Office of Missouri State Auditor

Nicole Galloway, CPA

Office of State Courts Administrator System of Case and Record Management of the Judiciary

Report No. 2016-055

August 2016

auditor.mo.gov

August 2016

Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Findings in the audit of the System of Case and Record Management of the Judiciary

Background

The Missouri Court Automation Committee (MCA), in conjunction with the Missouri Office of State Courts Administrator (OSCA) is responsible for development and implementation of the case and record management system (CRMS) of the judiciary. The OSCA is responsible for providing technical support to Missouri courts and relies extensively on information systems to support mission-related operations and on information security controls to protect the confidentiality, integrity, and availability of sensitive judicial information maintained in those systems. The judiciary relies extensively on the CRMS, including the Judicial Information System (JIS), to process and store court cases, financial information, and other data. The JIS stores personally identifiable information, court cases, financial information, and other data. As of December 2015, the JIS was used by 45 circuits, 3 appellate courts, the Supreme Court, 71 municipal courts, and the centralized Fine Collection Center.

User Account Management

OSCA management has not fully established and documented user account management policies and procedures. OSCA management has not fully established procedures for periodic reviews of user accounts and related privileges to confirm access rights are appropriate. User accounts are not routinely reviewed to determine whether accounts have not been accessed or used for a specified period of time. Additionally, 12 former OSCA or court employees still had access to the JIS after their employment ended. OSCA management also does not require supervisory reviews of system logged actions performed by privileged users or other users with significant access to the network or the CRMS.

Information Security Program

OSCA management has not fully implemented certain elements of an information security program on which security plans, policies, procedures, and controls can be formulated, implemented, and monitored. Weaknesses exist in the information security program that threaten the confidentiality, integrity, and availability of OSCA information and systems. Officials have not established a comprehensive risk assessment and management program or consistently ensured all users are uniquely identified and passwords kept confidential and changed regularly. They also have not established policies to monitor, review, and investigate audit trail records for security and audit related events. Additionally, OSCA management has not fully established an incident response plan for computer security incidents.

System Planning

OSCA management has not fully established some project cost management policies and procedures necessary to minimize project risk. OSCA management has not fully documented the system development life cycle (SDLC) methodology or the policies and procedures for guiding the software development and modification process, including change control management for the system. SDLC is the overall process of developing, implementing, and retiring information systems through a multistep process from initiation, analysis, design, implementation, and maintenance to disposal, according to accepted standards. OSCA management did not prepare project budgets or estimates of project costs for the development, implementation, updating, and maintenance of all system changes required for the CRMS. In addition, OSCA management has not properly accounted for some project costs. OSCA management has not developed a formal long-range plan or prepared adequate estimates of the additional costs expected for the CRMS. A major funding source for the CRMS is the court automation fee established in section 488.027, RSMo. However, this fee will sunset September 1, 2023. A formal long-range plan is necessary to ensure the General Assembly is aware of the state's total potential financial commitment prior to funding new features of the CRMS.

Contingency Planning

OSCA management has documented and informally adopted a business continuity plan; however, the plan has not been formally approved by management, updated, or tested, increasing the risk the plan may not be adequate to support the timely recovery of business functions after the occurrence of a disaster or other significant incident. OSCA management has developed certain contingency plans and implemented basic controls for recovery planning. However, the disaster recovery plan has not been fully established or fully tested to ascertain the effectiveness of recovery procedures. The disaster recovery plan was last updated in May 2014.

Monitoring Reports

Opportunities exist to increase the efficiency and effectiveness of the monitoring performed of activity processed in the CRMS at the local courts. These opportunities to assist the courts could be accomplished through additional monitoring reports or other tools. Examples of the reports not currently available to courts include a report to identify cases disposed with no fees or costs assessed or a report to identify cases exempt from debt collections.

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

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

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

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

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

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

All reports are available on our Web site: auditor.mo.gov

Office of State Courts Administrator
System of Case and Record Management of the Judiciary
Table of Contents

NICOLE GALLOWAY, CPA
Missouri State Auditor

Honorable Jeremiah W. (Jay) Nixon, Governor
and
Honorable Patricia Breckenridge, Chief Justice, Supreme Court of Missouri
and
Kathy S. Lloyd, State Courts Administrator
and
Honorable Gary W. Lynch, Chair, Missouri Court Automation Committee
Jefferson City, Missouri

We have audited the Office of State Courts Administrator, System of Case and Record Management of the Judiciary, in fulfillment of our duties under Chapter 29, RSMo. This audit was conducted to evaluate the effectiveness of the data governance approach, including security and privacy controls designed to secure confidential data and as a result of increasing concerns regarding security of information maintained in state databases. The objectives of our audit were to:

1. Evaluate internal controls over significant management and financial functions.

2. Evaluate compliance with certain legal provisions.

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

4. Evaluate the security and privacy controls designed to ensure the confidentiality, integrity, and availability of data and information processed and maintained by the applicable systems.

