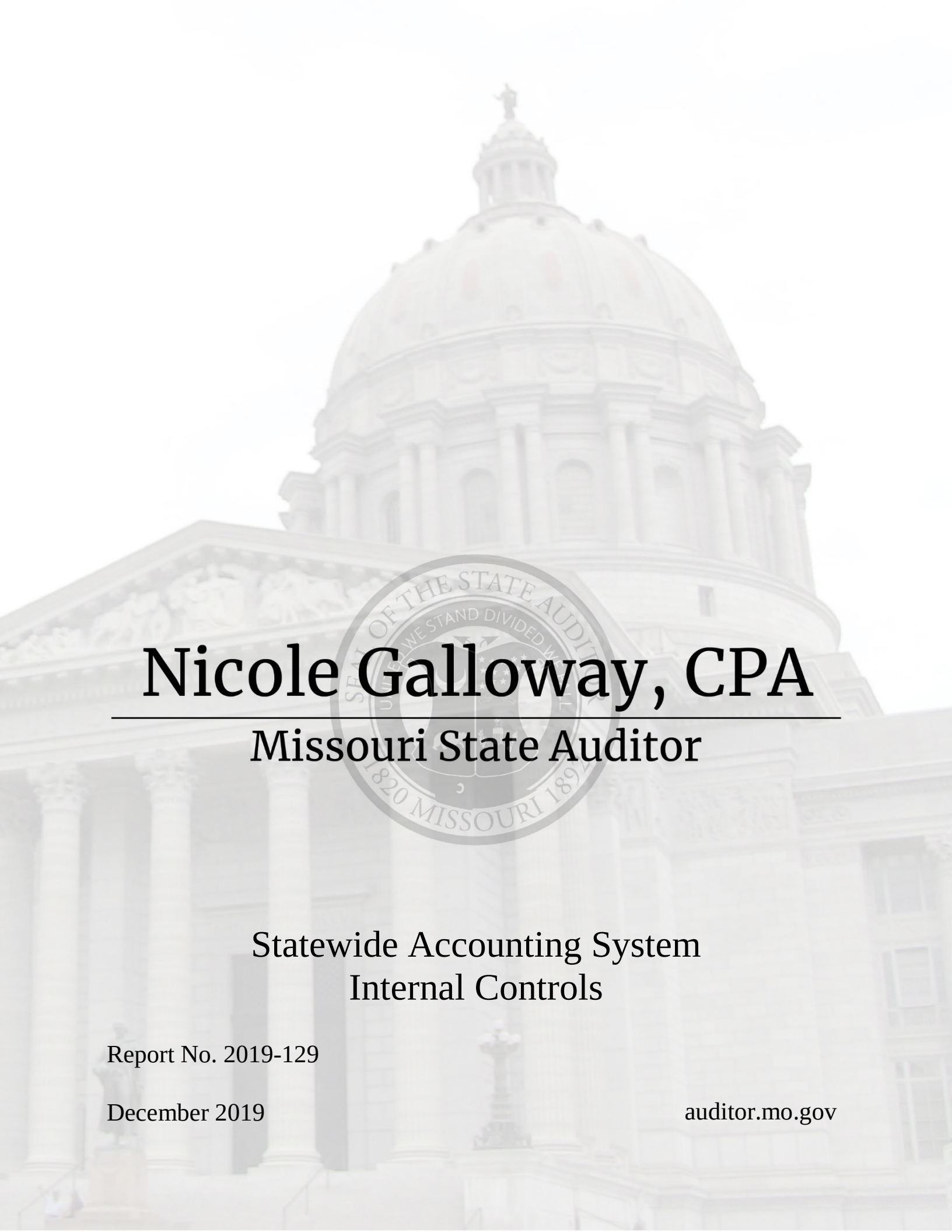


Nicole Galloway, CPA

Missouri State Auditor

Statewide Accounting System Internal Controls

Report No. 2019-129

December 2019

auditor.mo.gov

Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Findings in the audit of the Statewide Accounting System Internal Controls

