Thomas A. Schweich

Missouri State Auditor

REVENUE

Taxation Division Security Controls

September 2011

Report No. 2011-56

http://auditor.mo.gov

Thomas A. Schweich
Missouri State Auditor

CITIZENS SUMMARY

Findings in the audit of the Department of Revenue, Taxation Division Security Controls

Background

This audit reviewed security and other internal controls established and managed by the Department of Revenue (DOR), Taxation Division and the Office of Administration, Information Technology Services Division (OA-ITSD). The OA-ITSD provides technical support to the DOR, Taxation Division, which is responsible for collecting Missouri taxes and administering state tax laws. The section of OA-ITSD responsible for supporting the DOR is referred to as the ITSD in this summary and report.

Service Level Agreement

The DOR and the OA-ITSD do not have a current written agreement adequately documenting the terms of the partnership between the two entities. The memorandum of understanding, in place since 2006, is not up-to-date and lacks critical information, such as defining: operational responsibilities for each organization, qualitative or quantitative measures of services to be provided, or responsibilities for third-party software, backup, disaster recovery and continuity planning.

The OA-ITSD did not have a contract for disaster recovery facilities for some critical mainframe resources, including certain Taxation Division systems, for almost a year. Instead of renewing the existing disaster recovery contract when it expired in June 2010, the OA-ITSD decided to explore other more cost-effective options, but it took eleven months to get the new disaster recovery capability in place, leaving the state vulnerable in the interim in the event of a disaster.

The DOR has not told ITSD how long the Taxation Division systems could be down before significant losses would occur. ITSD needs this information to determine whether the current recovery plan is sufficient. In addition, the ITSD has not conducted recovery testing to ensure that backups are complete and accurate and contain all data necessary to recover critical systems in the event of a disaster.

User Account Management

The ITSD database administrators are able to add, edit or delete data directly in the DOR, Taxation Division databases without management review, which increases the risk of unauthorized changes going undetected. Such direct database revisions are not subject to system validation and edit checks.

DOR and ITSD do not periodically review user access rights to the network or the DOR, Taxation Division systems and data. DOR security policies require division directors to review reports of user access at least twice a year, but we were told by a DOR official this review is not conducted. When we reviewed user accounts with access to DOR systems, we discovered 24 former employees still had active user accounts (one of whom left the DOR in 2001); 9 accounts were active in the system but not assigned to specific users; and 807 active user accounts had not been accessed in over

	90 days, calling into question whether these users continue to need this access. As noted in our 2003 and 2006 reports, the ITSD maintains unassigned user accounts for DOR systems (2,700 at the time of the present audit), which increases the risk of unauthorized access to confidential data. The DOR also lacks a policy for granting system access to temporary employees.
Risk Assessment Program	The DOR lacks a comprehensive risk assessment and management program. A risk assessment helps identify potential threats, vulnerabilities and weaknesses and determines what steps should be taken to prevent losses.
Browsing of Taxpayer Records	Although the DOR uses security controls to limit access to tax systems, management does not have procedures in place to monitor employee access to ensure only appropriate access to tax return information is occurring.

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

American Recovery and Reinvestment Act 2009 (Federal Stimulus)	Not applicable.

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

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

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

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

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

Department of Revenue
Taxation Division Security Controls
Table of Contents

THOMAS A. SCHWEICH
Missouri State Auditor

Honorable Jeremiah W. (Jay) Nixon, Governor
and
Alana M. Barragán-Scott, Director
Department of Revenue
and
Doug Young, Chief Information Officer
Office of Administration, Information Technology Services Division
Jefferson City, Missouri

We have audited the Department of Revenue (DOR) and the Office of Administration Information Technology Services Division (ITSD) general controls related to the overall security of DOR Taxation Division computer systems and certain security controls related specifically to the Missouri Individual Income Tax System. This audit was conducted to evaluate the effectiveness of security controls and other related internal controls designed to secure confidential citizen information and tax-related data, and because most state general revenues are processed through the DOR Taxation Division systems. The objectives of our audit were to:

1. Evaluate the security controls designed to ensure the confidentiality, integrity, and availability of data and information maintained by the Taxation Division systems.

