Claire McCaskill
Missouri State Auditor

March 2006

INFORMATION TECHNOLOGY

Information Security Management in State Agencies

Report no. 2006-14

auditor.mo.gov

Claire McCaskill
Missouri State Auditor

YELLOW SHEET

State agencies have placed an increased emphasis on information security management since our prior audits

This audit included a follow-up of six information technology security and comprehensive continuity plan audits issued from 2001 through 2003. We determined the current status of information security management practices by evaluating the progress agency officials have made to establish security controls and comprehensive continuity plans. In addition, we evaluated the Office of Administration, Information Technology Services Division's (ITSD) strategy to address information technology governance, principles, and standards for the state through the establishment of an enterprise architecture.

Agencies implemented majority of prior recommendations

Agencies made progress in correcting security and comprehensive continuity planning weaknesses by implementing 43 of 67 recommendations from the 6 prior audit reports. As a result, the implemented recommendations increase the agencies' ability to protect information technology resources. However, the recommendations that have not been implemented continue to expose information technology resources to unnecessary risks. (See page 8)

Progress has been made developing the statewide enterprise architecture

Executive Order 03-26, issued in December 2003, authorized the state's Chief Information Officer (CIO) to establish an enterprise architecture for Missouri. Effective January 2005, the CIO was assigned responsibility to oversee the ITSD. According to the state's enterprise architecture manual, "the goal of statewide Enterprise Architecture is to enhance coordination, simplify integration, build a consistent infrastructure, and generally allow greater efficiencies in the development of technology solutions."

The state has made important progress developing an enterprise architecture, but this architecture is not complete. Developing, implementing, and maintaining an enterprise architecture is necessary for an organization's management of information technology resources. Managed properly, an enterprise architecture can help optimize the interdependencies and relationships among the state's business operations and the information technology resources that support these operations. According to the CIO, completion of the architecture has been hampered because each state agency's information technology units operated autonomously prior to the state's information technology consolidation. Beginning in 2005, information technology personnel and resources from most executive branch agencies were consolidated under the CIO. As a result, the CIO believes progress on the architecture development should now proceed more smoothly and quickly than prior to the consolidation. (See page 15)

All reports are available on our website: www.auditor.mo.gov

Contents

Abbreviations

CIO	Chief Information Officer
DCSE	Division of Child Support Enforcement
DOR	Department of Revenue
EA	Enterprise Architecture
GAO	U.S. Government Accountability Office
ITAB	Information Technology Advisory Board
ITSD	Information Technology Services Division
OA	Office of Administration
SAM II	Statewide Advantage for Missouri
SAO	State Auditor's Office
User ID	User Identification

CLAIRE McCASKILL
Missouri State Auditor

Honorable Matt Blunt, Governor
and
Dan Ross, Chief Information Officer
Office of Administration
Jefferson City, MO 65102

Rapid and dramatic advances in information technology, while offering tremendous benefits, have also created significant and unprecedented risks to government operations. State agencies depend heavily on security controls to manage these risks to avoid data tampering, fraud, inappropriate access to and disclosure of sensitive information, and disruptions in critical operations. From 2001 through 2003, the State Auditor's Office reviewed information security management practices by conducting six information technology security and comprehensive continuity plan audits to determine if controls were in place to adequately protect the state's information technology resources.

The Office of Administration Information Technology Services Division's (ITSD) responsibilities include, but are not limited to: developing information technology policies, coordinating information technology initiatives for the state, providing information technology services and expertise to customer agencies, and providing centralized data center services to state agencies. In fiscal year 2006, the information technology sections of most executive branch departments began the process of consolidating personnel and budgeted appropriations under ITSD.

The objectives of this audit include (1) determining the current status of information security management practices by evaluating the progress agency officials have made to establish security controls and comprehensive continuity plans and (2) evaluating ITSD's strategy to address information technology governance, principles, and standards for the state.

We found agencies have been placing an increased emphasis on information security management. Agencies have been making progress implementing security controls and developing comprehensive continuity plans to protect the information technology resources that support the missions and operations of the state. Many of the recommendations we made to correct security control weaknesses have been implemented. However, we also identified recommendations, which could enhance security of information technology resources, that had not yet been implemented. We also determined the state is establishing an enterprise architecture to address the technology environment and to enhance the coordination and integration of information technology governance, principles, and standards for the state. While work remains to complete the enterprise architecture, ITSD should now have the resources and commitment to complete and manage this critical task.

Our audit was conducted in accordance with applicable standards contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, and included such procedures as we considered necessary in the circumstances. This report was prepared under the direction of John Blattel. Key contributors to this report were Jeff Thelen, Lori Melton, and Frank Verslues.

Claire McCaskill
State Auditor

Introduction

The state has a fiduciary responsibility to safeguard information of its citizens as well as information sensitive in nature. Information must be safeguarded using various security controls and comprehensive continuity planning capabilities. State agencies depend heavily on security controls to avoid data tampering, fraud, inappropriate access to and disclosure of sensitive information, and disruptions in critical operations. According to accepted standards, computer security is the protection afforded to an automated information system to attain the applicable objectives of preserving the confidentiality, integrity, and availability of information system resources.