User Account Management	The Statewide Advantage for Missouri (SAM II) and MissouriBUYS systems are vulnerable to the risk of unauthorized or inappropriate transactions being processed because user accounts of terminated employees are not always removed timely. 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.
Security Administration	Controls in place over the centralized security administration function are not adequate, increasing the risk of improper activity in the SAM II system. Central security administrators have access to the SAM II system in excess of that required for their job duties. Office of Administration (OA) management does not require documented supervisory review of system logged user actions performed by the SAM II central security administrators.
Policies and Procedures	OA management has not fully developed policies and procedures for SAM II system 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 has not fully developed a policy for reversing changes in the event of unforeseen complications in the implementation process. OA management has not documented specific responsibilities for oversight and maintenance of the SAM II contingency plans.

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

*****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.

Statewide Accounting System Internal Controls
Table of Contents

NICOLE GALLOWAY, CPA
Missouri State Auditor

Honorable Michael L. Parson, Governor
and
Sarah H. Steelman, 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:

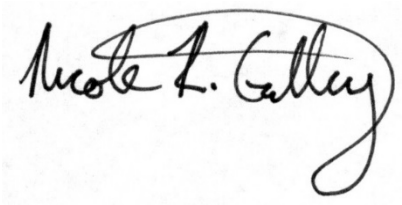
1. Evaluate the system's internal controls over significant management and financial functions.

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:

Senior Director:	Douglas J. Porting, CPA, CFE
Audit Manager:	Alex R. Prenger, M.S.Acct., CPA, CISA, CFE, CGAP
In-Charge Auditor:	Patrick M. Pullins, M.Acct., CISA, CFE
Audit Staff:	Joanne P. Lewis

Statewide Accounting System Internal Controls Introduction

Background

The state of Missouri processed approximately $40 billion of financial transactions during state fiscal year 2019. These transactions were processed to support the operations of 25 separate state legislative, judicial and executive entities. The system of record for these transactions is the Statewide Advantage for Missouri (SAM II) system. SAM II is supported by several other interfaced systems, including the MissouriBUYS eProcurement solution.

SAM II

The 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 on the SAM II system focused on two primary components, 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 2019, there were 2,849 Financial system user accounts and 1,659 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).[1] 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.

During fiscal year 2019, the state began the process of replacing the SAM II system. In April 2019, the state selected a contractor that is currently working

[1] Prior to July 2019, the state also contracted with the system vendor for additional support services. Due to rising costs, this contract was allowed to expire, and the system is now solely supported by the ITSD. If the state requires additional support from the vendor, an hourly charge applies.

to develop the request for proposals for a new Enterprise Resource Planning system and will help select the vendor(s) to provide and implement the new system.

MissouriBUYS

The MissouriBUYS system is the state's eProcurement system, which establishes a virtual marketplace between state departments and agencies, and vendors. The system replaced the state's previous On-Line Bidding and Vendor Registration systems. The system was fully implemented during 2018 and integrates with the SAM II system for financial processing. As of September 2019, there were 1,381 MissouriBUYS user accounts.

The MissouriBUYS system is provided by a third-party contractor using a Software-as-a-Service (SaaS) model. Under this model, the state pays a subscription fee to use the software, and the contractor is responsible for hosting the software on a password-secured website, and all maintenance and support of the software. The state has elected to retain responsibility for user account administration, and placed that responsibility within the OA Division of Accounting.

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 (1) internal controls established and managed by the OA, (2) policies and procedures, and (3) other management functions and compliance issues in place during the year ended June 30, 2019. Our scope did not include internal controls that are the responsibility of the management of agencies using the SAM II and MissouriBUYS systems.

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 2019. 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 obtained data files from the MissouriBUYS system of user accounts having access to the system as of September 2019. During testing, we determined this data was inaccurate, and a second data request of users with access as of October 2019 was obtained. Potential errors identified in our testing of September data were confirmed in the October dataset.

We obtained employment records of all state employees from the SAM II system. We matched these records to user accounts with SAM II or MissouriBUYS system access to determine if any terminated employees had active user accounts. We provided OA management a list of all terminated employees we found who had active access to the SAM II or MissouriBUYS systems.

