PERFORMANCE AUDIT

COMPREHENSIVE CONTINUITY PLANNING AND INFORMATION RESOURCE SECURITY MANAGEMENT OF THE STATE'S ACCOUNTING SYSTEM (SAM II)

From The Office Of State Auditor
Claire McCaskill

State financial operations face risk without a complete comprehensive continuity plan. In addition, management has not assessed the effectiveness of the system's security controls to ensure security measures are functioning properly.

Report No. 2003-108
October 23, 2003
www.auditor.state.mo.us

Office of
Missouri State Auditor
Claire McCaskill

October 2003

YELLOW SHEET

Comprehensive continuity planning framework and security controls should be established for state's accounting system

This audit reviewed the Office of Administration's (OA) management of the state's accounting system (SAM II) as it relates to plans for handling business continuity and information technology recovery should a disaster or other disruptive event occur. SAM II is the state government's integrated financial management, human resource and payroll system which processed approximately $25 billion in expenditure and transfer transactions in fiscal year 2003. The following highlights the finding:

Recommended controls not implemented

Many suggested controls described by the SAM II software vendor in a 1998 report were not implemented. Implementing these controls would have prevented almost half of the recovery and security weaknesses noted in this report. (See page 3)

Plans and training needed for resuming critical business operations and system processing

The OA has not identified critical resources necessary to operate the SAM II system, established an alternate offsite facility for the continuation of normal business operations or documented how manual processing of transactions will be performed if the SAM II system is not available. Auditors found that OA does not have an emergency management team to develop strategies for recovery support across all business functions. Such a team would activate continuity plans and coordinate recovery activities. In addition, SAM II and OA personnel are not trained on all aspects of their specific roles and responsibilities relating to recovery procedures. (See pages 4 and 5)

Some security controls need to be addressed

The OA cannot adequately protect the integrity, confidentiality and availability of data, which may result in unauthorized use or modification to sensitive information. Current management practices do not have sufficient controls for monitoring computer access or application administrator user rights. In addition, management practices do not adequately segregate duties related to system changes, sufficiently monitor access and security violations or ensure the integrity of system users. (See page 9)

Background checks for system users may be necessary

SAM II management does not require background checks on state employees using the

SAM II system. High-level background checks conducted by the Missouri State Highway Patrol at our request on over 7,000 SAM II users, identified 146 system users with one or more criminal records. Forty-six of the individual offenses for these users involved potential financial-related issues such as theft, robbery, fraud, etc. (See page 12)

All audit reports are available on our website: www.auditor.state.mo.us

COMPREHENSIVE CONTINUITY PLANNING AND INFORMATION RESOURCE SECURITY MANAGEMENT OF THE STATE'S ACCOUNTING SYSTEM (SAM II)

TABLE OF CONTENTS

Page

STATE AUDITOR'S REPORT 1

RESULTS AND RECOMMENDATIONS 2

1. Recovery Planning Needs Improvement 2

   Conclusions 7

   Recommendations 7

2. Some Security Controls Need to Be Addressed 9

   Conclusions 14

   Recommendations 14

APPENDIXES

I. OBJECTIVES, SCOPE AND METHODOLOGY 17

II. DEFINITION OF TERMS 18

III. REFERENCES 20

CLAIRE C. McCASKILL
Missouri State Auditor

Honorable Bob Holden, Governor
and
Jacquelyn D. White, Commissioner
Office of Administration
Jefferson City, MO 65102

The State Auditor's Office audited the comprehensive continuity planning preparedness and information resource security controls for the state's accounting system (SAM II). The objectives of this audit were to evaluate if the Office of Administration's SAM II management had (1) defined and implemented a comprehensive continuity plan to ensure recovery of business and computer processing operations in case of a disaster or other unexpected interruptions and (2) established security controls to ensure the integrity, confidentiality, and availability of data on the SAM II system.

We concluded SAM II management needs to develop a comprehensive continuity plan with the guidance of a department-wide framework. In addition, personnel need training in their responsibilities related to system recovery. Regarding information resource security, SAM II management needs to periodically assess established security controls and evaluate active user IDs to ensure their necessity.

We conducted the audit in accordance with applicable standards contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, and included such tests of the procedures and records as were considered appropriate under the circumstances.