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

For the areas audited, we identified (1) deficiencies in internal controls, (2) no noncompliance with legal provisions, (3) the need for improvement in management practices and information system control activities, and (4) the need to fully implement an information security program and related security controls. The accompanying Management Advisory Report presents our findings arising from our audit of the Office of State Courts Administrator, System of Case and Record Management of the Judiciary.

Nicole R. Galloway

Nicole R. Galloway, CPA
State Auditor

The following auditors participated in the preparation of this report:

Deputy State Auditor:	Keriann Wright, MBA, CPA
Director of Audits:	Douglas J. Porting, CPA, CFE
Audit Manager:	Lori Melton, M.Acct., CPA
In-Charge Auditor:	Amanda Locke, M.Acct.
Audit Staff:	Jill Wilson, MBA Hussein A. Arwe

Background

The Missouri Court Automation Committee (MCA), in conjunction with the Missouri Office of State Courts Administrator (OSCA) is responsible for development and implementation of the case and record management system (CRMS) of the judiciary. The OSCA is responsible for providing technical support to Missouri courts. The duties and responsibilities assigned to the state courts administrator are broad in scope and relate to all levels of the state court system. The OSCA relies extensively on information systems to support mission-related operations and on information security controls to protect the confidentiality, integrity, and availability of sensitive judicial information maintained in those systems.

Information security is a critical consideration for any organization dependent on information systems and networks to meet its mission or business objectives. Information security is especially important for state agencies, where public trust is essential for the efficient delivery of services. 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.

Since 1994, OSCA has worked on the Statewide Court Automation program, which is a multi-year plan to automate all courts in the state. Section 476.055, RSMo, established the Statewide Court Automation program, as well as an oversight body for the program, the MCA. The MCA has decision-making authority for all aspects of court automation. In addition, state law[1] established a $7 per-case court fee to be used for statewide court automation. The MCA administers the monies collected from this fee. The OSCA spent approximately $218 million on the court automation program for the period of July 1, 1994, through June 30, 2015.

The MCA, in conjunction with the OSCA, is primarily responsible for development, implementation, and oversight of the policies and procedures for security and control of agency information systems and technology resources and is the custodian of the CRMS. OSCA staff and personnel at courts are responsible for performing duties required by applicable security policies, procedures, or contracts. The court appointing authority in each court (usually the circuit clerk or presiding judge) is the resource owner of all data and information within the individual court.

[1] Sections 476.055, 488.012, and 488.027, RSMo

System of Case and Record Management of the Judiciary

The judiciary relies extensively on the CRMS, including the Judicial Information System (JIS), to process and store court cases, financial information, and other data.

In 1997 the state awarded a contract for a case management system, later known as the JIS. The JIS was primarily developed, implemented, and maintained by a contractor; however, in fiscal year 2014, the OSCA became primarily responsible for maintaining the JIS. The JIS stores personally identifiable information[2] (PII), court cases, financial information, and other data. As of December 2015, the JIS was used by 45 circuits (comprised of 114 counties and the City of St. Louis), 3 appellate courts, the Supreme Court, 71 municipal courts, and the centralized Fine Collection Center[3] (FCC). Each circuit, the three appellate courts, the Supreme Court, and the FCC have a separate JIS application and database to process and store case data.

In addition to the JIS, the CRMS also includes other functionalities and systems, including, but not limited to, the following:

- Case.net: an online system that allows users to view case records including charges, parties, attorneys, docket entries, and judgments. This information is derived from the JIS.
- Pay By Web (PBW): an online system that allows any public user to pay balances owed on disposed cases via Case.net. The payment information is sent to the JIS.
- eFiling: an online system that allows registered users to file cases and documents electronically. The eFiling system also accepts payment for the case filed. The cases filed and related payments are sent to the JIS.

Security and access controls

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

[2] According to accepted standards, PII is information that can be used to distinguish or trace an individual's identity such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

[3] Section 476.385, RSMo, authorized a centralized bureau to collect, with any plea of guilty, fines and all court costs for traffic and other related offenses for counties that participate in the program. The OSCA contracted development of a system to manage these monies and this contractor is responsible for the management of these duties.

information. Effective privacy controls depend on the safeguards employed within the information system that is processing, storing, and transmitting PII and the environment in which the system operates. Organizations cannot have effective privacy without a basic foundation of information security. Without proper safeguards and controls, information systems and confidential data are vulnerable to individuals with malicious intentions who can use access to obtain sensitive data or disrupt operations.