State agencies must also take steps to ensure they are adequately prepared to cope with a loss of operational capability. An agency's ability to accomplish its mission can be significantly affected if it loses the ability to process, retrieve, and protect information maintained electronically. An essential element in preparing for such catastrophes is an up-to-date, detailed, and fully tested comprehensive continuity plan. A comprehensive continuity plan specifies emergency responses, backup operations, and restoration procedures to ensure the availability of critical resources to 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 resources in order of criticality.

Executive Order 05-07, issued in January 2005, initiated a statewide information technology consolidation by combining the Office of Information Technology and the Division of Information Systems to create the Information Technology Services Division (ITSD). Prior to January 2005, these two organizations were separate entities within the Office of Administration (OA) having different objectives and missions. According to Executive Order 05-07, this consolidation was done to avoid duplication of activities and administrative costs. A new Chief Information Officer (CIO) was appointed in January 2005 to oversee the ITSD and to direct the consolidation effort. Effective July 1, 2005, information technology personnel and resources from most executive branch agencies[1] were consolidated to ITSD under the direction of the state CIO. This consolidation will be accomplished in two phases. In fiscal year 2006, the technology budgets for consolidating departments were placed under the CIO's oversight and approval. In fiscal year 2007, the technology budgets

[1] The Departments of Conservation and Transportation, as well as other entities governed by commissions, are not included in the information technology consolidation. In addition, entities not under the Governor, such as elected officials and the state courts system, are not included in the consolidation.

will be transferred completely and personnel from the consolidating departments will become ITSD employees. The consolidation for the Department of Revenue's (DOR's) information technology section will be accomplished in one phase in fiscal year 2007.

According to the U.S. Government Accountability Office (GAO), an enterprise architecture (EA) is an organizational blueprint that defines, in logical or business terms and in technology terms, how an organization operates today, intends to operate in the future, and intends to invest in technology to transition to this future state. The GAO also states an EA is an essential tool for effectively and efficiently engineering business processes and for implementing and evolving supporting systems. Executive Order 03-26, issued in December 2003, authorized the state's CIO to establish an EA for Missouri. When completed, the EA will be composed of 8 domains: application, information, infrastructure, interface, interoperability, privacy, security and systems management. Executive Order 03-26 also required the CIO to convene an Information Technology Advisory Board (ITAB), composed of representatives of each executive branch department or agency and other such members as deemed appropriate. ITAB's objective, according to its charter, is to advise the CIO on information technology issues and strategies applicable to the state. In line with this objective, ITAB members serve on committees to develop the EA.

Scope and Methodology

From 2001 through 2003, the State Auditor's Office (SAO) performed six information technology security and comprehensive continuity plan audits covering four state agencies. Table 1.1 lists these six reports.

Table 1.1: Prior Audits Reviewed

Agency	Report Title	Report Number Date Issued
Department of Labor and Industrial Relations	Computer Security Controls	2001-41 May 2001
Department of Revenue	Comprehensive Continuity Planning	2002-85 September 2002
Department of Revenue	Information Resource Security Management	2003-16 February 2003
Department of Social Services	Division of Child Support Enforcement[1] Computer Risk Management Program	2003-44 May 2003
Office of Administration	Comprehensive Continuity Planning and Information Resource Security Management of the State's Accounting System (SAM II)	2003-108 October 2003
Office of Administration	State Data Center Comprehensive Continuity Planning and Mainframe Security Administration	2003-113 November 2003

[1] The Division of Child Support Enforcement (DCSE) no longer exists. Child support enforcement is now managed under the Family Support Division.

Source: SAO

To determine the implementation status of prior audit recommendations, we interviewed agency personnel, reviewed documentation, and tested controls. We determined the status of the recommendations made in these reports as of November 2005.

To evaluate the state's strategy for information technology governance, principles, and standards, we reviewed the Missouri Adaptive Enterprise Architecture, its manuals, and other statewide standards. We also interviewed the CIO regarding the state's information technology strategy.

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

- National Institute of Standards and Technology
- Information Systems Audit and Control Association
- U.S. Government Accountability Office

We requested comments on a draft of our report from the CIO. We also provided a draft of our report to the Directors of the Department of Labor and Industrial Relations, the Department of Revenue, and the Department of Social Services. We conducted our work between June and November 2005.

Agencies Have Corrected Many Weaknesses, but Risks Remain

The state has been placing a greater emphasis on security management practices to protect information technology resources. Agencies reviewed made progress in correcting security and comprehensive continuity planning weaknesses by implementing 43 of 67 recommendations made in the 6 prior audit reports. As a result, the implemented recommendations increase the agencies' ability to protect information technology resources. However, the recommendations that have not been implemented continue to expose information technology resources to unnecessary risks and highlight the need to implement controls to reduce weaknesses in security and comprehensive continuity planning capabilities.

Agencies Implemented Majority of Prior Recommendations

We reviewed the 67 recommendations made in the 6 information technology reports listed in Table 1.1 on page 6. The full text of each recommendation along with its implementation status is presented in Appendix I. Table 2.1 summarizes the implementation status of the recommendations by agency and report number.