Claire McCaskill
State Auditor

The following auditors contributed to this report:

Director of Audits:	William D. Miller, CIA, CGFM
Assistant Director of Audits:	Jon Halwes, CPA, CGFM
In-Charge Auditor:	Tara Shah, CPA
Audit Staff:	Frank Verslues
	Lori Melton, CPA

224 State Capitol • Jefferson City, MO 65101

Truman State Office Building, Room 880 • Jefferson City, MO 65101 • (573) 751-4213 • FAX (573) 751-7984

RESULTS AND RECOMMENDATIONS

1. Recovery Planning Needs Improvement

The Office of Administration (OA), which administers the state's accounting system (SAM II), needs better preparation to prevent a significant interruption of SAM II business operations. State financial transaction and payroll processing are at risk for disruption because OA officials have not completed an office-wide comprehensive continuity plan which would include the SAM II system.

Without continuity planning, there is less assurance normal business operations and information technology processing could resume in the event of a disaster or other disruptive event. Due to the role of SAM II in state financial management, it is important critical business operations remain functioning or can be resumed promptly with the least possible disruption. Some weaknesses identified resulted from SAM II management misunderstanding who is responsible for system recovery planning. Other issues have not received adequate management consideration.

Description of comprehensive continuity planning

An organization must adequately prepare to cope with a loss of operational capability. An organization's ability to accomplish its mission can be significantly affected if it loses the ability to process, retrieve, and protect information that is maintained electronically. Three main classes of events might affect an organization's ability to continue business operations: an unplanned incident or accident such as an explosion or fire, a natural disaster such as a tornado or earthquake, or a deliberate act.

An essential element in preparing for such catastrophes is an up-to-date, detailed, and fully tested continuity plan. Comprehensive continuity planning encompasses both business continuity and information technology recovery. With business continuity planning, an organization is ensuring the availability of all business resources and supporting information technology needs to continue/resume business processes. For information technology recovery planning, the organization is ensuring the availability of information technology resources required to support the continuity or recovery of business processes. A comprehensive continuity plan specifies emergency response, backup operations, and restoration procedures to ensure the availability of critical resources and facilitate the continuity of operations. It addresses how an organization will deal with a full range of contingencies, from electrical power failures to catastrophic events, such as earthquakes, floods, and fires. The plan also identifies essential business functions and ranks critical resources. To be most effective, a continuity plan should be periodically tested in disaster simulation exercises and employees should be trained in and familiar with its use.

Criteria used to evaluate the OA

Currently, there are no state regulations requiring agencies to develop, implement, and maintain a comprehensive continuity plan. In addition, no state guidelines establish the need or specific parameters for information resource security controls. However, the State Data Center (data

center)[1] has a customer procedures manual, which outlines specific policies for state agencies as customers. The manual includes a section on business recovery planning and security.

In addition, there are federal, national and international standards related to continuity planning, information resource security controls and security program planning. For our audit, we used accepted standards from the following sources:

- National Institute of Standards and Technology
- Information Systems Audit and Control Association
- International Organization for Standardization
- American Institute of Certified Public Accountants
- U.S. General Accounting Office
- Canadian Institute of Chartered Accountants

SAM II is the state's integrated financial management, human resource and payroll system providing accounting, budgeting, procurement, inventory, and human resources management capabilities for state departments and agencies. The SAM II system processed approximately $25 billion in expenditure and transfer transactions in fiscal year 2003.

The SAM II system is managed by the OA's Commissioner's Office. The system has two system administrators and several application administrators. Technical support is provided by the systems and programming staff under the OA's Division of Information Services and the software vendor that customized the SAM II system for the state.

See Appendix II, page 18, for key terms and definitions used in the report.

Recommended controls not implemented

Many suggested controls described in the Technical Architecture Blueprint developed by the SAM II software vendor were not implemented. The document was prepared in 1998 during the evaluation of the SAM II software and installation of the applications. Implementing these controls would have prevented almost half of the recovery and security weaknesses noted in this report.

[1] Part of the Office of Administration. The data center provides data processing services to state agencies and is responsible for safeguarding information and data stored on its resources.

Plans are needed for resuming critical business operations and system processing

The OA does not have a comprehensive continuity plan for the SAM II system. SAM II management stated the data center is responsible for information technology recovery planning for the SAM II system. This statement demonstrates a misunderstanding of data center services. The directors of the data center and Division of Information Services explained the data center only has recovery plans for its service operations, even though the data center is under the OA. SAM II management is responsible for developing, testing, and maintaining recovery plans for the SAM II system.

A recent national study showed 43 percent of companies that experience a major disaster and do not have an adequate continuity plan do not re-open, while 29 percent are out of business within 2 years. The overall survival rate without a plan is 28 percent.[2] Although state financial transaction processing could not cease, the length of time critical SAM II operations may not be functioning could severely impact the state. During our audit, SAM II management developed a general disaster recovery plan, which prioritized SAM II system applications and defined tolerable outage times for these applications.