In the 2015 High-Risk Series[4] update, the Government Accountability Office (GAO) expanded the scope of the information security high-risk area to include protecting the privacy of PII. The GAO expanded this risk area due to the challenges of ensuring the privacy of PII created by advances in technology. Technology advances, such as lower data storage costs and increasing interconnectivity, have allowed both government and private sector agencies to collect and process extensive amounts of PII more effectively. Risks to PII can originate from unintentional and intentional threats. These risks include insider threats from careless, disgruntled, or improperly trained employees and contractors; the ease of obtaining and using hacking tools; and the emergence of more destructive attacks and data thefts.

Technology advances, combined with the increasing sophistication of individuals or groups with malicious intent, have increased the risk of PII being compromised and exposed. Correspondingly, the number of reported security incidents involving PII in both the private and public sectors has increased dramatically in recent years. At the same time, government agencies are increasingly reliant on technology and information sharing to interact with citizens and to deliver essential services. As a result, the need to protect information, including PII, against cybersecurity attacks is increasingly important.

OSCA management is responsible for ensuring the confidentiality and privacy of the data and information collected, maintained, used, or transmitted from the CRMS by implementing MCA approved security and access controls. Security of case and record management is especially important when such information can be directly linked to an individual. Confidentiality is threatened not only by the risk of improper access to electronically stored information, but also by the risk of interception during electronic transmission of the information.

The JIS is a private network information system that can be accessed by authorized users. Access to the JIS is controlled using various resources, including networks, a security system, and/or remote access mechanisms.

[4] Report GAO-15-290, *Report to Congressional Committees, High-Risk Series An Update,* February 2015, <http://www.gao.gov/assets/670/668415.pdf>, accessed July 28, 2016.

Users must have access to and logon to the network before they can access the JIS. The JIS security system controls the level of access a user is granted, including the actions a user can perform. Court users and their access levels are authorized by a local court official, which is usually the circuit clerk or presiding judge or their designee. In addition, the JIS assigns a security level to each court case type ranging from data made available to the public to court sealed information. The OSCA also uses internal databases to store user account information and to track user access to the JIS.

Scope and Methodology

The scope of our audit included information security and other relevant internal controls; policies and procedures; and other management functions and compliance issues in place during the 2 years ended June 30, 2015.

Our methodology included reviewing written policies and procedures, reviewing financial records, and interviewing various OSCA and court personnel. We obtained an understanding of the data governance approach and applicable controls that are significant within the context of the audit objectives and assessed whether such controls have been properly designed and placed in operation. We tested certain of those controls to obtain evidence regarding the effectiveness of their design and operation. We also obtained an understanding of legal provisions that are significant within the context of the audit objectives, and we assessed the risk that illegal acts, including fraud, and violations of contract or other legal provisions could occur. Based on that risk assessment, we designed and performed procedures to provide reasonable assurance of detecting instances of noncompliance significant to those provisions.

We obtained a listing of the JIS user accounts as well as user access requests for current users as of May 2015 from the OSCA officials. After our inquiries, the OSCA determined this information was inaccurate. We were subsequently provided revised records as of August 2015. As discussed in MAR finding number 1.1, we could not confirm the completeness of the data.

We obtained the employment records of all OSCA employees and court employees paid by the state for fiscal years 2001 to 2015 from the statewide accounting system for human resources. We matched these records to the JIS and internal database of user account records for current users to determine if any terminated employees had active accounts. Since the OSCA does not maintain social security numbers for user accounts, we relied on a name match. In addition, since an employee may be terminated from state employment but still work for and be paid by the local jurisdiction, we contacted the OSCA or the local jurisdiction for some of the matches to determine whether the individuals still worked at the local jurisdiction or were terminated and if access was necessary. This test was limited to individuals paid by the state and did not include terminated individuals paid by other funding sources. 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 access to a JIS test environment to evaluate the data integrity controls that validate and edit data entered in the system. We attempted to enter data containing errors and performed incorrect transactions to verify the JIS would reject and not accept the data or transactions. Based on this assessment, we determined these specific data integrity controls worked properly.

To assess the reliability of other data and information we analyzed, such as system control settings, authorization documents, and security policies and procedures, we corroborated the information with the OSCA officials and security administrators to determine whether the data obtained were consistent with system configurations and controls in place at the time of our review. Based on this assessment, we determined the data and information were reliable for the purposes of this report.