Table 2.1: Summary of the Status of Prior Audit Recommendations

Report	Implemented	Not Implemented
Department of Labor and Industrial Relations 2001-41	10	0
Department of Revenue 2002-85	0	4
Department of Revenue 2003-16	8	12
Department of Social Services 2003-44	6	0
Office of Administration 2003-108	8	7
Office of Administration 2003-113	11	1
Total	43	24

Source: SAO

We commend the Department of Labor and Industrial Relations and the Department of Social Services for implementing all recommendations and the Office of Administration's (OA) State Data Center for implementing 11 of 12 recommendations.

Failure to Implement Recommendations Leaves State Vulnerable

Although information technology continues to change, the underlying principles of security and comprehensive continuity planning remain the same. Information technology resources, including data and systems, must be adequately protected. Security controls and comprehensive continuity plans are essential to ensure information technology resources are adequately protected.

DOR did not implement most recommendations

DOR officials implemented 8 of 24 recommendations made in the Comprehensive Continuity Planning and Information Resource Security Management audit reports. Several of the recommendations not implemented may be implemented in the near future as DOR officials

finalize and approve a security policy and as DOR is included in the information technology consolidation effort.

Three recommendations made to DOR in the Comprehensive Continuity Planning report to (1) develop a continuity planning framework, (2) develop and maintain a comprehensive continuity plan, and (3) evaluate and test environmental controls have not been implemented.[2] In addition, another recommendation made in the Information Resource Security Management report to develop a department-wide security framework and security plan has not been implemented.[3] According to DOR officials, work on these four recommendations did not occur because of employee turnover and anticipated changes due to the information technology consolidation process that will impact DOR starting in July 2006. The CIO said all consolidated agencies will be required to comply with OA's continuity planning and security frameworks.

The pending information technology consolidation also resulted in another recommendation from the DOR Comprehensive Continuity Planning report not being implemented, according to DOR officials. In accordance with accepted standards, we recommended DOR officials should document the department's backup and offsite storage procedures.[4] DOR officials stated the backups would be the responsibility of ITSD after the consolidation. The CIO said ITSD will be responsible for the backup and offsite storage of data, but departments will be responsible for identifying the data to be backed up and the frequency required. Therefore, all departments will still need to have policies and procedures related to backup after the consolidation.

DOR officials told us a security policy has been drafted and addresses seven of the audit recommendations.[5] However, the officials would not allow us review the policy because it was still in draft form. As a result, we could not determine if the prior reported weaknesses will be properly addressed.

We recommended DOR officials discontinue the use of shared user identification (IDs) and passwords to ensure accountability.[6] We also recommended DOR remove all established and unassigned user IDs to reduce the risk of unauthorized system access.[7] DOR officials said these

[2] Recommendations number 1.1, 1.2, and 1.4 from report number 2002-85.

[3] Recommendation number 2.1 from report number 2003-16.

[4] Recommendation number 1.3 from report number 2002-85.

[5] Recommendations number 1.3, 1.5, 1.8, 1.9, 2.3, 2.4, and 3.1 from report number 2003-16.

[6] Recommendation number 1.10 from report number 2003-16.

[7] Recommendation number 1.11 from report number 2003-16.

recommendations had been implemented. However, based on a review of the list of DOR users as of October 2005, we identified user IDs that were still being shared and IDs still not assigned to any user. These officials said they were not aware the IDs were still shared and would investigate. All system users and their activity should be uniquely identifiable, according to accepted standards.

We reported DOR officials performed background investigations for all new employees, but did not perform background reinvestigations.[8] In addition, the audit reported DOR officials had not reviewed positions to determine sensitivity. A DOR official stated the only background checks obtained by the department as of October 2005 are those required by OA for employees with access to the state's accounting system (SAM II). The official also stated there have been no assessments completed to determine which employees need to have background reinvestigations completed. Accepted standards state sensitivity levels are used to determine if job positions require background screenings. Without determining levels of sensitivity of job positions, management cannot determine if job positions require additional background screenings and reinvestigations.

We reported DOR officials did not train personnel on an ongoing basis regarding computer security and their role in ensuring appropriate use of department resources.[9] No changes have been made to DOR's training program since our audit. A DOR official said security training is given to all new employees and security notices are sent to employees periodically when security concerns arise. According to accepted standards, continuous education, training and awareness are all necessary to successfully implement any computer security program.

Some recommendations made to OA regarding the SAM II system still not implemented

OA officials implemented 8 of the 15 recommendations made regarding SAM II. Recommendations made to OA in the SAM II report to (1) establish a data classification framework scheme and appoint data resource owners, (2) assess the effectiveness of system security controls, (3) log, monitor and investigate security-related events, and (4) update the responsibilities and procedures for security administrators have not been implemented.[10] According to the SAM II system administrator, OA does not have the funding or resources necessary to implement these four recommendations but will reevaluate the recommendations if funds and resources become available.

[8] Recommendation number 1.12 from report number 2003-16.

[9] Recommendation number 2.2 from report number 2003-16.

[10] Recommendations number 2.1, 2.2, 2.9, and 2.10 from report number 2003-108.