The OA has not established an alternate offsite facility for the continuation of normal business operations and no other plans for ensuring the ongoing operations of SAM II business functions are documented.

If the information technology function of SAM II is not available, OA management plans for agencies to manually process transactions. However, management has not documented how this manual processing will be performed. In addition, SAM II management has not listed critical resources necessary to operate the SAM II system. Without knowing the equipment and resources necessary to run the system, it would be difficult for management to ensure the availability of these resources in a recovery situation.

According to accepted standards,[3] continuity plans should:

- Be documented and approved by senior management.
- Identify all critical business applications and operations.
- Prioritize the critical business applications and operations.
- Identify resources needed to support critical functions.
- Satisfy the established maximum outage time.
- Address disasters of varying degrees.
- Include alternate processing facility agreements.
- Be periodically tested to ensure they are kept relevant and effective.

At the end of our fieldwork, SAM II management had identified and prioritized all critical business applications and operations.

---

[2] *Business Continuity Management In Today's Environment,* a seminar presented to the St. Louis Chapter of the Institute of Internal Auditors on October 25, 2001 by Jefferson Wells International.

[3] Standards established by the six organizations identified on page 3.

Organizational policies should require a continuity planning framework to ensure consistency in continuity plans and that all necessary items are included in the plan. This framework should be a part of normal operational requirements and function as an outline guiding management to the general issues documented in the plan. The framework should define the roles, responsibilities, and the risk-based approach/methodology to be adopted, the rules and structures to document the plan, and the approval procedures.

Management team and personnel training would improve recovery preparedness

The OA does not have an emergency management team to develop strategies for recovery support across all business functions. In the midst of a disaster, the OA would lack the consolidated input of a management team to implement appropriate recovery strategies. This weakness could result in the loss of valuable time in the assessment and recovery phases of a disaster. For employees to respond in an orderly fashion, accepted standards suggest an emergency management team or similar function would activate continuity plans and coordinate recovery activities.

Time could be lost during disaster recovery efforts

SAM II and OA personnel are not trained on all aspects of their specific roles and responsibilities relating to recovery procedures. Personnel have responsibilities to uphold in the event of a disaster. The only recovery training they receive is how to perform the restoration procedures of the application data. However, they would be responsible for other duties in the event of a disaster that may include:

- Manual processing of transactions.
- Coordination with state agency recovery teams and system users.
- Damage assessment of resources.
- Assessment of data completeness.
- Obtaining replacement resources.

Without guidance and training on such issues, OA management cannot ensure personnel will react properly to a disaster and effectively and efficiently carry out their responsibilities.

Management needs to evaluate the impact of risks or threats

SAM II management does not have procedures to analyze the impact of various disruptive events. According to accepted standards, updating potential risks and exposures should be an ongoing risk management activity. A business impact analysis would consider different types of risks and their corresponding impact on business functions. Potential business interruptions and acceptable tolerable downtimes should be identified for all critical business functions. This analysis will allow management to identify how long a critical function may be down, the impact on other business functions if it is out longer than anticipated, and what alternatives should be considered to resume business operations.

Various strategies are available for recovering business operations. The appropriate strategy balances preventive and recovery costs against the business impact of possible outages. This business impact analysis would allow management to select the most appropriate alternative to resume operations based on the risks identified.

Backup and offsite procedures are not documented

Backup procedures for data files are incomplete. SAM II system data are maintained either on the mainframe system or on servers. Management has not documented backup procedures for application data maintained on the mainframe system. The vendor provided backup procedures, which support the software used for backing up server data. However, the additional procedures documented by SAM II management are not complete. These backup procedures lack documentation of the backed up files and data, the personnel responsible for the backup functions, proper description of the methods and frequency of data file backups, and definition of arrangements for collection and transportation of files to an offsite location. SAM II management said backup file and data documentation is part of the tape stored off-site and system and programming staff can produce a list.

Accepted standards state management should have documented procedures for off-site storage or availability of all material which would be required to restore and recover critical business functions. Although paper checks and forms are maintained off-site, SAM II management has not documented procedures for storing and maintaining these critical business function materials.

Restoration testing needs to be more frequent

Per accepted standards, backup data should be retrieved on a regular basis from off-site storage and tested to ensure data are being stored correctly and that the files can be retrieved without errors or lost data. Currently, SAM II system backup files are only tested during the state's annual mock disaster recovery testing.

Testing backup systems effectively identifies weaknesses

With more frequent testing of both off-site backup files, weaknesses in restoration procedures could more quickly be identified and corrected. An impact analysis would assist SAM II management in determining how often backup media should be tested.