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

- OSCA security policy
- Court Operating Rules
- Office of Administration - Information Technology Services Division (ITSD)
- National Institute of Standards and Technology (NIST)
- Government Accountability Office (GAO)
- ISACA (previously known as the Information Systems Audit and Control Association)

1. User Account Management

OSCA management has not fully established and documented user account management policies and procedures. In addition, policies and procedures for the management of privileged user accounts or users with significant access[5] have not been fully established. 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.

1.1 Periodic review of user accounts

OSCA management has not fully established procedures for administering and reviewing user access to data and other information resources on the network or the CRMS to ensure access rights are commensurate with job responsibilities and remain appropriate.

Accepted standards support regular review of all accounts and related privileges. At a minimum this review should include levels of authorized access for each user, whether all accounts are still active, and whether management authorizations are up to date, according to accepted standards. Without a review of user access rights, there is an increased risk that unauthorized alterations of these rights would go undetected or that access rights would not be aligned with current job duties.

Review of accounts to determine inappropriate access

OSCA management has not fully established procedures for periodic reviews of accounts and related privileges.

OSCA management has not periodically provided a list of user accounts with access to the network or the CRMS to appropriate OSCA or local court appointing authority personnel for review. Without providing a complete list of all accounts, management cannot review or confirm user access rights are appropriate.

An OSCA official said the OSCA currently relies on the reviews performed at each local court prior to the implementation of the eFiling system to determine whether access appears appropriate. However, not all courts have been reviewed and a follow-up schedule has not been established. An OSCA official said a review was performed in March 2015 (after our audit began) to determine whether OSCA users' access appeared appropriate. OSCA management could provide no documentation of such a review prior to this for the 2 years ended June 30, 2015.

[5] Privileged users are individuals who have access to system control, monitoring, or administrative functions (such as a system administrator). Users with significant access have the ability to perform most functions within the network or the system of case and record management or other supporting systems.

A similar condition was noted in our prior audit report. Requiring a review of all accounts ensures the right type and level of access has been provided. Otherwise, user accounts and accesses can be granted to or maintained for users who should not have access, according to accepted standards.

Inactive user accounts

OSCA management has not routinely reviewed user accounts to identify user accounts that have not been accessed or used for a specified period of time, for either the network or the JIS.

This weakness occurred, in part, because the JIS does not have the functionality to record the last date a user accessed the JIS. OSCA officials said the agency instead relies on password controls to help prevent inappropriate users from accessing the JIS. In addition, the OSCA relies on local courts who are responsible for notifying the OSCA if a user no longer needs access.

The last date a user accessed the network on which the JIS is housed is available through the user's network user account. An OSCA official said periodic reviews of network user accounts are performed to identify accounts that have not accessed the network for a specified period of time. An OSCA official said OSCA personnel conducted a review in July 2014; however, sufficient documentation was not maintained to substantiate this review.

Without appropriate security control functionality, OSCA management is unable to identify user accounts that have not been accessed or used for a specified period of time. Inactive accounts indicate users no longer need the access privileges provided by the accounts and may be attractive targets for individuals attempting to gain unauthorized access since the account owners may not notice illicit activity on the accounts, according to the Government Accountability Office (GAO).

Tracking user account information

OSCA management has not ensured internal databases that maintain user account information are periodically reconciled to the JIS user accounts. An internal database is used to store and track information about user accounts, including access requests, and is an important component for maintaining security. This database is necessary because the JIS does not track identifying information of the user associated with each account. This database does not interface with the JIS and must be manually updated by OSCA or court personnel. An OSCA official said reconciliations between the internal database and the JIS are performed. However, we found the internal database had data integrity issues, which jeopardized the reliability for managing user accounts. For example, we identified 55 user accounts in the JIS without a corresponding record in the internal database. Upon our inquiry, the OSCA identified 9 of the 55 user accounts should not have access due to either the users no longer being employed or the access being inappropriate. In addition, the internal database had user access requests for user accounts where a name of the user was either invalid or missing.

Without performing periodic reconciliations, there is an increased risk of data integrity issues between information sources and an increased risk of inappropriate access to system resources.

1.2 Termination of user accounts

As of August 2015, 12 former OSCA or court employees still had access to the JIS. These former employees left employment from 2012 to June 2015. OSCA management has not established policies and procedures to perform periodic reviews to identify terminated or transferred users. OSCA policies and procedures require supervisors to ensure user access is removed as soon as it is no longer needed by notifying OSCA of employees that have left employment. OSCA staff are then responsible for disabling or removing the user account. However, controls were not effective or applied consistently, resulting in the former employees who still had access to the JIS.

Without removing terminated employees' user access to OSCA information resources, management may increase the risk of unauthorized access and compromise the confidentiality and integrity of data maintained by the agency.