We recommended OA officials document backup and offsite storage procedures for the SAM II system.[11] The SAM II system administrator said no changes had been made to the documented procedures because she believed the procedures in place were already adequate. However, these procedures still lack essential elements including documentation of the backup files and data, the personnel responsible for the backup functions, and details of the methods and frequency of backups. Accepted standards state management should have documented procedures for the availability of all data files required to restore and recover critical business functions.

To ensure SAM II data was being backed up and stored correctly, we recommended OA officials test backup files more frequently than just during the state's annual disaster recovery test.[12] The system administrator said no additional testing of the backup files had been performed outside of the annual disaster recovery test because management felt this test was as frequent as needed. According to accepted standards, additional tests are necessary to identify weaknesses in restoration procedures and to ensure backups are being performed correctly.

Our audit recommended OA officials segregate programmer duties by limiting access rights to essential job functions.[13] If segregation was not possible, we recommended OA establish compensating controls. OA officials took steps to implement this recommendation by segregating duties as much as they thought possible, according to the system administrator. However, the officials did not take steps to implement compensating controls, such as increased supervisory monitoring, where segregation was not possible. Accepted standards state management should implement a division of roles and responsibilities or other controls to reduce the possibility for a single individual to subvert a critical process.

State Data Center implemented nearly all recommendations

State Data Center officials took action to implement 11 of 12 recommendations. To improve the protection of information technology resources and system integrity, we recommended that as administrators of data center security, oversight controls should be established to monitor state agencies' compliance with the data center's security policies.[14] This recommendation has not been implemented. Data center officials commented in the prior report that monitoring other agencies was not within the scope of the data center's services or responsibilities. However, the information technology consolidation effort places agency technology

[11] Recommendation number 1.3 from report number 2003-108.
[12] Recommendation number 1.4 from report number 2003-108.
[13] Recommendation number 2.8 from report number 2003-108.
[14] Recommendation number 2.2 from report number 2003-113.

personnel in the same department as the data center, which should allow oversight controls to be more effectively established and enforced. The state CIO agreed monitoring compliance for the consolidated agencies would be possible after the consolidation.

Conclusions

Agencies have corrected many of the previously reported weaknesses by devoting the resources to and placing a greater emphasis on information security management practices. However, addressing the 24 recommendations that have not been implemented would enhance security and provide additional protection for the state's information technology resources. To ensure protection of information technology resources in today's rapidly changing environment, agencies must ensure security controls and comprehensive continuity planning capabilities are in place.

Recommendation

The Chief Information Officer work with the agencies to implement the remaining recommendations and to monitor their progress towards full compliance.

Agency Comments

The Information Technology Services Division (ITSD) agrees that it will continue to work with the consolidated agencies to implement the remaining recommendations and to monitor their progress toward full compliance.

With respect to the three recommendations in the Comprehensive Continuity Planning report and the recommendation in the Information Resource Security Management report, all four to the Department of Revenue (DOR), the DOR, as one of the consolidated agencies, will be required to comply with OA ITSD's continuity planning and security frameworks. (See page 9)

With respect to the recommendation in the Comprehensive Continuity Planning report that the DOR document its backup and offsite storage procedures, consolidated departments will be responsible for identifying the data to be backed up and the frequency required; thus, the DOR will need to document its policies and procedures regarding backups. (See page 9)

With respect to the recommendations regarding DOR's security policy, and that DOR discontinue the use of shared user identification (IDs) and passwords, train personnel on an ongoing basis regarding computer security, and determine the level of sensitivity of job positions which require additional background screenings and reinvestigations, consolidated agencies must comply with OA ITSD's security policy. (See pages 9 and 10)

With respect to the four recommendations to OA in the SAM II report, OA ITSD responds as follows: (See page 10)

> *The Enterprise Architecture Committee is currently drafting a data classification standard. As soon as that standard has been approved, SAM II will adopt that standard and appoint data resource owners based on data classification.*
>
> *OA ITSD has purchased software and hardware that will test the effectiveness of system security controls. Staff has just completed training on the product and testing will begin in the near future.*
>
> *One of the tasks assigned to the OA ITSD Information Security Management Office is to monitor and investigate all security related events within the consolidated agencies. As we move forward, appropriate logging requirements will be implemented.*
>
> *Due to consolidation, this task is being held until the consolidation has been completed and appropriate responsibilities have been assigned to the appropriate staff.*

With respect to the recommendation that OA officials document backup and offsite storage procedures for the SAM II system, the ITSD believes that it has included the essential elements in its procedures. (See page 11)

> *The SAM II system uses automated database utility batch jobs to perform file backups. They run automatically every night immediately after the online system is brought down. These same backups also run at the end of various SAM II nightly batch cycles such as the HR Daily, HR Paycycle, and the Financial Daily. No personnel intervention is required to perform backups. The backup files can be used for system/file restores.*

With respect to the recommendation that OA officials test SAM II backup files more frequently than just during the state's annual disaster recovery test, the ITSD clarifies its prior response as follows: (See page 11)

> *Production file backups and disaster recovery backups are produced daily for the SAM II system. Production file backups are tested throughout the year for production database restores. They are also tested when we load a test database in that we use the production backup file for that purpose.*
>
> *Consequently, backups are successfully tested and used for restoration tasks periodically throughout the year.*

Restoration from the disaster recovery backups occur during an annual statewide drill. Disaster recovery testing is very expensive and would be cost prohibitive to perform more than annually.