Documentation and assessment of results critical to system recovery testing

The only documentation the SAM II management had from the July 2002 disaster recovery test was a list identifying 13 problems areas to be corrected. A written corrective action plan explaining how these problems would be resolved and their ultimate resolution was not prepared.

Once the testing phase is completed, it is important to perform a documented assessment of the testing. Accepted standards state:

- The objectives of the test should be clearly stated.
- The capability to retrieve backup data files from the offsite storage facility should be assessed.
- The overall performance of information systems should be assessed and measured. This includes documenting if the restoration was performed within a reasonable timeframe and if the applications were adequately restored.
- A performance evaluation of the personnel involved in the test should be performed.
- A corrective action plan should be developed for all problems encountered during restoration.

2003 test was better documented

We discussed the July 2002 test documentation weaknesses with SAM II management prior to a March 2003 disaster test and management significantly improved the documentation prepared for that test.

Conclusions

State financial operations face risk without a complete comprehensive continuity plan. Backup and offsite storage procedures need to be documented. Officials need to evaluate the potential risks to the SAM II system and ensure SAM II operations can be timely resumed in the event of a business operation disruption. For testing any procedures, management needs to document the objectives and develop corrective action plans.

Recommendations

We recommend the Commissioner, Office of Administration:

1.1 Define and implement an office-wide continuity planning framework, including standards and policies for the development and maintenance of comprehensive business continuity and information technology recovery plans. This framework should include provisions to:

- Formally assign the responsibilities for recovery planning and ensure all personnel are aware of and trained in their duties.

- Incorporate periodic business impact analysis to monitor the ongoing requirements of the business continuity plans.

1.2 Develop, implement, and maintain a comprehensive continuity plan for the SAM II system, which consists of both a business continuity plan and an information technology recovery plan. Once the plans are implemented, they should be periodically tested.

1.3 Document SAM II system backup and offsite storage procedures necessary to recover system operations and resume business processes.

1.4 Test off-site back up files more frequently than during the state's annual recovery test.

Office of Administration Comments

1.1 The Office of Administration agrees that a continuity planning framework should be implemented. The Missouri Security Council is currently developing statewide guidelines and a template that will be reviewed by a committee made up of state department deputy directors. We will follow the guidelines adopted by the deputy directors committee for implementing a continuity planning framework if resources are available.

1.2 The Office of Administration currently has an information technology recovery plan that is tested once a year. We do agree that additional documentation of this process could be beneficial and will put that in place. The Office of Administration's comprehensive business continuity plan will cover department-wide responsibilities including the SAM II system. Therefore, we feel developing and maintaining a separate business continuity plan for SAM II will provide little benefit and is not justified given the current budget restrictions and limited resources.

1.3 The Office of Administration feels critical SAM II backup and recovery procedures are adequately documented.

1.4 The Office of Administration disagrees with this recommendation. We consider annual testing of the offsite backup files and restoration of the SAM II system to be adequate. This is currently the statewide standard testing cycle for all systems located on the mainframe in the State Data Center. More frequent testing would require additional resources for use of the offsite recovery center in excess of current contracted service and approximately 80 hours of staff time for each additional restoration exercise. We do not feel the benefits of more frequent restoration testing justify the additional costs.

2. Some Security Controls Need to Be Addressed

The OA lacks a computer security management program to guide SAM II management regarding security policies and standards. In addition, because the SAM II system is still relatively new, management has not evaluated the security controls over the system to ensure they are working effectively and efficiently. During the audit, we noted current management practices do not:

- Have sufficient controls for monitoring computer access or application administrator user rights.
- Adequately segregate duties related to system changes.
- Sufficiently monitor security violations.
- Ensure the integrity of system users.

As a result, the OA cannot adequately protect the integrity, confidentiality and availability of data, which may result in unauthorized use or modification.

Background

Our security audit work focused primarily on the two major SAM II system applications: financial accounting (financial) and human resources (HR). The financial application, used for purchasing and payment processing, was implemented in July 1999. The HR application, used to maintain and process payroll information, was implemented in phases between November 2000 and June 2001. Users may have rights to add or change data or they may only have inquiry access. As of December 2002, there were 5,604 financial application user identification codes (IDs) and 7,652 HR application user IDs which have been created by state agencies for system users. Ninety percent of these users had more than inquiry access.