1.3 Privileged user supervision

OSCA management does not require supervisory reviews of system logged actions performed by privileged users or other users with significant access to the network or the CRMS.

We identified instances where duties were not properly segregated and additional supervisory reviews were not performed. For example, certain computer operations personnel with privileged access to the JIS for system support also have access to add system users.

Privileged users have extensive access rights necessary to keep systems running efficiently. Sometimes these job duties are difficult to segregate due to staffing or other issues. Even when proper segregation has been established, the actions of privileged users warrant supervision due to the extensive rights these users are provided. However, OSCA management did not provide supervisory oversight or establish other mitigating controls to ensure these privileged users performed only authorized functions. Changes made by privileged users or users with significant access to the JIS are logged, but an OSCA official said the logs are not reviewed regularly.

A similar condition was noted in our prior audit report. An OSCA official said the OSCA does not have sufficient resources to perform supervisory reviews of actions performed by these users.

Routinely monitoring actions performed by privileged users or other users with significant access can help identify significant problems and deter employees from inappropriate activities. Without effective monitoring, an increased risk exists that these individuals could perform unauthorized system activities without being detected.

1.4 Access roles and functionality

OSCA management has not designed the JIS functionality for user account access to ensure incompatible functions are appropriately segregated.

We found certain accounting access roles allowed users to perform incompatible functions. For example, one access role allows user accounts the ability to perform most accounting functions, such as the ability to assess costs to a case, receipt payments, prepare deposits, create disbursements, and void transactions.

Inadequately segregated duties increase the risk that erroneous or fraudulent transactions could be processed.

Recommendations

The OSCA, in conjunction with the Missouri Court Automation (MCA) Committee:

1.1 Periodically review user access to data and other information resources to ensure access rights are commensurate with job duties and responsibilities, identify and evaluate inactive accounts, and reconcile user account information maintained in internal databases to account information from the network or the JIS. In addition, ensure lists of user accounts and related privileges with access to the JIS are complete and accurate and periodically provide applicable user information to the local court appointing authorities for review.

1.2 Implement procedures to ensure user accounts and related access privileges are removed timely upon employee termination.

1.3 Perform periodic supervisory reviews of certain actions performed by privileged users and users with significant access.

1.4 Perform a comprehensive review of the JIS user access roles to ensure incompatible functions are identified and properly segregated.

Auditee's Response

1.1 The responsibility to review local court user accounts is with the local appointing authority. This topic will be presented to the Missouri Court Automation (MCA) Committee to consider a security guideline to address this recommendation.

1.2 In conjunction with the MCA, procedures will be reviewed in an effort to improve timely removal of terminated user accounts.

1.3 Review of the work of privileged users is a best practice. OSCA is currently evaluating auditing software for the case management system. This recommendation will be presented to the MCA for consideration.

1.4 It is the responsibility of the local appointing authority to assign access roles to staff, selecting from user roles as provided within JIS.

Auditor's Comment

1.4 OSCA management defined the access roles from which the local appointing authorities choose to assign access rights. Certain of these defined roles are broad and allow users to perform incompatible functions. OSCA management should consider more narrowly defining the access roles so they are not inherently in conflict.

2. Information Security Program

Opportunities exist to strengthen the information security program and to improve the protection of information system resources.

OSCA management has not fully implemented certain elements of an information security program on which security plans, policies, procedures, and controls can be formulated, implemented, and monitored. Weaknesses exist in the information security program that threaten the confidentiality, integrity, and availability of OSCA information and systems.

An information security program provides a framework for managing risks, developing security policies, assigning responsibilities, and monitoring the adequacy of an agency's security controls. An information security program is the foundation of an agency's security control structure and a reflection of management's commitment to addressing security risks. Implementing a security program is essential to ensuring controls over information and information systems work effectively on a continuing basis, according to the GAO.

OSCA management has not fully established and/or documented policies and procedures for the following elements of an information security program:

- Risk assessment
- Password policies
- Transactional password policies
- Security activity monitoring
- Incident response plan

- Review of security settings

According to accepted standards, policies are necessary to set organizational strategic directions for security and assign resources for implementation of security. A key element of an effective information security program is to develop, document, and implement risk-based policies and procedures that govern the security over an agency's computing environment, according to the GAO.

2.1 Risk assessment

OSCA management has not established a comprehensive risk assessment and management program.

Accepted standards state organizations should develop, document, and implement an information security program that includes periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems. A risk assessment is necessary to identify potential threats, identify vulnerabilities in systems, determine the likelihood that a particular threat may exploit vulnerabilities, and assess the resulting impact on the organization's mission, including the effect on sensitive and critical systems and data, according to accepted standards. Risk assessments should include essential elements such as discussion of threats, vulnerabilities, impact, risk model, and likelihood of occurrence, and be updated based on a frequency defined by 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, OSCA management has less assurance that established security controls are cost-effectively addressing programmatic risks.