Given the periodic testing of production backups and the annual disaster recovery backup testing, OA feels that the current processes are adequate for the SAM II backups and restoration.

With respect to the recommendation that OA officials implement compensating controls in segregating programmer duties, ITSD agrees with the recommendation. (See page 11)

OA/Systems and Programming will create a separate document to log all occurrences and details that describe changes to SAM II source code made by on-call programming staff that is moved to the production environment in order to successfully complete a batch cycle. The manager/supervisor will review the documentation, initial, date, and file a hardcopy. Note: It is very rare that SAM II source code is changed in this manner and under these circumstances.

With respect to the recommendation that OA officials establish oversight controls to monitor state agencies' compliance with the data center's security policies, the ITSD agrees that monitoring the consolidated agencies is within the scope of the data center's services and responsibilities and will be possible after consolidation. (See page 11 and 12)

Enterprise Architecture on Road to Completion

The state has made progress developing an EA, but this architecture is not complete. Necessary work remains to develop and manage a fully mature EA capable of providing all of the benefits needed to more effectively and efficiently manage the state's information technology resources. The architecture has not been fully developed because, prior to the state's information technology consolidation, the CIO had no authority to commit the resources needed for the task.

Status of EA Development

We evaluated Missouri's EA and manual using a benchmarking tool as of November 2005. According to the state's EA manual, "the goal of statewide Enterprise Architecture is to enhance coordination, simplify integration, build a consistent infrastructure, and generally allow greater efficiencies in the development of technology solutions. The intent of the Missouri Adaptive Enterprise Architecture program is to realize these goals while ensuring effective use of state resources, thereby enabling consistent, effective delivery of services to the employees, citizens, and businesses of Missouri."

In April 2003, GAO published a management maturity framework to provide a benchmarking tool for planning and measuring efforts to improve EA management.[15] The maturity framework is made up of five stages of EA maturity with stage 1 being the least mature and stage 5 representing a fully mature architecture. Each stage reflects a collection of key best practices or conditions needed for effective EA management. The state has implemented some of the framework's Stage 2 key practices for building the EA management foundation, but important foundational practices still need to be fully developed. Some additional practices and conditions have also been met for the subsequent stages. Table 3.1 lists the key best practices included in the GAO framework along with an indication of which practices the state has met.

[15] *A Framework for Assessing and Improving Enterprise Architecture Management*: GAO 03-584G, April 2003, www.gao.gov.

Table 3.1: Summary of Missouri's Satisfaction of Key Enterprise Architecture Management Practices Described in GAO EA Management Maturity Framework (Version 1.1)

Stage	Key Best Practices and Conditions	Status as of November 2005
Stage 1: Creating EA awareness	Agency is aware of EA.	✓
Stage 2: Building the EA management foundation	Adequate resources exist.	✓
	Committee or group representing the enterprise is responsible for directing, overseeing, or approving EA.	✓
	Program office responsible for EA development and maintenance exists.	✓
	Chief architect exists.	✓
	EA is being developed using a framework, methodology and automated tool.	✓
	EA plans call for describing both the "as-is" and the "to-be" environments of the enterprise, as well as a sequencing plan for transitioning from the "as-is" to the "to-be."	—
	EA plans call for describing both the "as-is" and the "to-be" environments in terms of business, performance, information/data, application/service, and technology.	—
	EA plans call for business, performance, information/data, application/service, and technology descriptions to address security.	—
	EA plans call for developing metrics for measuring EA progress, quality, compliance, and return on investment.	—
Stage 3: Developing EA products	Written and approved organization policy exists for EA development.	✓
	EA products are under configuration management.	✓
	EA products describe or will describe both the "as-is" and the "to-be" environments of the enterprise, as well as a sequencing plan for transitioning from the "as-is" to the "to-be."	—
	Both the "as-is" and the "to-be" environments are described or will be described in terms of business, performance, information/data, application/service, and technology.	—
	Business, performance, information/data, application/service, and technology descriptions address or will address security.	—
	Progress against EA plans in measured and reported.	—

Table 3.1: Summary of Missouri's Satisfaction of Key Enterprise Architecture Management Practices Described in GAO EA Management Maturity Framework (Version 1.1) *(Continued from previous page)*

Stage	Key Best Practices and Conditions	Status as of November 2005
Stage 4: Completing EA products	Written and approved organization policy exists for EA maintenance.	✓
	EA products and management processes undergo independent verification and validation.	✓
	EA products describe both the "as-is" and the "to-be" environments of the enterprise, as well as a sequencing plan for transitioning from the "as-is" to the "to-be."	—
	Both the "as-is" and the "to-be" environments are described in terms of business, performance, information/data, application/service, and technology.	—
	Business, performance, information/data, application/service, and technology descriptions address security.	—
	Organization CIO has approved current version of EA.	✓
	Committee or group representing the enterprise or the investment review board has approved current version of EA.	✓
	Quality of EA products is measured and reported.	—
Stage 5: Leveraging the EA to manage change	Written and approved organization policy exists for information technology investment compliance with EA.	—
	Process exists to formally manage EA change.	✓
	EA is integral component of information technology investment management process.	—
	EA products are periodically updated.	✓
	Information technology investments comply with EA.	—
	Organization head has approved current version of EA.	✓
	Return on EA investment is measured and reported.	—
	Compliance with EA is measured and reported.	—

✓ Fully satisfied

— Not fully satisfied

Source: GAO EA Management Maturity Framework (Version 1.1) and SAO evaluation of Missouri's EA

Table 3.1 shows the state is making progress towards completion of the EA.