Computer security framework needed to establish guidance

The OA does not have an office-wide security framework. According to accepted standards, an organization should have a written, up-to-date security policy covering all major facilities and operations to address:

- Security planning
- Risk management
- Review of security controls
- Life-cycle management
- Authorization for processing
- Personnel
- Physical and environmental aspects
- Computer support and operations
- Contingency planning
- Documentation, training and responses to incidents
- Access controls
- Audit trails

From the framework, the organization's management should develop more detailed guidance or standards that describe an approach for implementing policy. Despite the lack of an office-wide framework, SAM II management has developed procedures which cover most security issues. However, there are some critical security issues which are not sufficiently addressed including: classifying data; assigning data ownership; assessing security controls; and reviewing user accounts for terminated employees, inactivity and redundancy. A security plan framework would provide policies for the SAM II management to follow.

SAM II management currently does not require system data to be formally classified into security levels. Data is generally classified into four levels: public, internal, confidential, and classified. Data center procedures and accepted standards require defined data classification levels. Data owners should use the classification levels to identify the data's security level and the application administrators should follow the access rules for the class type. SAM II management said they believe agency management and users know what data is confidential and what data is public. When the SAM II system was implemented, an operations committee established data owners for all the tables and documents in SAM II. The procedures for determining or changing ownership have not been documented and ownership has not been formally established for tables and documents created after system implementation. The operations committee no longer exists and the data owners have not been reviewed since established to determine if they are still adequate.

Effectiveness of security controls has not been assessed

SAM II management has not implemented procedures for assessing the effectiveness of security controls. Without such an assessment process, there is less assurance the security measures are effective and functioning properly. Accepted standards state periodic self-assessments and independent reviews should confirm compliance with established procedures. These standards recommend a security evaluation every 3 years or after a major modification to the system.

Documentation is lacking in system life-cycle changes

Although the system administrators state they review every SAM II system change request, their review is not always documented. Per SAM II work order procedures, management requires each issue needing assistance from the system administrators, system and programming staff, and/or the SAM II vendor to be assigned and reviewed by a system administrator. For 7 of the 10 work orders we reviewed, there was no documentation a system administrator reviewed the order before it was assigned to the responsible party.

In addition, after a change is made, the responsible party can close the work order and a system administrator is not required to review the final changes. Accepted standards state system administrators should periodically review program changes to determine whether controls were followed. In addition, the final acceptance or quality assurance testing of new or modified information systems should include a formal evaluation and documented approval of the test results. Although the system administrators stated they

are aware of and review all changes made to the system, there is no documentation of their review and approval of changes.

Security settings for SAM II are not sufficient

Currently, the SAM II system does not log out a user from the system after a period of inactivity. Accepted standards state computer terminals should automatically log off after a period of inactivity. The SAM II software has a setting for logging out accounts after a period of inactivity; however, that setting is currently not functioning due to a problem caused by the vendor. Management reported this problem to the vendor in October 2002; however, it remained uncorrected as of March 2003. Without proper security settings, there is less assurance data are adequately protected from unauthorized access.

Application administrators' duties are not properly reviewed

SAM II management does not review the use of application administrator accounts. Although the application administrators granting access to the SAM II applications are segregated from the individuals approving access, there is no supervisory review over the application administrators. Changes made by the application administrators are logged, but management does not review the log regularly. Additionally, management does not regularly review the list of individuals with special access rights in the SAM II system. During our audit, we identified two users with possible excessive administrative rights based on work responsibilities. A system administrator determined these rights were no longer necessary for these employees and removed them.

User IDs are not evaluated adequately

According to SAM II management, each agency is responsible for periodically reviewing user access to the SAM II system. The application administrators perform only limited reviews of user IDs. Although agencies are responsible for submitting access requests to add, change, or remove user access rights, SAM II management is ultimately responsible for the security of the system.

86 former state employees or contractors had active user IDs

During January 2003, auditors noted the following problems in access to the SAM II system that would have been identified through periodic reviews of user accounts.

- Sixty financial user IDs and 32 HR user IDs were active for 86 individuals no longer employed or contracted by the state. Forty-six of these IDs were used to access data center systems after the individual's termination date; however, the SAM II application administrators could not readily tell us if the SAM II system had been accessed.

- At least 35 employees had more than one active user ID in the financial application. SAM II personnel stated these employees should not be assigned more than one active SAM II user ID. During the audit, 13 of the redundant user IDs were removed and the financial application administrator is following up on the other IDs.

- At least 1,164 SAM II user IDs, which had been used at least once, had not been accessed for 90 days or more. In addition, 441 user IDs, which had been created over 90 days ago, had never been accessed. These inactive IDs account for approximately 16 percent of the 9,886 unique financial and HR application IDs.

Background checks for system users may be necessary

SAM II management does not require background checks on state employees using the SAM II system. We asked the Missouri State Highway Patrol to conduct a high-level background check on over 7,000 SAM II users who had more than inquiry access during December 2002. The analysis identified 146 system users with one or more criminal records. Forty-six of the individual offenses for these users involved potential financial-related issues such as theft, robbery, fraud, etc. We were not provided details of the offenses or any details related to a specific user submitted for review; however, the results indicate there may be individuals with questionable backgrounds with access to the SAM II system.