2. Evaluate compliance with certain legal provisions.

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

Certain information contained in DOR records was not provided to us based on the Director of Revenue's interpretation of the decision rendered by the Missouri Supreme Court in the case of Director of Revenue v. State Auditor 511 S.W.2d 779 (Mo. 1974). Other information was not readily available due to the age, design, and complexity of the Taxation Division computer systems and underlying technology. As a result, we could not audit certain information because of these limitations imposed on the scope of our audit.

Our audit determined DOR and ITSD management have not taken some measures necessary to maintain effective security controls to ensure the confidentiality, integrity, and availability of data and information maintained by the Taxation Division systems. We determined DOR management, while in compliance with certain legal provisions we reviewed, could implement additional controls to protect the privacy of taxpayer data. We also determined certain weaknesses in management practices and information system control activities exist, which increase the risk of confidential information being compromised.

Except as discussed in the second paragraph, we conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform our audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides such a basis.

Thomas A. Schweich
State Auditor

The following auditors participated in the preparation of this report:

Director of Audits:	John Luetkemeyer, CPA
Audit Manager:	Jeffrey Thelen, CPA
In-Charge Auditor:	Lori Melton, M.Acct., CPA
Audit Staff:	Patrick M. Pullins, M.Acct.

Department of Revenue
Taxation Division Security Controls
Introduction

Background

Data security is a critical consideration for any organization dependent on information systems and networks to meet its mission or business objectives. Data security is especially important for state agencies, where the public's trust is essential for the efficient delivery of services. Security can be a significant investment, which adds to an already long list of administrative duties. Managing secure networks, developing and implementing new system functionality, maintaining thousands of system users, and other day-to-day security tasks can strain limited administrative resources. However, agency management must understand proper protection of citizen information is a requirement and not a luxury in the current interconnected cyber environment. Without proper safeguards and controls, computer systems and confidential data are vulnerable to individuals with malicious intentions who can use access to obtain sensitive data or disrupt operations.

The Department of Revenue (DOR) was created by Article IV, Section 12, of the 1945 Missouri Constitution and serves as the central collection agency for state revenues.

The DOR Taxation Division is responsible for collecting Missouri taxes and administering state tax laws. During fiscal year 2010, the Taxation Division processed tax receipts of approximately $11.9 billion, according to DOR records. The Taxation Division administers and collects personal taxes, including individual income, partnerships, fiduciary, and estate taxes and also administers the Property Tax Credit and Homestead Tax Credit programs. In addition, the Taxation Division also collects various business taxes including sales/use, financial institution, insurance premium, franchise, excise, cigarette and other tobacco products, motor fuel, corporate income, and withholding taxes.

To administer and process the collection of individual income taxes, the Taxation Division uses the Missouri Individual Income Tax System (MINITS). This system was established in 1989 and has been updated at least yearly to account for tax law and other necessary changes. The MINITS is based on dated technology for which the pool of skilled personnel with the ability to maintain the system continues to decline. This dated technology platform limits management data analytical capabilities and the ability of the MINITS to interface with other more modern Taxation Division systems.

In the fiscal year 2012 budget proposal, released January 2011, the Governor proposed a $5 million appropriation to the DOR to fund implementation of "a modern, efficient collections information technology system" for the department. This proposed system is expected to replace the MINITS as well as other systems used to administer and collect personal and business taxes. The $5 million appropriation was included in the DOR

2012 budget as introduced in the legislature. However, only $1 million was appropriated in the final budget. The state issued a request for proposals in May 2011, for this consolidated system. The estimated total cost of the project is approximately $62 million. Benefit studies conducted by potential vendors found a new integrated tax system could result in additional revenue due to opportunities for improvement in collections and additional processing efficiencies.

The mission of the Office of Administration, Information Technology Services Division (OA-ITSD)[1] is to provide technology services and solutions to state agencies, including assistance to support DOR technology resources. The DOR maintains ownership of its information systems and data, while the ITSD provides technical support. As part of the technology support function, the OA-ITSD established the Missouri Adaptive Enterprise Architecture (MAEA)[2] to guide information technology decisions. The DOR is required to follow MAEA standards and policies.

According to accepted standards, security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Confidentiality refers to preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information. Integrity relates to guarding against improper information modification or destruction, and availability ensures timely and reliable access to and use of information.

Scope and Methodology

The scope of our audit included security controls and other related internal controls established and managed by the DOR and OA-ITSD; policies and procedures; and other management functions and compliance issues in place during the 2 years ended June 30, 2011.

