of noncompliance significant to those provisions.

We obtained data files from the SAM II system of user accounts having access to the HR and Financial systems as of June 2016. 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 did not find any instances where a user could approve transactions the user had also entered in the system.

We obtained employment records of all state employees from the SAM II system. We matched these records to user accounts with SAM II system access to determine if any terminated employees had active user accounts. We provided 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 SAM II 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)
- ISACA (previously known as the Information Systems Audit and Control Association)

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

1. Terminated Users

The Statewide Advantage for Missouri (SAM II) system is vulnerable to the risk of unauthorized or inappropriate transactions being processed because user accounts of terminated employees are not always removed timely.

Office of Administration (OA) management could reduce the risk of unauthorized access by increasing efforts to identify user accounts assigned to former employees and by providing periodic reminders to agency security coordinators of the importance of promptly removing user access assigned to former employees. We found 18 former employees still had access to the system 30 days or more after terminating employment from the state agency that had granted the user access.

According to the Missouri Adaptive Enterprise Architecture (MAEA),[1] agencies must have a procedure in place for the timely notification of administrators when a user no longer needs access. 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 all individuals who have access still need the access. When a user no longer needs access, SAM II procedures require agency security coordinators to submit a form to the OA security administrator requesting removal of the user's access to the system.

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. The OA has documented procedures in place for the SAM II security administrators to regularly check for SAM II user IDs associated with terminated employees and report any findings to agency security coordinators. In addition, the OA occasionally provides user security reports to agencies listing SAM II users and access levels for use by agency security coordinators in reviewing user access. However, these controls are not consistently effective since terminated employees continued to have active SAM II access.

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 Government Accountability Office (GAO).

[1] The Enterprise Architecture includes standards, policies and guidelines established by OA management. The Enterprise Architecture is made up of several information technology domains, including domains dedicated to security and information. The domains define the principles needed to help ensure the appropriate level of protection for the state's information and technology assets.

A similar condition was noted in our prior two audit reports.

Recommendations

The OA periodically review user accounts to ensure access of terminated or transferred employees is removed and provide more frequent reminders to agency security coordinators of the importance of promptly removing user access assigned to former employees.

Auditee's Response

The OA reviews user account access on a regular basis. The OA will continue oversight by providing employee access reports to all agencies on a monthly basis. Additionally, the OA has already implemented an improved policy of immediately inactivating users in SAM II Financial and SAM II HR once the individual appears on the termination report. This will remove the ability for activity to occur until the user is officially deleted.

2. Policies and Procedures

While OA management has improved documentation of certain policies and procedures, additional effort is needed to fully develop policies and procedures for SAM II system administration. Access to software libraries has not been appropriately segregated, a documented review of security administrator actions is not performed, a policy for the reversal of programming changes has not been established, and the responsibility for maintaining contingency plans has not been formally documented. The resulting internal control weaknesses leave the system vulnerable to unauthorized changes being made, inappropriate access being granted, and less assurance the contingency plans will remain current.

2.1 Programmer segregation of duties

OA management has not fully established policies and procedures to segregate programmer access to the SAM II system software libraries, including the production environment, or to ensure software libraries are 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 are allowed to move source code into the production environment. Management review procedures are not sufficient to ensure the source code placed in production is the approved version. As a result, a programmer can modify source code or insert new code without detection. According to an OA official, the agency does not have sufficient personnel to segregate the library management functions from programmers and instead relies on supervisory review. However, supervisory reviews are not documented to provide evidence of the review's effectiveness.

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. Management can reduce the risk of unauthorized changes and help ensure the appropriateness of changes by performing and documenting supervisory review of programmer actions if adequate resources are not available to properly segregate duties.

2.2 Security administrator supervision

OA management did not require supervisory review of system logged user actions performed by the SAM II security administrators.

As part of their job responsibilities, the SAM II security administrators have the ability to create and modify user accounts. OA policy requires approval of a security request form by agency personnel before a user account is created. The security administrators are responsible for ensuring the security request forms received have been approved by appropriate agency personnel. However, a reconciliation of the approved security request forms received to user account changes is not performed. Changes made by the security administrators are logged, but OA management said the logs are not reviewed regularly. According to OA officials, the agency does not have sufficient personnel to segregate duties or to regularly review changes made by security administrators.

Routinely monitoring security administrator actions can help identify significant problems and deter employees from inappropriate activities.

2.3 Change management

OA management has improved documentation of change management policies and procedures by developing test plan standards, including a baseline set of tests to be performed on all changes; however a policy for reversing changes still needs to be fully developed.

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.

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. OA management stated written procedures have not been developed because procedures are dependent on the specific change being implemented.

Failure to document reversal procedures for proposed changes leaves the system at risk of extended failure and outages if a change fails to produce the expected results and necessary resources to reverse the change are not readily available.

2.4 Contingency planning

OA management has improved documentation of contingency plans and related processes by (1) performing and maintaining documentation of a risk assessment, (2) completing the development of a comprehensive disaster recovery plan, and (3) ensuring the results of contingency plan tests are properly documented and processed. However, OA management has not documented specific responsibilities for oversight and maintenance of the SAM II contingency plans.

Contingency plans establish policies, procedures, and technical measures that can enable a system to be recovered quickly and effectively following a service disruption or disaster, according to the MAEA. According to accepted standards, contingency plans should be reviewed for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan. While responsibility for maintaining the contingency plans has been informally assigned, OA management has not documented the formal assignment of specific responsibilities for maintaining the contingency plans.

Without a formal designation of staff responsible for oversight and maintenance, there is increased risk that contingency plans and related policies and procedures may not remain current, potentially impacting the ability to promptly restore the system and related business functions.

Similar conditions previously reported

Similar conditions to sections 2.1, 2.2, and 2.3 were noted in our prior 2 audit reports, and a similar condition to section 2.4 was noted in our prior audit report.

Recommendations

The OA:

2.1 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 performed.

2.2 Perform periodic supervisory reviews of defined actions performed by security administrators.

2.3 Continue to enhance change management policies and procedures by documenting procedures for the reversal of changes to the SAM II system if the implementation did not operate as intended.

2.4 Formally assign responsibilities for oversight and maintenance of the contingency plan to appropriate personnel.

Auditee's Response

2.1 The OA recognizes that segregation of programmer duties is desired. However, resource constraints prohibit complete segregation of duties. 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.

2.2 Departments request security to be set up and changes as needed. The OA reviews those requests and, when acceptable, establishes the requested security settings. Each department receives a summary of its users' security for review. The OA will ensure that each month, these reports are received. The OA believes this separation of duties is sufficient to ensure proper actions. However, the OA will periodically conduct a random sample of security actions to provide additional oversight.

2.3 The OA will attempt to document a generic policy for reversing changes to SAM II.

2.4 The OA will update its existing SAM II disaster recovery plan to assign responsibilities for oversight and maintenance of the plan.