Although we used computer-processed data from the SAM II and MissouriBUYS systems for our audit work, we did not rely on the results of any processes performed by these systems 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

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

1. User Account Management

The Statewide Advantage for Missouri (SAM II) and MissouriBUYS systems are vulnerable to the risk of unauthorized or inappropriate transactions being processed because user accounts of terminated employees are not always removed timely. Additionally, two Financial system users are not prevented from approving transactions they created.

1.1 SAM II terminated users

The SAM II system's terminated user accounts 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 promptly removing user access assigned to former employees. We found 21 former employees still had access to the SAM II system 30 days or more after terminating employment from the state agency that had granted the user access. These users were employed by the agencies (and non-agency entities) identified in Table 1 below.

Table 1: SAM II terminated users by entity

Entity	Financial system terminated users	HR system terminated users
Conservation	0	1
Corrections	3	0
Higher Education	0	2
Legislature	1	0
Mental Health	3	0
Missouri Consolidated Health Care Plan	0	1
Natural Resources	1	0
Public Safety[1]	1	6
Social Services	2	0
Total	11	10

Source: SAO analysis of SAM II user accounts

[1] Department of Public Safety users include users from the Missouri Capitol Police (1 HR user), Missouri State Highway Patrol (1 Financial and 2 HR users), Missouri Veteran's Commission (1 HR user), and the Office of the Director (2 HR users).

According to the Missouri Adaptive Enterprise Architecture (MAEA),[2] agencies must have a procedure in place for the timely notification of administrators when a user no longer needs access. SAM II policies and

[2] 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.

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, 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 provides user security reports to agencies listing SAM II users and access levels for use by agency security coordinators, who are expected to review 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).

1.2 MissouriBUYS terminated users

The MissouriBUYS system's terminated user accounts are not always removed timely. We found 41 former employees still had access to the MissouriBUYS system 30 days or more after terminating employment. These users were employed by the agencies (and non-agency entities) identified in Table 2.

Table 2: MissouriBUYS terminated users by entity

Entity	Number of terminated users
Agriculture	1
Corrections	18
Elementary and Secondary Education	2
Health and Senior Services	3
Judiciary	1
Mental Health	3
Natural Resources	4
Office of Administration	1
Public Safety[1]	4
Secretary of State	1
Social Services	1
Transportation	2
Total	41

Source: SAO analysis of MissouriBUYS user accounts

[1] Department of Public Safety users include users from the Missouri Veteran's Commission.

Similar to the process for the SAM II system described in section 1.1, agency security coordinators for the MissouriBUYS system are expected to review monthly security reports provided by the OA to identify any users whose system access should be removed. Agency security coordinators submit removal request forms to MissouriBUYS security administrators, who remove the access. However, these controls are not consistently effective since terminated employees continued to have active MissouriBUYS access.

User access can be removed by three methods: account deletion, suspension, or inactivation. Deletion and suspension are security administrator actions that take immediate effect. An account's circumstances affect the choice between deletion and suspension. However, both methods are effective due to their immediate, deliberate nature.

Inactivation is an automated system control, independent of security administrator action. Inactivation triggers when the account does not access the system within 180 days. This trigger can be delayed, potentially indefinitely, if the account regularly accesses the system within 180 days, which resets the countdown, making inactivation a less effective control.

Our review of the 41 accounts identified two scenarios, each representing a different weakness in current procedures.

- For 39 accounts, according to OA management, the agency security coordinator did not submit a removal request to the MissouriBUYS security administrator for more than 30 days after the user terminated

employment. For 32 of 39 accounts, this delay exceeded at least 6 months. Although the agencies eventually submitted removal requests for all accounts, many of these requests did not occur until October 2019, after audit staff alerted the applicable agencies. While 38 of 39 accounts were in an inactive status, the remaining account was active as of October 4, 2019, for a user who terminated employment in May 2019. The OA did not receive a removal request for this account until October 7, 2019, after audit staff alerted the agency.

