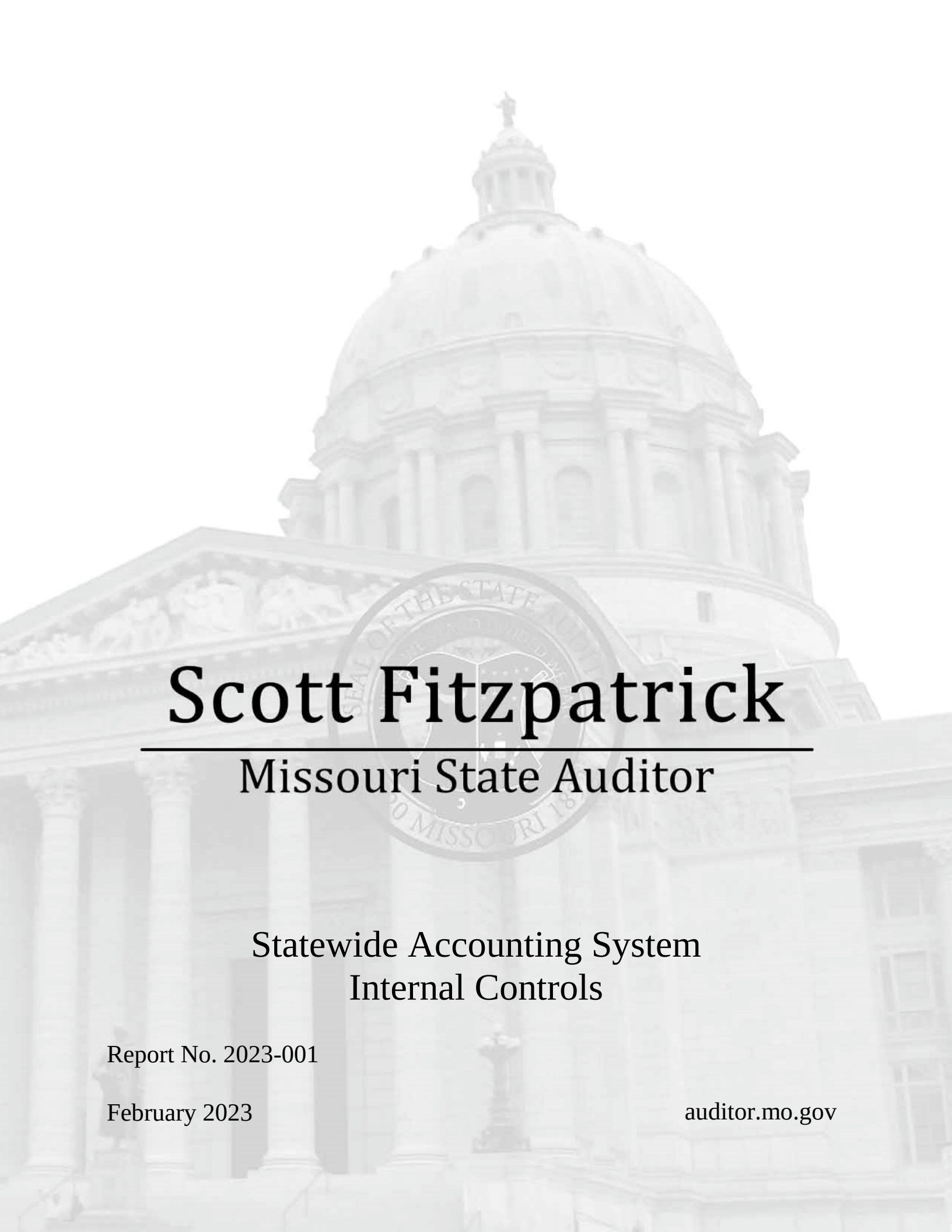

Scott Fitzpatrick

Missouri State Auditor

Statewide Accounting System Internal Controls

Report No. 2023-001

February 2023

auditor.mo.gov

Scott Fitzpatrick
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. OA management has not fully corrected a weakness in the SAM II 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.
Security Administration	OA management does not require supervisory review of system-logged user actions performed by the SAM II central security administrator, resulting in increased risk of unauthorized activities.
Policies and Procedures	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

SCOTT FITZPATRICK
MISSOURI STATE AUDITOR

Honorable Michael L. Parson, Governor
and
Kenneth J. Zellers, 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 operations and financial functions, including the effectiveness of information security controls for protecting the confidentiality, integrity, and availability of significant systems and information.