Responsibilities for changes to the system need to be properly segregated

Fourteen system programmers and technical support staff have access rights to datasets containing program code. Their access rights allow them to make changes to system programs and move those changes into the production environment. An additional three financial application programmers' job responsibilities specifically include making and moving changes into the production environment. These 17 staff also have access to live production data. Accepted standards state management should implement a division of roles and responsibilities, which should exclude the possibility for a single individual to subvert a critical process. Segregation of duties should be maintained between functions including data entry, change management, and systems development and maintenance. SAM II management explained the lack of segregation of duties was due to the small number of system programming and technical support staff. However, other compensating controls have not been implemented to mitigate these control weaknesses. If access to live data is needed by programmers, the number of users with such overlapping access rights should be limited.

Access and security violations are not sufficiently monitored

SAM II management has not taken sufficient steps to ensure system security controls are functioning properly. The first step in establishing effective security is developing procedures for logging appropriate security-related events, monitoring specific access, and investigating apparent security violations. Currently, a security feature is activated for SAM II which logs changes including those made to the tables controlling security and user access levels. There is also a separate log maintained for changes made by programmers directly to SAM II production data through the back end process.

The system administrators do not routinely review either log. Potential violations are brought to the attention of appropriate officials by personnel once the concern is noted, rather than through periodic review of these logs. Documented procedures are not in place regarding investigation of potential violations and necessary actions to be taken. SAM II management does not routinely

review computer system reports, which identify changes made to critical functions, such as system security. Accordingly, unauthorized changes to critical security controls could go undetected. In addition, access to confidential data is not monitored to detect failed attempts or unusual patterns of successful access to such information. Routinely monitoring access activities can help identify significant problems and deter employees from inappropriate activities.

The SAM II system also can log security violations. SAM II management stated they decided not to use the log because of the additional costs involved; however, a cost-benefit analysis could not be provided to support this decision.

A security monitoring program should include (1) identifying sensitive system files, programs, and data files on computer systems and networks, (2) using the audit trail capabilities of security software to document both failed and successful access to these resources, (3) defining normal patterns of access activity, (4) analyzing audit trail information to identify and report on access patterns that differ significantly from defined normal patterns, (5) investigating potential security violations, and (6) taking appropriate action to discipline perpetrators, repair damage, and remedy the control weaknesses that allowed improper access to occur.

Administrative procedures and policies need to be updated

During the implementation of the SAM II financial and HR applications, the OA documented the responsibilities for system and application administrators and procedures for system security. Officials did not revise these documents after significantly changing the structure of SAM II system. Without accurate, up-to-date system procedures and documented responsibilities, there is less assurance all staff are aware of the current procedures.

Personnel policies need improvement

Although SAM II is a statewide system used by most state agencies, we limited our review of personnel policies to the OA. During December 2002, there were 403 OA employees with access to the financial application and 271 OA employees with access to the HR application. The OA does not have a policy requiring interviews of applicants or reference checks. OA management stated although there are no office-wide hiring procedures, the individual OA divisions may have procedures. Historically, background checks have been done on new hires of the building and facilities maintenance staff and data center personnel. Due to heightened security to state buildings, the OA recently started performing reinvestigations on the building and facilities maintenance staff. However, OA management has not determined if other positions, such as those with SAM II access, should be classified as sensitive. Also, employees are not required to sign confidentiality agreements. Accepted standards require procedures to verify the background and work history of new hires and include:

- Verifying references of prospective employees.
- Obtaining and reviewing resumes.
- Performing background checks and periodic reinvestigations at least once every 5 years for sensitive positions.

The OA's administrative manual documents exit procedures for terminated employees. However, these procedures do not include removing the computer access of employees when they terminate. Consequently, supervisors could overlook submitting a request to remove the access. Divisions within the OA may have separate exit procedures that consider computer access removal.

Conclusions

The OA does not have a security framework to provide guidance to SAM II management. The system's security procedures have not been assessed and system changes lack some necessary documentation. Therefore, management cannot ensure security controls are working effectively and system changes were made properly. Current access controls may allow users to have unnecessary access to system resources. Limited policies or procedures exist to monitor access and detect security violations. The procedures describing how to administer the security controls of the SAM II system need to be updated. Personnel policies may not be sufficient to ensure the integrity of employees with access to the system.