- For 2 accounts, according to OA management, OA received the removal requests within a week of the user terminating employment. While these requests were received in April and May 2019, the accounts remained active as of October 2019. Because security administrators had not deleted or suspended the accounts, and a minimum of 180 days had not passed for the inactivity control to trigger, these accounts allowed continued access.

OA management indicated if an account is already inactive when a removal request is received, often no further action is taken to delete or suspend the account. We observed this situation for 6 additional inactive accounts, despite associated removal requests being submitted within 30 days of the users terminating employment.

While deletion, suspension and inactivation all prevent an account from accessing the system, relying on inactivation leaves the system at risk for an extended period (a minimum of 180 days, versus 30 days) and increases opportunities for an account to be reactivated accidentally or maliciously.

1.3 Transaction approvals

OA management has not fully corrected a weakness in the Financial system security settings that allows users to create a transaction and then apply approval to the same transaction without review or additional approval from another party.

Each user account in the Financial system is assigned certain rights and privileges from a list of available options, including the authority to create and approve 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. While OA management has taken steps to limit this risk, we identified two Financial system user accounts had authority to enter and approve the same expenditure transaction as of June 2019.

Allowing users to approve their own transactions without another approval increases the risk that inappropriate or unauthorized transactions may be processed.

Similar conditions previously reported

A condition similar to section 1.1 was noted in our prior 3 audit reports, and a condition similar to section 1.3 was noted in our 2010 and 2013 audit reports.

Recommendations

The OA:

1.1 &
1.2 Continue monthly reviews of SAM II and MissouriBUYS user accounts to ensure access of terminated or transferred employees is removed, and develop additional procedures to identify accounts no longer needing access. In addition, consistently and timely remove access to MissouriBUYS by deleting or suspending accounts upon receiving a removal request.

1.3 Continue to work with agencies to limit the risk of users approving transactions they create and establish policies to ensure future users are not granted this right.

Auditee's Response

1.1 &
1.2 We do not agree that risk associated with unauthorized access to the SAM II system is as significant as reported in the audit because a user must access the state network in order to access the accounting system. The audit fails to acknowledge or evaluate this initial security measure. OA will continue to provide oversight of user accounts. System limitations exist related to deleting accounts in MissouriBUYS; however, OA will review the possibility of actively suspending accounts.

1.3 We concur.

Auditor 's Comment

1.1 &
1.2 While the SAM II system has the referenced control of requiring users to be on the state network, the risk of inappropriate access is not fully reduced because certain users can access the state network from remote locations. Further, the control is not effective in situations where a user transfers from one state agency to another, and thus legitimately retains access to the state network. Failing to remove the accounts also leaves them vulnerable to unauthorized access by others, such as a former co-worker or supervisor who may know the former employee's user name and password. The most effective way to reduce the risk of inappropriate access is to timely disable the accounts of the users in question.

2. Security Administration

Controls in place over the centralized security administration function are not adequate, increasing the risk of improper activity in the SAM II system.

The SAM II system decentralizes responsibility for providing user access to the system. Each agency designates a security coordinator, who reviews and approves requests from staff of that agency to access the SAM II system, and periodically reviews reports provided by OA to ensure agency users' access remain appropriate. Agency security coordinators do not have access rights in the SAM II system to directly make changes. They instead submit documentation (request forms and supporting information as necessary) requesting any additions, changes, or removals of users to an OA-centralized SAM II security administrator, who has the access rights necessary to process the requested changes.

2.1 Security administrator duties

Central security administrators have access to the SAM II system in excess of that required for their job duties.

Every user of the SAM II system is assigned a user profile, which controls the actions a user is allowed to perform. These actions can include the ability to create, view, edit, approve, and delete transactions; modify system security; change system configuration options; and other specific functions. While some functions are broad and low-risk (for example, most users can view any transaction statewide), others are high-risk and tightly controlled (for example, few users can view security tables, and fewer still can modify them).

The security profile assigned to security administrators grants them excessive access to the SAM II system. In addition to their security administration functions, these security administrators have the ability to enter transactions including cash receipts, journal vouchers, manual checks, transfers, and expenditure documents including employee expense accounts. To reduce risk of improper activity, the ability to enter transactions should be disabled.