Our methodology included conducting interviews with appropriate officials and staff; obtaining and reviewing available policies and procedures, federal laws, and other applicable information; and performing testing.

We obtained data files from the ITSD of user accounts having access to DOR systems as of January and March 2011. To ensure completeness of the

[1] In this report, OA-ITSD refers to the entire division, while ITSD refers to the section within the OA-ITSD assigned specific responsibility for supporting DOR technology resources.

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

data, we reviewed the accounts for reasonableness and scanned the names of employees. Although we used computer-processed data from DOR systems to identify and test user accounts and related information, we did not rely on the results of any processes performed by these systems in arriving at our conclusions. Our conclusions were based on our review and testing of controls over user accounts.

We obtained the employment records of all DOR and ITSD employees for fiscal years 2001 to 2011 from the statewide accounting system for human resources. We matched these records to user accounts with access to DOR systems to determine if any terminated employees had active user accounts. We provided DOR officials a list of all terminated employees we found who had active access to DOR systems. Although we used computer-processed data from the human resources system for our audit work, we did not rely on the results of any processes performed by this system in arriving at our conclusions. Our conclusions were based on our review of the issues specific to the audit objectives.

We obtained individual state income tax data, excluding confidential personally identifiable data, for taxpayers who filed paper tax returns for tax year 2009. We performed basic reasonableness tests on this data and did not find any reportable issues. However, due to the design and age of the system and technology platform the system operates in, we were not able to review all system controls because records of processing edits[3] applied to certain data or processing events are not maintained after tax returns are processed. Although we used computer processed data from the MINITS for our audit work, we did not rely on the results of any processes performed by this system in arriving at our conclusions.

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

- Missouri Adaptive Enterprise Architecture (MAEA)
- National Institute of Standards and Technology (NIST)
- Government Accountability Office (GAO)
- IT Governance Institute Control Objectives for Information and related Technology (COBIT)

[3] An edit, also known as a data validity check, is program code that tests the input for correct and reasonable conditions; such as account numbers falling within a range; numeric data being all digits; dates having a valid day, month, and year; etc.

1. Service Level Agreement

The Department of Revenue (DOR) and the Office of Administration Information Technology Services Division (OA-ITSD) do not have a current agreement documenting the terms of the partnership between the two entities. As a result, DOR management does not have minimum performance targets for information technology (IT) services and cannot determine if the services delivered meet targeted levels.

A Service Level Agreement (SLA) is a document used by organizations entering into a partnership for the provision of IT services. According to accepted standards, the SLA should document the agreements reached regarding:

- Technical and administrative support to be provided by the service provider
- Service support requirements, including availability, reliability, performance, and capacity for growth
- Roles and responsibilities of each party, including responsibility for oversight
- Backup, recovery, and security responsibilities of each party
- Quantitative and/or qualitative metrics for measuring service
- Funding arrangements
- Customer commitments

1.1 Current agreement

The DOR and OA-ITSD management do have a signed memorandum of understanding for IT services in place. However, the memorandum is not current and does not include provisions of a SLA necessary to protect the DOR and ensure alignment of business requirements for all critical IT services.

Review and update of agreement

The memorandum of understanding between the DOR and OA-ITSD has not been updated since it was signed in 2006. We found one of the Information Technology Services Division (ITSD) contacts listed in the memorandum is no longer employed by the state. Given the speed of technological innovation, failure to regularly review and update the IT service agreement leaves both organizations at risk of relying on an outdated agreement and expectations to perform the DOR's critical business tasks.

The memorandum of understanding documents financial issues related to the transfer of IT services from the DOR to the OA-ITSD, which was completed in 2007. The memorandum also specifies that limited administrative support responsibilities will continue after the transfer. Operational responsibilities, which are necessary for each organization to understand expectations, are not included in the memorandum. In addition, the memorandum does not include any qualitative or quantitative measures of services to be provided to the DOR by ITSD, does not stipulate who is responsible for funding or maintenance of customized third-party software,

does not state what level of service is expected by the DOR, and does not assign responsibility for backup, disaster recovery, and continuity planning. As a result, the DOR is at risk of not receiving the services necessary to achieve the department's mission.

Responsibility for security

DOR management, as owner of DOR information systems and data, is responsible for ensuring data maintained in the systems is secure and adequately protected. Although the DOR has partnered with the ITSD to provide IT services, the DOR has not ensured the ITSD is providing adequate security to protect DOR information.