Consolidation Helps in EA Development

ITAB began work on the EA in 1997. The CIO said since each state agency's information technology units operated autonomously before the state's information technology consolidation, the previous CIO did not have the authority to require work on and compliance with the EA. Due to the consolidation, the CIO stated he now has the authority to require participation in the development process and to enforce compliance with it.

The CIO said the process to develop and implement the EA should proceed at a smoother and quicker pace than prior to the consolidation. According to the GAO, the importance of developing, implementing, and maintaining an EA is a basic tenet of both organizational transformation (consolidation) and information technology management. Managed properly, an EA can clarify and help optimize the interdependencies and relationships among an organization's business operations and the underlying information technology resources and systems that support these operations.

Conclusions

Important steps have been taken to develop, implement, and manage the EA for the state. However, until the EA has been fully developed, including management procedures to measure and improve architecture effectiveness, the state is at risk of having missing or inadequate principles and standards and incompatible or redundant information technology resources. Although the EA is not complete, progress is expected to continue and the consolidated state agencies will be required to comply with architecture policies.

Recommendation

The Chief Information Officer continue to develop the EA and use the GAO maturity framework, or similar framework, to measure and improve EA management effectiveness.

Agency Comments

ITSD agrees that consolidation provides the authority to allow it to reach a fully mature architecture as described in the GAO maturity management framework. Efforts are ongoing to address those Key Best Practices and Conditions currently not achieved.

Status of Prior Recommendations

Table I.1 presents the status of our prior recommendations for Department of Labor and Industrial Relations report number 2001-41, as of November 2005.

Table I.1: Status of Prior Recommendations for Department of Labor and Industrial Relations report number 2001-41

Prior recommendations		Status
1.1	Develop a risk management program, that includes (1) asset valuation to determine the near-term and long-term consequences if data are lost or corrupted, and computer and LAN support is lost, (2) threat identification such as, intentional and unintentional errors, disgruntled employees, fire, and natural disaster, (3) vulnerability analysis to determine if current controls could be exploited by identified threats, and (4) design security processes and procedures to mitigate the identified risks that are not currently controlled.	Implemented
1.2	Prepare a disaster recovery plan to ensure the department can continue to process and pay unemployment and second injury fund payments if computer and/or LAN operations are disrupted for an extended period.	Implemented
1.3	Establish a monitoring process to periodically reassess the effectiveness of computer security controls, including computer logging systems and employees' access rights to sensitive systems and data.	Implemented
1.4	Establish a written policy that requires all employees with desktop computers to activate their desktop screen passwords after 5-10 minutes of inactivity.	Implemented
1.5	Assign sensitivity levels to job positions and perform background screening where appropriate.	Implemented
1.6	Follow the procedures and steps in the National Institute of Standards and Technology's Special Publication 800-12, where appropriate, in implementing the above recommendations. This publication and other National Institute of Standards and Technology computer security related publications are electronically available at **http://csrc.nist.gov**.	Implemented
2.1	Assign overall responsibility and authority for the department's computer security program to an appropriate senior official, and designate a department computer security officer.	Implemented
2.2	Develop comprehensive computer security policies that include such elements as security planning, risk management, periodic reviews of security controls, personnel background screening, contingency planning, training, access controls, and audit trails.	Implemented
2.3	Use the National Institute of Standards and Technology computer security self-assessment guide to evaluate the effectiveness of its computer security program and make improvements where needed.	Implemented
2.4	Establish a security awareness and training program based on National Institute of Standards and Technology guidelines as appropriate.	Implemented

Source: SAO

Appendix I
Status of Prior Recommendations

Table I.2 presents the status of our prior recommendations for Department of Revenue report number 2002-85, as of November 2005.

Table I.2: Status of Prior Recommendations for Department of Revenue report number 2002-85

Prior recommendations		Status
1.1	Define and implement a continuity planning framework, including standards and policies for the development and maintenance of comprehensive business continuity and information technology recovery plans. Ensure this framework includes provisions to: • Assign the responsibility of coordinating disaster recovery and business resumption activities to an emergency management team, and ensure all personnel are aware of and trained in their duties and responsibilities as they apply to the comprehensive continuity plan. • Develop formal procedures to incorporate periodic business impact analysis to monitor the ongoing requirements of the business continuity plans and arrangements. • Develop and document adequate emergency response procedures regarding information technology recovery activities, and ensure staff are appropriately trained on how to respond in the event of an emergency.	Not Implemented
1.2	Develop, implement, and maintain a comprehensive continuity plan, which consists of both a business continuity plan and an information technology recovery plan. Once the plans are implemented, they should be periodically tested.	Not Implemented
1.3	Develop and document backup, recovery, and offsite storage procedures for critical data files, applications, media, documentation, and other information technology resources to support the recovery and resumption of business processes and system operations. These procedures should include policies to test recovery of backup applications and data, use of a librarian to track backup data, perpetual inventories of backup data and media in secondary storage, segregation of duties for personnel responsible for creating backup data, and proper storage of backup data.	Not Implemented
1.4	Evaluate the adequacy of environmental controls in place and test the controls periodically.	Not Implemented

Source: SAO

Appendix I
Status of Prior Recommendations

Table I.3 presents the status of our prior recommendations for Department of Revenue report number 2003-16, as of November 2005.