OA management noted that the security administrators, by virtue of their duties, can change their level of access to the system at any time by self-assigning profiles. For this reason, it is important that compensating controls be established, such as periodic managerial review of system changes made by the security administrators to ensure changes are supported by appropriate documentation, and documented formal monitoring of certain high-risk accounts and changes (see section 2.2).

Accepted standards require that users be allocated the minimum access rights necessary to perform their assigned job functions, and that access to security functions be explicitly assigned. Allowing users access to the system in excess of that required for their job responsibilities increases the risk of improper activity occurring without collusion between multiple users.

2.2 Security administrator supervision

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

As part of their job responsibilities, the SAM II central security administrators have the ability to create and modify user accounts. OA policy requires approval of a security request form by the agency security coordinator before a user account is created. The central security administrators are responsible for ensuring the security request forms received have been approved by appropriate agency personnel. OA management indicated they periodically compare logged changes made by the central security administrators against approved security request forms submitted by agency security coordinators. However, they also indicated these comparisons are neither documented nor performed regularly. According to OA management, the agency does not have sufficient personnel to segregate duties or to regularly review changes made by central security administrators.

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

A similar condition was noted in our prior 3 audit reports.

Recommendations

The OA:

2.1 Disable security administrators' ability to enter transactions in the SAM II system. Because of their ability to re-enable this permission, implement documented compensating controls to mitigate this risk.

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

Auditee's Response

2.1 Security has been changed.

2.2 Monthly reviews of MissouriBUYS system security administrators' activities have been occurring and will continue. OA will periodically conduct a random sample of SAM II administrator security actions to provide additional oversight.

3. Policies and Procedures

OA management has not fully developed policies and procedures for SAM II system administration. Access to software libraries has not been appropriately segregated, 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 and less assurance the contingency plans will remain current.

3.1 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 OA management, the agency does not have sufficient personnel to segregate the library management functions from programmers and instead relies on supervisory review. However, supervisory reviews performed are not documented to provide evidence of their 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.

3.2 Change management

OA management has not fully developed a policy for reversing changes in the event of unforeseen complications in the implementation process.

According to the MAEA, change management defines the roles, processes, and standards for 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 told us standard written procedures have not been developed because procedures are dependent on the specific change being implemented. However, the OA has not taken any action to formally document any change-specific procedures within its change documentation.

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.

3.3 Contingency planning

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. OA management indicated responsibilities related to contingency planning have not been formalized because contingency operations are very similar to regular operations and therefore require no specialized knowledge. In addition, with the process of replacing the SAM II system underway, OA management indicated expending limited resources on the existing system would not be practical.

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 3.1, and 3.2 were noted in our prior 3 audit reports, and a similar condition to section 3.3 was noted in our prior 2 audit reports.

Recommendations

The OA:

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 performed and documented.

3.2 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.

3.3 Ensure adequate, complete documentation of the system is maintained throughout the entire system life-cycle, including replacement. This documentation should include formally designating responsibility for creating and maintaining contingency plans to ensure the system is available in the event of a disaster.

Auditee's Response

3.1 OA recognizes that segregation of programmer duties is desired. However, resource constraints prohibit complete segregation of duties. OA recognizes that periodic supervisory audits of system changes are a best practice, however, we also recognize given the age of the system, few to no changes are occurring. While this finding was very relevant 10 years ago, we believe the applicability of the concern is greatly reduced or eliminated in the current environment.

3.2 Since OA is making few to no changes given the age of the accounting system, OA does not believe it is a good use of taxpayer resources to draft a policy and procedure with little to no value.

3.3 OA has successfully managed to maintain operations during recent disasters including snow storms, floods, and a tornado that unexpectedly shut down offices for two days. The morning of the recent tornado in Jefferson City was the critical day for processing state employee payroll. Even though offices were closed, employees were paid timely and without interruption because advances in technology allow staff to work from anywhere and procedures are documented sufficiently that staff completing unfamiliar tasks were successful. OA believes we have proven our abilities to maintain systems with the existing documentation.