For instance, DOR staff do not have access to system security logs and rely on ITSD staff to monitor the logs. According to ITSD officials, audit trail records for Taxation Division systems are available. An OA-ITSD official said the logs are not reviewed regularly, and only limited monitoring of the audit trail records is performed to identify reports of incidents compromising security or data integrity. ITSD officials said resources are not available to regularly monitor security activity or events. Since the memorandum does not delineate responsibility for monitoring the logs, DOR management does not have assurance this critical security function is performed.

Audit trail records should be reviewed for inappropriate or unusual activity, suspicious activity should be investigated, and appropriate actions should be taken, according to accepted standards. Failure to document responsibility for security functions could leave both the DOR and the ITSD at risk of a security incident compromising established controls, including disclosure or use of confidential data, without detection.

Agreement measurements

The memorandum of understanding does not include expected service level performance criteria or measurements to ensure the ITSD is providing IT services based on DOR business requirements.

ITSD staff prepare a report each quarter documenting the status of certain service level measurements. This report categorizes ITSD actions as promoting two outcomes: efficiently manage IT resources and maintain availability of IT resources. For each outcome, the report states several performance measures used to determine if the ITSD is meeting the desired outcomes. However, there is no documentation establishing the stated outcomes and measures and how the stated outcomes relate to the mission of the DOR, or indicating if DOR management agreed to the stated outcomes and measures. Further, for those measurements the ITSD did not meet, no corrective action plan was provided to address the failure and bring the ITSD into compliance with expected performance goals.

By not documenting the level of service expected from the ITSD or any corrective actions required to meet performance criteria, DOR management does not have reasonable assurance the department is receiving the level of service expected in return for the budgetary authority transferred to the OA-ITSD.

1.2 Disaster recovery contract

The OA-ITSD did not have a contract in place for disaster recovery facilities for some critical mainframe resources, including certain critical Taxation Division systems, during fiscal year 2011. The OA-ITSD elected to request bids for a new contract as a cost saving measure instead of exercising the renewal clause when the contract expired in June 2010. After almost a full year and two rounds of bidding and negotiations with vendors, OA-ITSD management determined the bids were still too expensive and elected to not award a new contract. Instead, OA-ITSD management decided to acquire the technological resources to establish a state owned disaster recovery capacity. The new recovery capacity become operational in July 2011. As a result, for the period July 2010 through June 2011, a contract for use of a disaster recovery facility was not in place, leaving the state vulnerable in the event of a major disaster.

The memorandum of understanding does not require the OA-ITSD to ensure appropriate disaster recovery facilities are available. Without a provision for disaster recovery facilities, the DOR faces a significant risk that critical IT systems will not be restored to operational status in the event of a disaster, subjecting the DOR to severe operational difficulties.

1.3 Maximum tolerable downtime

DOR management has not formally documented and communicated to ITSD management a maximum tolerable downtime expectation for Taxation Division systems. According to accepted standards, the maximum tolerable downtime is the maximum period of time an entity is able to tolerate a critical system being unavailable for use before the entity suffers significant losses. This time should be calculated by entity management based on an analysis of business functions. IT system management should be informed of the expectation to ensure the systems can be restored within the established limits.

Although DOR management has not established a maximum tolerable downtime, the department's continuity of operations plan acknowledges a risk that several critical functions could be difficult to restore in a 12 hour period. ITSD documentation of the 2009 disaster recovery test indicates restoring the operating system, before any applications could be restored, would take a full day, after traveling to the alternate location. Without documenting a maximum tolerable downtime and ensuring applications and systems can be restored within this time, the DOR faces an increased risk that critical functions may not be restored within a reasonable amount of time after a disaster.

1.4 Recovery testing

The memorandum of understanding between the DOR and OA-ITSD does not sufficiently address each organization's responsibility for ensuring DOR data can be recovered in the event of a disaster. DOR management has no assurance critical data and applications are backed up appropriately and can be recovered in the event of a disaster because the ITSD has not tested the restoration procedures for certain systems. An ITSD official said DOR staff are responsible for ensuring all necessary data is backed up while ITSD staff are responsible for performing the backups. In addition, the completeness of some backups is not tested because of the limited amount of time for recovery testing available under the previous disaster recovery contract. ITSD officials said recovery testing may also be performed on state equipment dedicated for testing purposes, but certain critical systems cannot be recovered in this location due to a lack of available space.