Recommendations

We recommend the Commissioner, Office of Administration:

2.1 Implement an office-wide security framework and security plan. The security framework should document and ensure consistent implementation of effective and consistent security practices for all divisions and personnel. The plan should include:

- A data classification framework scheme and guidelines for classifying data in terms of criticality and sensitivity.

- A structure for formally appointing data resource owners and for defining their roles and responsibilities, which includes making decisions about classification and access rights.

2.2 Establish procedures for assessing the effectiveness of system security controls.

2.3 Establish procedures to improve the system administrator's documentation authorizing requests for system changes and the ultimate approval of the change before it is put in place.

2.4 Work with the software vendor to resolve the system inactivity user logoff feature that has been unavailable since October 2002.

2.5 Ensure system administrators perform supervisory reviews of the assignment and use of privileged accounts.

2.6 Periodically review user IDs to ensure access of terminated employees is removed. Inactive and duplicate user IDs should also be evaluated for possible removal.

2.7 Communicate with state agencies the importance of performing background checks by the Missouri State Highway Patrol on employees with access to state financial systems.

2.8 Ensure programmer duties are properly segregated and access rights are limited to essential job functions. If proper segregation cannot be done, implement compensating controls, such as increased supervisory monitoring.

2.9 Log appropriate security-related events, monitor access, investigate apparent security violations, and take appropriate remedial action to ensure the proper functioning of controls in the system.

2.10 Update SAM II documents outlining responsibilities for system and application administrators and procedures for system security for current practices and keep them updated as changes take place.

2.11 Establish hiring and termination procedures which give appropriate consideration to security issues and technical skills.

Office of Administration Comments

2.1 The Office of Administration will consider the costs and benefits of implementing an office-wide security framework and security plan and will review the current data ownership and classification process for the SAM II system.

2.2 The Office of Administration agrees that procedures for assessing the effectiveness of system security controls should be established and will conduct security evaluations as resources are available to do so.

2.3 The Office of Administration agrees that the documentation for authorizing and approving system changes could be improved and will establish appropriate procedures.

2.4 The Office of Administration will continue to work with the software vendor to resolve the system inactivity logoff feature.

2.5 The Office of Administration agrees and will implement procedures to ensure privileged accounts are properly reviewed and authorized.

2.6 The Office of Administration agrees. Procedures have already been implemented to ensure user IDs for terminated employees are removed and inactive and duplicate user IDs are evaluated for removal.

2.7 The Office of Administration agrees and is drafting a statewide policy on background checks. The policy will allow agencies to determine whether background checks are necessary based on an individual's job duties and responsibilities.

2.8 The Office of Administration agrees that a proper segregation of programmer duties is desired. However, due to the limited technical resources supporting the SAM II system, it is not possible to completely segregate programmer duties. On-call programmers need to have access rights to make changes to system programs and move those changes into the production environment to resolve problems during critical batch processing (i.e., payroll). The Office of Administration will consider implementing other compensating controls to the extent that resources are available.

2.9 The Office of Administration agrees that security-related events should be logged, monitored and investigated. However, it is not cost effective to review the SAM II system baseline security logs because the majority of transactions recorded are routine security edits that prevent users from unauthorized activity. This would require additional resources and provide very little benefit. Alternative approaches will be evaluated to assess the risks vs. costs of implementing a more robust review of system security controls.

2.10 The Office of Administration agrees and will update documents outlining responsibilities and procedures for system and application administrators as resources are available.

2.11 The Office of Administration will consider establishing department-wide hiring and termination procedures. Some divisions in the Office of Administration currently have hiring and termination procedures that consider security issues and technical skills.

APPENDIX I

OBJECTIVES, SCOPE AND METHODOLOGY

Objectives

The objectives of this audit were to evaluate if the Office of Administration's SAM II management had (1) defined and implemented a comprehensive continuity plan to ensure recovery of business and computer processing operations in case of a disaster or other unexpected interruptions and (2) established security controls to ensure the integrity, confidentiality, and availability of data on the SAM II system.

Scope and Methodology

Auditors conducted fieldwork during October 2002 through March 2003. The audit included:

- Review of applicable federal, national, and international standards related to comprehensive continuity planning and information resource security controls.
- Discussion with OA personnel involved in comprehensive continuity planning and information resource security.
- Review of OA records related to comprehensive continuity planning and information resource security.
- Analysis of user ID information for access to the SAM II system.
- Evaluation of management controls pertinent to comprehensive continuity planning and information resource security.