2. Evaluate compliance with certain legal provisions.

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, and (2) no significant noncompliance with legal provisions.

The accompanying Management Advisory Report presents our findings arising from our audit of the SAM II system.

Scott Fitzpatrick
State Auditor

Statewide Accounting System Internal Controls Introduction

Background

The state of Missouri processed approximately $53.7 billion of revenue and $47.0 billion of expenditure and transfer transactions during state fiscal year 2022. 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. The SAM II system is supported by several other interfaced systems, including the MissouriBUYS eProcurement solution.

According to the National Institute of Standards and Technology (NIST),[1] security controls are the safeguards or countermeasures employed within a system or an organization to protect the confidentiality, integrity, and availability of the system and its information and to manage information security risk. 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. Effective privacy controls depend on the safeguards employed within the information system that is processing, storing, and transmitting personally identifiable information (PII) and the environment in which the system operates. Organizations cannot have effective privacy without a basic foundation of information security. Without proper safeguards and controls, information systems and confidential data are vulnerable to individuals with malicious intentions who can use access to obtain sensitive data or disrupt operations.

The NIST defines cybersecurity as the process of protecting information by preventing, detecting, and responding to attacks[2] while ISACA states cybersecurity encompasses all that protects enterprises and individuals from intentional attacks, breaches, and incidents as well as the consequences.[3] Cybersecurity should be aligned with all other aspects of information security, including governance, management, and assurance. The state of being secure requires maintenance and continuous improvement to meet the needs of stakeholders and the demands of emerging cyber threats.

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

[1] NIST, Special Publication 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* p. 1, 396, 398, and 406, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>, accessed October 17, 2022.

[2] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 2018, p. 45, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>, accessed October 17, 2022.

[3] ISACA, *Transforming Cybersecurity*, 2013, p. 11.

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 April 2022, there were 2,529 Financial system user accounts and 1,531 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).[4] An ITSD security administrator is 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.

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 May 2022, there were 1,911 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

[4] 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.

account administration, and placed that responsibility within the OA Division of Accounting.

SAM II system replacement

During fiscal year 2019, the state began the process to identify a new enterprise resource planning (ERP) system to replace the SAM II system, to be named the Missouri Vital Enterprise Resource System (MOVERS). Steering committees and other teams were created for oversight and governance. Following competitive bids, in January 2022, the OA selected the Oracle Fusion Cloud Application software suite as its MOVERS solution. This selection was awarded to Mythics, Inc., an Oracle Corporation software reseller, at an estimated $142 million for up to 20 years. In August 2022, the OA selected Accenture as the MOVERS integrator, the contractor primarily responsible for implementation activities such as design, configuration, testing, and training, for $102 million over the project lifetime. Other contractors were also selected for additional MOVERS responsibilities, such as project management and independent review of implementation activities.

By September 2022, contractor implementation efforts began, state departments joined the project to exchange knowledge, and the state planned implementation in three major phases:

- Phase 1 - Budgeting: Implementation in July 2023 (beginning of fiscal year 2024)
- Phase 2 - Finance and Procurement: Implementation in July 2024 (beginning of fiscal year 2025)
- Phase 3 - Human Resources and Payroll: Implementation in January 2026 (beginning of calendar year 2026)

The state has already shifted resources from the current SAM II system toward its eventual replacement. The OA has ceased updates to the SAM II system that are not directly required by law (such as changes in tax regulations), and has minimized administrative changes related to the system (such as updating of policies and procedures and system documentation). This approach is reasonable. However, many of the issues identified in this report are repeat occurrences, detected long before the implementation of the new system began. The recommended improvements to the current system in this report should be considered during the development of the new system.