Table I.3: Status of Prior Recommendations for Department of Revenue report number 2003-16

Prior recommendations		Status
1.1	Evaluate the usage of the mainframe user ID management systems and implement procedures to eliminate the discrepancies between the systems.	Implemented
1.2	Evaluate the number of system and application administrators that control access to department data and information system resources. In addition, establish procedures for supervisors to periodically review system and application administrator activity.	Implemented
1.3	Establish department-wide controls over the configuration of user and group profiles to ensure that access rights for users are commensurate with users' job responsibilities.	Not Implemented
1.4	Document and define datasets and ensure only appropriate users have access.	Implemented
1.5	Ensure policies, procedures, and standards are documented and followed in granting access to data and information system components.	Not Implemented
1.6	Ensure the functions of critical processes including that of data entry and systems development and maintenance are properly segregated.	Implemented
1.7	Ensure a list of contractors with access to department resources and the access given is maintained.	Implemented
1.8	Ensure supervisors perform documented periodic reviews of user access levels to determine if they remain appropriate.	Not Implemented
1.9	Establish policies, procedures, and standards which document the criteria to be followed in closing user accounts and removing access to data and information system resources. These procedures should include policies on monitoring and removing inactive user accounts.	Not Implemented
1.10	Establish user groups for users with similar job functions and access rights and discontinue the use of shared IDs and passwords.	Not Implemented
1.11	Remove all unassigned user IDs established and formalize procedures to create new IDs upon authorized request.	Not Implemented
1.12	Ensure background reinvestigations are performed periodically for applicable employees.	Not Implemented
2.1	Complete design, development, and approval of a department-wide security framework and security plan. The security framework should be designed to document and ensure consistent implementation of effective and consistent security practices for all divisions and personnel. Ensure the plan includes: • A data and information classification framework scheme and guidelines for classifying all data and information in terms of criticality and sensitivity, which is determined by a formal and explicit decision by the data owner. • A structure for formally appointing data and information resource owners and for defining their roles and responsibilities, which includes making decisions about classification and access rights.	Not Implemented

Table I.3: Status of Prior Recommendations for Department of Revenue report number 2003-16
(Continued from previous page)

Prior recommendations		Status
2.2	Implement an ongoing security awareness program to ensure all personnel and end-users are aware of appropriate, department-wide security policies and standards and are informed of their individual responsibilities relative to ensuring a secure processing environment.	Not Implemented
2.3	Establish policies and procedures for assessing the effectiveness of operational security controls. Consider using the National Institute of Standards and Technology computer security self-assessment guide to evaluate this effectiveness and make improvements where needed.	Not Implemented
2.4	Develop and document department-wide policies and procedures for (1) logging system access, (2) monitoring access and security violations, and (3) reporting to ensure the proper functioning of controls in the department security framework.	Not Implemented
2.5	Ensure employee termination policies and procedures are enforced.	Implemented
3.1	Ensure the responsibilities for physical security and protection are clearly defined, documented, and enforced.	Not Implemented
3.2	Ensure policies for identifying and monitoring visitors to department facilities are enforced.	Implemented
3.3	Maintain accurate reports of individuals with physical access to the department's facilities and regularly review those reports to ensure that current employees have appropriate access.	Implemented

Source: SAO

Appendix I
Status of Prior Recommendations

Table I.4 presents the status of our prior recommendations for Department of Social Services report number 2003-44, as of November 2005.

Table I.4: Status of Prior Recommendations for Department of Social Services report number 2003-44

Prior recommendations	Status
1.1 Develop a comprehensive risk management program, which would include policies and procedures requiring: • Risk assessments, specifying their frequency, and the responsible personnel. • Risk assessments when major system changes occur.	Implemented
1.2 Develop a comprehensive and current disaster recovery plan for DCSE's computerized system which: • Reestablishes communication lines with the DCSE contractor who issues child support checks, reestablishes DCSE's computerized system capability on a statewide basis, and identifies the responsibilities of those carrying out the disaster recovery plan. • Identifies and prioritizes critical operations and data, reflects current conditions, and is approved by senior program managers. • Lists resources such as hardware, software, system documentation, and other computer supplies, which support critical operations. • Lists facilities housing critical resources.	Implemented
1.3 Develop policies and procedures to: • Ensure plans for backup and restoration of all critical applications are complete, reflect changes as they occur, and are checked for accuracy at least semi-annually. • Require storing the proper system and application documentation at the off-site location, which are needed for successful recovery of application resources. • Require deficiencies disclosed during disaster recovery testing be corrected, and verified when possible, prior to the next disaster recovery exercise. • Require applications testing be performed by day-to-day users of the system during disaster recovery testing to ensure all needed data and screens are available. At a minimum, day-to-day users should review the documented results of the applications testing.	Implemented