Without performing complete data recovery testing, DOR management cannot ensure backups are complete and accurate and contain all data necessary to recover critical systems in the event of a disaster.

Recommendations

The DOR, in conjunction with the OA-ITSD:

1.1 Establish a service level agreement for the provision of IT services, which identifies measurements and performance criteria to ensure service requirements are met. The agreement should be regularly monitored to ensure specified service level performance criteria remain relevant.

1.2 Ensure the service level agreement addresses the availability of disaster recovery facilities providing the capacity for the DOR to restore critical computing systems in the event of a disaster.

1.3 Formally document the methodology and determination of maximum tolerable downtimes for critical systems in the event of a disaster.

1.4 Perform a test of the data recovery procedures for all critical systems to ensure the systems can be recovered in the event of a disaster.

Auditee's Response

1.1 The department agrees with this recommendation and has begun developing a Service Level Agreement (SLA) that will include performance expectations to ensure service requirements are met. The department expects to complete the SLA by December 31, 2011.

1.2 The department agrees with this recommendation and will include the availability of disaster recovery facilities in the SLA.

1.3 The department agrees with this recommendation and will include tolerable downtimes for critical systems in the SLA.

1.4 The department agrees with this recommendation and will include testing of data recovery in the SLA.

2. User Account Management

DOR and ITSD management had not established or documented adequate user account management policies and procedures. User account management includes requesting, establishing, issuing, suspending, modifying, closing, and periodically reviewing user accounts and related user privileges, according to accepted standards. User account management policies and procedures should be established for all user accounts, including system administrators and other privileged users.

2.1 Database administrator access

ITSD database administrator access to databases supporting Taxation Division systems is not monitored by management. As a result, certain database administrators can add, edit, or delete data directly in the databases without the changes being reviewed by management or being subject to system processing edits. System data is periodically scanned to detect invalid or corrupt data, according to an ITSD official. However, these scans will not detect unauthorized data entered directly into the database.

According to accepted standards, logging and monitoring functions are critical to enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed. An ITSD official said database monitoring is performed on a statewide basis by the state Information Security Management Office (ISMO). However, the ISMO Chief Information Security Officer said monitoring of internal system activity is only performed as requested and most monitoring efforts are directed at external threats.

Failure to monitor the actions of database administrators results in an increased risk of unauthorized changes to tax data without being detected. In addition, direct database changes are not subject to system validation and edit checks, potentially allowing the recording of inaccurate data in the databases.

2.2 Management review of user accounts

DOR and ITSD management have not implemented procedures for periodically reviewing user access rights to the network or to Taxation Division systems and data to ensure access rights remain appropriate. The DOR security policies require division directors to review reports of user access to information systems at least semi-annually. However, this review is not performed, according to a DOR official. According to the Missouri Adaptive Enterprise Architecture (MAEA), agencies must periodically review user accounts. Accepted standards also support regular review of all accounts and related privileges.

During our review of user accounts with access to DOR systems, we found 24 former employees still had active user accounts. One of these former employees had left the DOR in 2001. In addition, we found nine accounts that were active in the system, but had not been assigned to specific users. We also found 807 active user accounts that had not been accessed in over 90 days.

Without a review of user access rights, management faces an increased risk that unauthorized alterations of these rights will go undetected or access rights may not be aligned with current job duties.

2.3 Revoked accounts

The ITSD has a pool of approximately 2,700 revoked user accounts for DOR systems that are not assigned to specific users. This pool of user accounts includes new accounts created for the convenience of having pre-established user accounts assigned with basic access rights and accounts of former users available for re-assignment to new users.

Accepted standards require unique user accounts be assigned to individual users. All user accounts created should have an associated request and approval from appropriate administrators of information resources. According to the MAEA, agencies must periodically review user accounts, including identification of inactive, idle, or orphaned accounts.

By allowing unassigned accounts to exist in the information system, management may increase the risk of unauthorized access and compromise the confidentiality and integrity of data maintained by the DOR.

Similar conditions previously reported

Maintaining a pool of user accounts was addressed in our 2003 audit of the DOR Security,[4] and again in a follow-up audit in 2006.[5] In both cases, DOR and/or ITSD management said corrective action would be taken. The number of unused accounts currently outstanding is greater than at the time of either of our prior reports, indicating DOR and ITSD management have not made a dedicated effort to correct the situation by implementing our prior recommendation.