Scope and Methodology

The scope of our audit included internal controls and policies and procedures established and managed by the OA, and other management operations and financial functions and compliance issues in place during the year ended June 30, 2022. 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 internal control that is significant to the audit objectives and planned and performed audit procedures to assess internal control to the extent necessary to address the audit objectives. 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 April 2022. 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 May 2022.

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, 3 SAM II Financial system users were not prevented from approving transactions they created.

1.1 Terminated users

The SAM II and MissouriBUYS systems' terminated user accounts are not always removed timely, resulting in an increased risk of unauthorized access.

We found 28 former employees still had access to the SAM II Financial system, SAM II Human Resources (HR) system, or MissouriBUYS 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.

Table 1: SAM II and MissouriBUYS terminated users by entity

Entity	SAM II Financial users	SAM II HR users	MissouriBUYS users
Elementary and Secondary Education	2	0	4
Health and Senior Services	0	0	2
Labor and Industrial Relations	0	1	0
Mental Health	0	1	2
Missouri Consolidated Health Care Plan	0	1	0
Natural Resources	0	0	3
Office of Administration[1]	1	2	0
Public Safety[2]	2	0	1
Revenue	4	0	0
Social Services	1	0	1
Total	10	5	13

[1] The Office of Administration users include users from the Division of Facilities Management, Design and Construction (1 SAM II Financial user and 1 SAM II HR user) and the Division of General Services (1 SAM II HR user).
[2] The Department of Public Safety users include users from the Missouri State Highway Patrol (1 SAM II Financial user), the Missouri State Emergency Management Agency (1 SAM II Financial user), and the Division of Fire Safety (1 MissouriBUYS user).

Source: SAO analysis of SAM II user accounts as of April 2022 and MissouriBUYS user accounts as of May 2022

According to the Missouri Adaptive Enterprise Architecture (MAEA),[5] agencies must have a procedure in place for the timely notification of the

[5] The Enterprise Architecture includes standards, policies and guidelines established by OA Information Technology Services Division 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.

administrator when a user no longer needs access.[6] SAM II and MissouriBUYS 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, procedures require agency security coordinators to submit a form to the OA security administrator requesting removal of the user's access to the system.

OA management indicated that while the OA provides resources to agencies to identify terminated employees, including monthly user reports, OA staff cannot remove a user's access without the agency submitting a request. Agencies contacted by the SAO did not identify any specific reasons why they had failed to remove an account.

Although agencies are responsible for submitting requests to add, change, or remove user access rights, OA management is ultimately responsible for security of the systems. The OA has documented procedures in place for the central security administrator to regularly check for 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 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 system access.

In order to access the SAM II system, authorized users must be connected to the state network. While this is a strong control, it is not always effective in eliminating unauthorized access. For example, users retain access to the state network when they transfer employment between agencies. Failing to remove 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.

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).[7]

[6] OA Information Technology Services Division, MAEA, Maintaining User Accounts, February 2022, <https://oa.mo.gov/sites/default/files/CC-Maintaining-User-Accounts.pdf>, accessed October 17, 2022.

[7] GAO, Report GAO-09-232G, Federal Information System Controls Audit Manual, February 2009, p. 176 and 225, <https://www.gao.gov/assets/gao-09-232g.pdf>, accessed October 17, 2022.

1.2 Transaction approvals

OA management has not fully corrected a weakness in the SAM II 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 3 Financial system user accounts had authority to enter and approve the same expenditure transaction as of April 2022. These users were employed by the agencies identified in table 2.

Table 2: SAM II users with authority to create and approve transactions by entity

Entity	Number of users
Public Safety[1]	1
Office of Administration[2]	2
Total	3

[1] The Department of Public Safety user was from the Division of Alcohol and Tobacco Control.
[2] The Office of Administration users were from the Division of Accounting.

Source: SAO analysis of SAM II Financial user accounts

Management of the Department of Public Safety indicated the user who could enter and approve transactions could do so because the employee was primarily assigned to review and approve transactions, but needed to be able to enter transactions in the event the employee normally assigned to those duties was unavailable. However, this arrangement creates risk of inappropriate or unauthorized transactions.