2.2 Password policies

OSCA management has not consistently ensured all JIS users are uniquely identified and JIS passwords are not shared and changed regularly. We identified the following risks and noncompliance with applicable policies:

- The JIS does not have the capability to require passwords that meet accepted standards. For example, there is not a minimum password length or complexity requirement. Instead, the security administrator assigns passwords to ensure the password meets OSCA policy.

- Users are not required to change their password on a periodic basis or after a user account has been reset by a security administrator. The JIS has the ability to allow users to change their passwords; however, OSCA management disabled this capability because the JIS could not require users to create passwords that met OSCA policy or accepted standards.

- OSCA password management controls are not sufficient to prevent unauthorized access to the JIS data since employees with security administrator duties and/or employees with system administration duties[6] have access to each user's JIS password. Security administrators enter passwords in the security management database containing information on users and their access rights. The passwords have been encrypted and stored in a file that all security administrators can access. The security of a password system is dependent upon keeping passwords secret. Allowing users access to a centralized list of passwords threatens the confidentiality and integrity of the data and information. In addition, system administrators have access to the passwords for the JIS user accounts they establish and the JIS does not have the capability to require passwords be changed upon the first logon session. Because these individuals have access to the passwords, they could use this information to masquerade as another user to gain unauthorized access to court case data.

- User accounts and passwords are shared. As noted above, the user account and password used to administer user accounts is shared by OSCA employees with security administration duties and the password is not periodically changed. In addition, the user accounts and passwords for privileged system-level accounts are shared among OSCA employees with system administrator duties and the passwords are not periodically changed.

- The JIS does not have the capability to retain previous passwords to prevent re-use.

Similar conditions were noted in our prior audit report. The OSCA Security Guidelines policy contains provisions for protecting user identifications and passwords. Policy requires users be uniquely identified and responsible for protecting login information, including passwords, from others. In addition, the OSCA policy requires passwords to be changed at least every 90 days. Without strong password controls, the likelihood that accounts could be compromised and used by unauthorized individuals to gain access to sensitive information is increased, according to the GAO. By allowing users to share accounts and passwords, individual accountability for system activity could be lost and unauthorized system activity could occur.

[6] Security administrators are the individuals who set up and modify who has access to the system, according to accepted standards. System administrators are the managers and technicians who design and operate computer systems.

2.3 Transactional password policies

OSCA management has not ensured the JIS is designed effectively to ensure passwords are not shared. The JIS uses passwords to control who has the ability to perform certain functions, to help ensure incompatible functions are appropriately segregated. Specifically, the JIS has a password to control the ability to adjust fees and void a receipt and a separate password to void checks and payables. However, the passwords used to control each of these transactions are the same for all users of a single court. An OSCA official said a circuit clerk is provided access to the passwords and the ability to change the passwords. However, our audits of courts have noted this password may be shared with other users at the court. In addition, the password is only changed when deemed necessary by the local court appointing authority. The JIS does not have the functionality to require separate passwords for different users when the transaction is voided or to require the password to be changed on a periodic basis. Without the functionality to properly control these transactions, unauthorized system activity could occur.

2.4 Security activity monitoring

OSCA management has not established policies or procedures to monitor, review, and investigate audit trail records for defined security and audit related events. Determining what, when, and by whom specific actions were taken on a system is crucial to establishing individual accountability, monitoring compliance with security policies, and investigating security violations, according to the GAO.

The systems log certain activity by maintaining a record of every transaction made. However, OSCA officials said due to the large number of transactions generated by the systems, the logs are not being maintained in a manner that is easily retrievable and there are insufficient resources to monitor the logs in the current form. As a result, the OSCA does not proactively monitor for unusual or inappropriate activity on a regular basis.

In addition, the systems are not capable of logging all pertinent information, such as user account additions, changes, or deletions; unauthorized attempts to access the system; and unauthorized attempts to view or change security definitions and rules. Policies and procedures should establish the criteria for significant system events that should be logged and independently reviewed by management, according to accepted standards.

By not maintaining these logs, the OSCA is not able to provide logs to local court appointing authorities for their review. According to OSCA officials, logs may be reviewed on a case-by-case basis, but there is no proactive review. Instead the reviews are more reactive, based upon inquiries from appointing authorities about potential instances of inappropriate use. A similar condition was noted in our prior audit report.