2.4 Temporary employee accounts

Although DOR management has a policy for granting computer access to permanent employees, management has not established a policy for granting access to temporary employees. According to DOR personnel, the procedure for granting access to temporary employees is not the same process as

[4] SAO Audit Report 2003-16, *Department of Revenue - Information Resource Security Management*, issued in February 2003.
[5] SAO Audit Report 2006-14, *Information Technology - Information Security Management in State Agencies*, issued in March 2006.

granting access to permanent employees. In March 2011, the DOR employed approximately 100 temporary employees during tax season to input and process tax returns. Without documented policies or procedures, DOR management does not have assurance user accounts assigned to temporary employees are consistently or correctly controlled, which increases the risk of unauthorized access to data and information maintained in Taxation Division systems.

Recommendations

The DOR, in conjunction with the ITSD:

2.1 Regularly monitor database administrator access to ensure data is not changed without authorization.

2.2 Perform periodic reviews of user access rights to ensure access rights are commensurate with job duties and responsibilities.

2.3 Discontinue the practice of maintaining a pool of user accounts not associated with active system users.

2.4 Establish policy and procedures for granting system access to temporary employees.

Auditee's Response

2.1 OA-ITSD agrees with this recommendation and will develop procedures to regularly audit database administrator activity. OA-ITSD expects this process will be in place by December 31, 2011.

2.2 The department has requested a list of all users with access to department systems. ITSD will provide the department with this information by system. A list of priority systems to review user access has been submitted to ITSD.

2.3 OA-ITSD agrees with this finding. OA-ITSD will disable all inactive pool of user accounts and remove authorization to all production systems. OA-ITSD will provide the department a list of all user accounts to ensure all inactive accounts are disabled. OA-ITSD expects this process will be in place by December 31, 2011.

2.4 The department agrees with this recommendation and will add specific language to address granting system access to temporary employees to the current policy.

3. Risk Assessment Program

DOR management has not established a comprehensive risk assessment and management program. DOR officials perform an audit risk assessment when creating the internal audit plan each year; however, this assessment is not a substitute for an overall business risk assessment.

A risk assessment helps identify potential threats, vulnerabilities, and weaknesses which could be exploited and determines what controls are required and what level of resources should be expended on controls to prevent losses. According to accepted standards, an effective risk management process is an important component of a successful IT security program. The principal goal of an organization's risk management process should be to protect the organization and its ability to achieve the mission, not just protect IT assets, making risk management an essential management function of the organization.

Without an established risk management and assessment framework in place, unidentified risks or threats may expose an unknown system vulnerability; resulting in lost information, lost privacy, loss of availability, or loss of system integrity. In addition, DOR management has less assurance that established security controls are cost-effectively addressing programmatic risks.

Recommendation

The DOR, in conjunction with the ITSD, should implement and document a business risk assessment and management framework, which includes policies, standards, and procedures for performing periodic risk assessments so management can better protect department resources and the ability to cost-effectively address risk and accomplish the DOR's mission.

Auditee's Response

The department agrees with this recommendation and will develop policies and perform periodic risk assessments.

4. Browsing of Taxpayer Records

DOR management has established policies to comply with the federal Taxpayer Browsing Protection Act of 1997[6] and with state law; however, additional controls could be implemented to further secure the privacy of taxpayer data.

The Taxpayer Browsing Protection Act states tax returns and return information shall be confidential. Specifically, the Act requires states receiving federal return information restrict access to the information to only those persons whose duties or responsibilities require access. Additionally, under state law,[7] any person with access to taxpayer data may not disclose the data or information, with certain exceptions. Although there is no provision of state law limiting access, DOR policy prohibits users from accessing tax return information not necessary to carry out official duties.

[6] 26 USC Sections 7213, 7213A, and 7431
[7] Section 32.057, RSMo

DOR management uses certain security controls to limit access to tax systems, but has not established procedures to monitor employee access to ensure only appropriate access is occurring. The DOR Internal Audit Bureau has planned a review of employee access to taxpayer accounts; however, this is the first audit of this type.

Recommendation

The DOR should continue current efforts to further strengthen procedures and determine if additional opportunities exist, such as monitoring employee access to certain tax return information, to improve security and ensure the confidentiality of taxpayer information.

Auditee's Response

The department agrees with this recommendation and the Compliance and Investigations Bureau will work with ITSD to identify verification opportunities.