OA management indicated the authority for both users to enter and approve transactions was unintended. Such authority began when the OA enabled (and ended when the OA later disabled) statewide system access for both users. Such access was intended to temporarily support the state's processing and oversight of Coronavirus Relief Fund transactions. However, while enabled, this access, combined with the users' pre-existing rights, provided the users the authority to enter and approve transactions. We confirmed that neither user had both entered and approved any transactions inappropriately during their respective 2 and 9 month period with such authority.

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 4 audit reports, and a condition similar to section 1.2 was noted in our 2010, 2013, and 2019 audit reports.

Recommendations

We recommend the OA consider the following improvements. In addition, we recommend the OA consider them, if applicable, when implementing the new statewide accounting system:

1.1 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.

1.2 Continue to eliminate the risk of users approving transactions they create and establish policies to ensure future users are not granted this ability.

Auditee's Response

The department's written response is included in the Appendix.

Auditor's Comment

The department's written response to section 1.1 states the audit fails to acknowledge or evaluate the requirement for users to access the state network in order to access the SAM II accounting system. Our report acknowledges this is a strong, but not always effective, control. 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

OA management does not require supervisory review of system-logged user actions performed by the SAM II central security administrator, resulting in increased risk of unauthorized activities.

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.

OA management indicated the security administrator, by virtue of her duties, can change her 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 administrator to ensure changes are supported by appropriate documentation, and documented formal monitoring of certain high-risk accounts and changes. Routinely monitoring security administrator actions can help identify significant problems and deter employees from inappropriate activities.

Management from the OA Division of Accounting indicated that the central security administrator is not an employee of the Division of Accounting, but rather of the Information Technology Services Division (ITSD). Accordingly they state they are unable to perform this monitoring. ITSD management has indicated they can provide the necessary information to the Division of Accounting upon request.

A similar condition was noted in our prior 4 audit reports.

Recommendation

The OA perform and document periodic supervisory reviews of defined actions performed by the security administrator. In addition, the OA should consider this, if applicable, when implementing the new statewide accounting system.

Auditee's Response

The department's written response is included in the Appendix.

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.

Changes to an information system can potentially have significant effects on the security of the system. As a result, organizations should define, document, approve, and enforce access restrictions associated with changes to the information system.[8]

[8] NIST, Special Publication 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* p. 102, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>, accessed October 17, 2022.

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.

According to the GAO,[9] access to software libraries (such as development, testing, and production) 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.[10] Organizations should also conduct periodic reviews of information system changes to determine whether unauthorized changes have occurred, according to NIST.[11]

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.[12] 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.

Configuration (i.e., change) management provides assurance that the system in operation has been configured to organizational needs and standards, that any changes to be made are reviewed for security implications, and that such changes have been approved by management prior to implementation.[13] Good

[9] GAO, Report GAO-09-232G, *Federal Information System Controls Audit Manual,* February 2009, p. 282 and 283, <https://www.gao.gov/assets/gao-09-232g.pdf>, accessed October 17, 2022.
[10] Ibid., p. 282.
[11] NIST, Special Publication 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* p. 100 and 101, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>, accessed October 17, 2022.
[12] GAO, Report GAO-09-232G, *Federal Information System Controls Audit Manual,* February 2009, p. 301, <https://www.gao.gov/assets/gao-09-232g.pdf>, accessed October 17, 2022.
[13] NIST, Special Publication 800-12 Revision 1, *An Introduction to Information Security,* p. 45, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf>, accessed October 17, 2022.

configuration management provides strict control over the implementation of system changes and thus minimizes corruption to information systems.[14]

OA's 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. 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.[15] OA management indicated standard written procedures have not been developed because the SAM II system is in the process of being replaced, thus making changes a rare occurrence.

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.[16] Contingency plans should be reviewed for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan.[17] 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 the SAM II system is in the process of being replaced.