Audit and monitoring involve the regular collection, review, and analysis of auditable events for indications of inappropriate or unusual activity, and the appropriate investigation and reporting of such activity, according to the GAO. Further, the lack of frequent reviews of audit trail information may result in significant instances of misuse not being detected.

2.5 Incident response plan

OSCA management has not fully established an incident response plan. Incident handling and response is the process and actions an organization takes in detecting, reporting, and responding to a computer security incident, according to accepted standards. Once an incident has been identified, an agency's incident response procedures should provide the capability to correctly log the incident, properly analyze it, and take appropriate action, according to the GAO.

Examples of procedures recommended by accepted standards that have not been effectively established or documented include:

- Roles and responsibilities of those responsible for incident handling
- Prioritization of incidents, including timeframes for resolving incidents
- Collection of incident evidence
- Containment, eradication, and recovery strategies
- Lessons learned, including metrics to measure the incident response capability and its effectiveness

Without effective incident handling policies and procedures, an agency may be hampered in its ability to detect incidents, report incidents to the appropriate authorities, minimize the resultant loss and destruction, mitigate the exploited weaknesses, and restore services, according to the GAO.

2.6 Review of security settings

OSCA management has not established formal written policies to periodically review and evaluate the effectiveness of security settings for the system or the network. Although policies have not been established, an OSCA official said security settings for the JIS cannot be modified without programming changes, which would be accomplished through the change control process. According to the GAO, a key element of a security management program is ongoing testing and evaluation to ensure systems are in compliance with policies, and that policies and controls are both appropriate and effective.

Recommendations

The OSCA, in conjunction with the MCA Committee:

2.1 Establish a comprehensive risk assessment and management framework.

2.2 Investigate system changes to strengthen password controls to reduce the risk of password compromise and to help prevent unauthorized access. In addition, discontinue maintaining a centralized list of passwords.

2.3 Strengthen the transactional password controls to increase accountability.

2.4 Determine security events that should be logged and reviewed, including unusual and inappropriate activity, and monitor and review the audit trail logs to identify improper access or use of data. In addition, develop separate reports of security violations for use by local court officials.

2.5 Establish and document an incident response plan.

2.6 Develop formal policies to periodically review and test security settings.

Auditee's Response

2.1 &
2.5-2.6 This recommendation will be presented to the MCA for consideration.

2.2 The JIS is deficient in its password capacity; however, JIS is only accessible through the court's network. There are approved network password guidelines which require complex passwords which must be changed at least every 90 days and force an inactivity logout every 15 minutes. The concern with JIS password limitations was raised in a previous audit and in response this issue is being addressed in development of the new CRMS (Show-Me Courts/SMC).

2.3 There are MCA approved security policies which prohibit sharing of passwords. The deficiencies noted are JIS limitations and are being addressed in development of Show-Me Courts.

2.4 The review of audit logs is a best practice. OSCA is currently evaluating software for the case management system. This recommendation will be presented to the MCA for consideration.

3. System Planning

Opportunities exist to strengthen the planning and oversight of the CRMS.

Significant resources, both financial outlays and staff time, have been invested for the development and maintenance of the CRMS. However, OSCA management has not fully established some project cost management policies and procedures necessary to minimize project risk.

According to accepted standards, a project is a temporary process, which has a clearly defined start and end time, a knowable set of tasks, a management structure and a budget that is developed to accomplish a well-defined goal or objective. A project is considered a temporary process because once the end goal is achieved, the project is complete. For this reason, the end point of a project needs to be defined at the very beginning of the project to ensure successful completion. The reason some projects never end is because no one ever defined what constitutes a project's completion.

3.1 System development life cycle methodology

OSCA management has not fully documented the system development life cycle (SDLC) methodology or the policies and procedures for guiding the software development and modification process, including change control management for the system. SDLC is the overall process of developing, implementing, and retiring information systems through a multistep process from initiation, analysis, design, implementation, and maintenance to disposal, according to accepted standards. Change control is the process for managing and controlling changes to the configuration of an information system, according to accepted standards. Application software development and change controls help ensure that only authorized programs and authorized modifications are implemented, according to the GAO. This process is accomplished by instituting policies, procedures, and techniques that help ensure all programs and program modifications are properly authorized, tested, and approved.

Examples of procedures recommended by accepted standards that OSCA management has not effectively documented include:

- Security impact analysis procedures, including how and with what level of rigor analysis results are to be documented, and requirements for post-implementation review to confirm that the change was implemented as approved and that no additional security impact has resulted
- Requirements for testing of changes (such as a test plan, schedule, and test results)
- Requirements for access restrictions for change
- Requirements for rollback of changes in the event that problems occur

For the methodology to be properly applied, it should be sufficiently documented to provide staff with clear and consistent guidance, according to the GAO. Without proper application software development and change controls, there is a risk that security features could be inadvertently or deliberately omitted or "turned off" or that processing irregularities or malicious code could be introduced, according to the GAO.