The audit reviewed SAM II management practices and procedures for comprehensive continuity planning and information resource security except for activities that are the responsibility of the State Data Center (data center). Therefore, our audit did not review the security controls of the data center related to the SAM II system or the controls of the data center related to the OA's ability to recover the SAM II system after a significant disruption to business operations. Because the objective of our review was to assess the overall effectiveness of the SAM II security and access controls, we did not fully evaluate all computer controls and we did not perform any penetration testing.[1]

During the audit, we provided SAM II management with specific detail on security concerns noted for their immediate consideration.

[1] A test of a network's vulnerabilities by having an authorized individual actually attempt to break into the network. The tester may undertake several methods, workarounds and "hacks" to gain entry, often initially getting through to one seemingly harmless section, and from there, attacking more sensitive areas of the network.

APPENDIX II

DEFINITION OF TERMS

Some key terms and definitions accepted by the organizations noted on page 3 that have developed national and international standards for continuity planning and computer security include:

Access Control: Controls designed to protect computer resources from unauthorized modification, loss, or disclosure. Access controls include both physical access controls, which limit access to facilities and associated hardware, and logical controls, which prevent or detect unauthorized access to sensitive data and programs that are stored or transmitted electronically.

Application: Any of a class of "programs" or "software," which causes a computer to perform some useful function such as data entry, update or query.

Back end: The support components of a computer system. It typically refers to the database management system, which is the storehouse for the data.

Business Continuity: The discipline of planning for the recovery of business operations in the event that normal business resources, such as office space, terminals, microcomputers, office machines, terminals and networks, are made unavailable following a disaster.

Dataset: A data file or collection of interrelated data. The term is used in a mainframe environment, whereas file is used almost everywhere else.

Disaster Recovery: The discipline of planning for the recovery of information technology operations in the event that normal operations are made unavailable as a result of a disaster; normally, closely related to the discipline of business continuity planning.

Framework: An outline of the issues that need to be addressed in a comprehensive department-wide computer security plan. Provides background and rationale for information technology security, evaluation, certification and system accreditation. It is intended to be used at management levels.

Information Resource: All computer-related activities involving any device capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, and network environments. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Mainframe: A multi-user computer designed to meet the computing needs of a large organization.

Production data: The data that supports an agency's operational information processing activities. It is maintained in the production environment as opposed to the test environment.

Production environment: The system environment where the agency performs its operational information processing activities.

Profile: Data that describes the nature and extent of system access for a user, a group of users, or one or more computer resources.

Recovery: The ability to resume processing without irreparable loss of system data after an error or malfunction in software or hardware.

System Administrator: The person(s) responsible for administering use of a multi-user computer system, communications system, or both.

APPENDIX III

REFERENCES

American Institute of Certified Public Accountants

AICPA/CICA SysTrust: Principles and Criteria for Systems Reliability, Version 2.0, January 2001.

Auerbach Publishers

Information Technology Control and Audit, Frederick Gallegos, Daniel P. Manson and Sandra Allen-Senft, 1999.

Standard for Auditing Computer Applications, Martin A. Krist, 1999.

Canadian Institute of Chartered Accountants

Information Technology Control Guidelines 3rd Edition, July 1998.

Federal Chief Information Officers Council

Federal Information Technology Security Assessment Framework, November 28, 2000, http://www.cio.gov.

Information Systems Audit and Control Foundation

Control Objectives for Information and Related Technology (COBIT), 3rd Edition, July 2000, http://www.isaca.org.

Certified Information Systems Auditor (CISA) Review Manual, 2002, http://www.isaca.org.

International Organization for Standardization / International Electrotechnical Commission

ISO/IEC 17799:2000(E), *Information Technology – Code of Practice for Information Security Management,* December 2000, http://www.iso.ch.

McAtte, Bryan

Introduction to Information Technology Auditing, 2002.

Missouri Office of Administration - Division of Information Systems State Data Center

Customer Procedures Manual, Section IX, January 2002.

National Institute of Standards and Technology

Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook,* October 1995, http://csrc.nist.gov.

Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996, http://csrc.nist.gov.

Special Publication 800-18, *Guide For Developing Security Plans For Information Technology Systems,* December 1998, http://csrc.nist.gov.

Special Publication 800-26, *Security Self-Assessment Guide For Information Technology Systems,* November 2001, http://csrc.nist.gov.

Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002, http://csrc.nist.gov.

APPENDIX III

U.S. Office of Management and Budget

Appendix III to OMB Circular No. A-130, *Security of Federal Automated Information Resources*, November 2000, http://www.whitehouse.gov/omb/circulars/index.html.

U.S. General Accounting Office

Federal Information System Controls Audit Manual: GAO/AIMD-12.19.6, January 1999, http://www.gao.gov.

Warren Gorham & Lamont/RIA Group

Handbook of IT Auditing, 2001 Edition.