According to accepted standards, assigning responsibilities for oversight and maintenance of the contingency plan is a crucial element of the contingency

[14] GAO, Report GAO-09-232G, *Federal Information System Controls Audit Manual,* February 2009, p. 275, <https://www.gao.gov/assets/gao-09-232g.pdf>, accessed October 17, 2022.
[15] ISACA, *Control Objectives for Information and Related Technologies 2019 Framework: Governance and Management Objectives,* November 2018, p. 197.
[16] Missouri Office of Administration - Information Technology Services Division, Missouri Adaptive Enterprise Architecture, *Contingency Plan Development, Documentation, and Technical Considerations*, November 2006, <https://oa.mo.gov/sites/default/files/CC-ContingencyPlanDevelmtDocTechConsids112806ARC.pdf>, accessed October 17, 2022
[17] Missouri Office of Administration - Information Technology Services Division, Missouri Adaptive Enterprise Architecture, *Contingency Plan Testing, Training, Exercises, and Manteca*, July 2019, <https://oa.mo.gov/sites/default/files/CC-ContingencyPlanTestingTrainingExerciseMaintenance.pdf>, accessed October 17, 2022

planning process.[18] This formal designation will continue to be an important consideration for the SAM II replacement system.

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 4 audit reports, and a similar condition to section 3.3 was noted in our prior 3 audit reports.

Recommendations

We recommend the OA consider the following improvements. In addition, we recommend the OA consider them, if applicable, when implementing the new statewide accounting system:

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 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

The department's written response is included in the Appendix.

[18] NIST, Special Publication 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* p. 115, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>, accessed October 17, 2022.

Michael L. Parson
Governor

Kenneth J. Zellers
Commissioner

State of Missouri
OFFICE OF ADMINISTRATION
Division of Accounting
570 Truman Building, 301 West High Street
Post Office Box 809
Jefferson City, Missouri 65102
(573) 751-2971
INTERNET: http://www.oa.mo.gov/acct
E-MAIL: acctmail@oa.mo.gov

Stacy Neal
Director

January 10, 2023

Honorable Scott Fitzpatrick
Missouri State Auditor
P.O. Box 869
Jefferson City, Missouri 65102

Dear Mr. Fitzpatrick:

This letter is to document formal responses to your office's audit of the Statewide Accounting System Internal Controls.

1. **The OA consider the following improvements. In addition, the OA consider them, if applicable, when implementing the new statewide accounting system:**

   1.1 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.

   Division's Response: We do not agree that risk associated with unauthorized access to the SAM II system is as significant as reported in the audit because 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 providing oversight of user accounts. System limitations exist related to deleting accounts in MissouriBUYS. The system limitations revolve around employees that establish a transaction in MissouriBUYS and subsequently transferred to another agency or leave State employ. MissouriBUYS will not allow us to delete a user with an open transaction. Therefore, we must suspend the account.

   1.2 Continue to eliminate the risk of users approving transactions they create and establish policies to ensure future users are not granted this ability.

   Division's Response: OA will continue providing oversight of user accounts.

2. **The OA perform and document periodic supervisory reviews of defined actions performed by the security administrator. In addition, the OA should consider this, if applicable, when implementing the new statewide accounting system.**

Division's Response: 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. **The OA consider the following improvements. In addition, the OA consider them, if applicable, when implementing the new statewide accounting system:**

   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.

   Division's Response: OA recognizes that segregation of programmer duties is desired. However, resource constrains 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 and its impending replacement, very few to no changes are occurring which reduces any risk. OA will determine if this restriction can be done within MOVERS, the new system currently being implemented.

   3.2 Enhance change management policies and procedures by documenting procedures for the reversal of changes to the system if the implementation did not operate as intended.

   Division's Response: Since OA is making few to no changes given the age of the accounting system and we are currently implementing MOVERS; OA does not believe it is a good use of state resources to draft a policy and procedure with little to no value.

   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.

   Division's Response: OA has successfully managed to maintain operations during the recent pandemic when state offices were closed. 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.

Sincerely,

Stacy Neal

Stacy Neal, CPA
Director, Division of Accounting