Table I.4: Status of Prior Recommendations for Department of Social Services report number 2003-44
(Continued from previous page)

Prior recommendations	Status
2.1 DCSE officials should: • Ensure paperwork is completed and remitted timely to the technical support division when revoking user IDs for employees and non-department users who terminate, transfer, or no longer need access to DCSE's computerized system. • Ensure employees do not share user IDs and passwords, and employees are not allowed to use multiple user IDs. • Discontinue issuing multiple user IDs that result in bypassing security protocols. • Track all suspected DCSE system access violations and report all suspected and proven violations to division management. • Document policies and procedures for periodically reviewing user access rights for DCSE system users. • Review policies allowing technicians read-only access to all cases and update access to all members on DCSE cases, to determine if this access is actually needed for the technicians to perform their duties. • Develop specific policies and procedures for granting dial-up access to the computerized system. Additionally, this access should be reviewed periodically to ensure it remains appropriate.	Implemented
2.2 The department's technical support division should: • Establish a process for monitoring inactive user IDs, specifically for DCSE's computerized system. • Ensure department password resetting protocols are properly followed. • Develop accurate and up-to-date policies and procedures for reviewing audit trails, including who is responsible for reviewing audit trail reports and what follow-up action should be taken on apparent access violations. • Develop policies and procedures to ensure only appropriate employees have access to make changes through security software.	Implemented
2.3 Department officials should ensure criminal background checks are properly performed and documented on each newly hired or newly transferred employee with access to DCSE's computerized system.	Implemented

Source: SAO

Appendix I
Status of Prior Recommendations

Table I.5 presents the status of our prior recommendations for Office of Administration report number 2003-108, as of November 2005.

Table I.5: Status of Prior Recommendations for Office of Administration report number 2003-108

Prior recommendations		Status
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.	Implemented
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.	Implemented
1.3	Document SAM II system backup and offsite storage procedures necessary to recover system operations and resume business processes.	Not Implemented
1.4	Test off-site back up files more frequently than during the state's annual recovery test.	Not Implemented
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.	Not Implemented
2.2	Establish procedures for assessing the effectiveness of system security controls.	Not Implemented
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.	Implemented
2.4	Work with the software vendor to resolve the system inactivity user logoff feature that has been unavailable since October 2002.	Implemented
2.5	Ensure system administrators perform supervisory reviews of the assignment and use of privileged accounts.	Implemented
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.	Implemented

Table I.5: Status of Prior Recommendations for Office of Administration report number 2003-108
(Continued from previous page)

Prior recommendations		Status
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.	Implemented
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.	Not Implemented
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.	Not Implemented
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.	Not Implemented
2.11	Establish hiring and termination procedures which give appropriate consideration to security issues and technical skills.	Implemented

Source: SAO

Appendix I
Status of Prior Recommendations

Table I.6 presents the status of our prior recommendations for Office of Administration report number 2003-113, as of November 2005.

Table I.6: Status of Prior Recommendations for Office of Administration report number 2003-113

Prior recommendations		Status
1.1	Complete development and implementation of a detailed comprehensive continuity plan which will support the data center's recovery strategy that ensures critical information systems processing functions can continue in the event of a significant disruption to normal computer operations. Procedures and objectives of testing the plan should be incorporated.	Implemented
1.2	Establish a formal maximum tolerable outage time for the data center's operations.	Implemented
1.3	Review the current access rights to the recovery plan to ensure they are appropriate and necessary as well as prepare procedures for establishing future access to the plan.	Implemented
1.4	Develop procedures to incorporate a periodic impact analysis process to monitor the ongoing requirements of recovery plans.	Implemented
1.5	Develop and document backup and off-site storage procedures for critical data files to support the recovery and resumption of business processes and system operations.	Implemented
1.6	Test off-site backup files more frequently than during the state's annual recovery test.	Implemented
1.7	Improve contract procedures, which should include ensuring planned specifications are used in soliciting bids and re-bidding contracts once renewal options have expired or sooner if warranted.	Implemented
2.1	Establish security guidelines and procedures for the state entities to ensure adequate controls of access to data.	Implemented
2.2	Establish and perform oversight controls for the RACF system to be used to monitor state entities.	Not Implemented
2.3	Implement internal security procedures and controls regarding access of data center personnel to ensure the protection of information technology resources and integrity of information technology systems for the state. These procedures should include: • Performing documented periodic reviews of user access rights to determine if they remain appropriate. • Routinely reviewing security-related events, monitoring access, investigating apparent security violations, and taking appropriate remedial action. • Reviewing the actions of privileged accounts.	Implemented
2.4	Perform and document a review of current RACF system security settings to ensure they are appropriate and establish procedures to ensure future changes to system security settings are documented and approved.	Implemented

Table I.6: Status of Prior Recommendations for Office of Administration report number 2003-113
(Continued from previous page)

Prior recommendations	Status
2.5 Ensure system security duties are properly segregated from auditing duties and access rights are limited to essential job functions. If proper segregation cannot be done, implement compensating controls to limit any resulting control weaknesses.	Implemented

Source: SAO