3.2 Project cost management

OSCA management did not prepare project budgets or estimates of project costs for the development, implementation, updating, and maintenance of all system changes required for the CRMS. In addition, OSCA management has not properly accounted for some project costs. Although vendor contracted costs are available to estimate and track project costs, OSCA management did not track these costs as an overall project budget or consider other project costs outside of the contracts, such as agency personnel costs.

The OSCA does not fully estimate the costs expected for each planned change. Since budgets had not been developed for projects or planned changes, OSCA management had not maintained the information needed to effectively monitor whether actual project costs were aligned with expected costs or to timely identify significant deviations. OSCA officials said costs were not monitored at the project level, but actual costs for court automation and IT expenditures were monitored against the budget at the department level.

OSCA records indicate at least $218 million has been spent for the period of July 1, 1994, through June 30, 2015, for the court automation program; however, OSCA personnel indicated this amount is not completely accurate. Some reasons for inaccurate cost information include the following:

- Some hardware and software costs reported were not directly attributable to the CRMS and were directly attributable to other systems.
- OSCA staff time and costs were not tracked at the project level. As a result, the OSCA is unable to determine the amount of time charged that relates to the CRMS.
- Other project costs may have been incurred but charged to different funding sources.

OSCA officials said managing the CRMS is an ongoing process that is part of their daily duties and, as a result, they do not consider it necessary or beneficial to manage the system at a project level. The CRMS costs are a subset of the costs for the court automation program and some costs were shared.

According to accepted standards, organizations should prepare project budgets that reflect the full economic life cycle costs and the related benefits. In addition, organizations should manage project performance against key criteria, such as costs and schedule, to identify deviations from the plan and take remedial actions when required. To develop the budgets, management should identify the applicable cost factors associated with the project tasks, according to accepted standards. The development of costs for each task should be simple and direct and consist of labor (internal and external), material and other costs. The cost of performing a task is directly related to the personnel assigned to the task, the duration of the task, the cost of any non-labor items required by the task and any allocated indirect cost. Non-labor charges include such items as material costs, reproduction, travel, the cost of capital (if leasing equipment), computer center charges and equipment costs.

As part of the ongoing improvement to the CRMS, the OSCA is currently developing a new system to replace the JIS. To ensure prudent use of funds and resources, OSCA management should prepare a budget for this new system. A complete and well-planned budget can serve as a useful management tool by establishing specific cost expectations for each project, providing a means to effectively monitor actual costs, and assisting in keeping cost overruns to a minimum. In addition, an adequate system to track actual costs of developing and implementing a large system is necessary to properly monitor actual project costs and should be used to compare against project estimates and budgets. This information is necessary for making key project management decisions.

3.3 Future plans and costs

OSCA management has not developed a formal long-range plan or prepared adequate estimates of the additional costs expected for the CRMS. Officials said additional functionality and changes are still needed and planned for the CRMS. According to accepted standards, management should create a strategic plan that includes the initiatives required to achieve organizational goals. These initiatives should be translated into a high-level road map indicating the relative scheduling and interdependencies of the initiatives.

OSCA officials said plans are in place that establish the priorities of certain projects. However, these plans do not include some of the information recommended by accepted standards, such as clear details of the work breakdown structures. In addition, a complete long-term plan has not been established. The current plan is short-term, on a one-year timeframe. An OSCA official said priorities may change and plans are limited to available funding; in addition, unexpected mandates, such as statutory requirements, also require plans to be modified and schedules adjusted.

A report issued by the Committee on Legislative Research, Oversight Division in 2000 identified the OSCA had not developed long-range plans for the implementation and maintenance of the case management systems at the courts. In addition, Report No. 2006-01, *Office of State Courts Administrator,* issued in January 2006, noted the OSCA had not estimated the long-range costs.

A major funding source for the CRMS is the court automation fee established in section 488.027, RSMo. This fee was to sunset in 2018 but was reauthorized through September 2023 by the General Assembly in

2016. A formal long-range plan was not prepared before the legislature extended the fee, but is necessary to ensure the General Assembly is aware of the state's total potential financial commitment prior to funding new features of the CRMS. Without developing formal long-range plans and cost projections, OSCA management is unable to ensure sufficient funding is available to support and complete additional system projects and ensure changes are prioritized and scheduled appropriately.

Recommendations

The OSCA, in conjunction with the MCA Committee:

3.1 Fully implement an appropriate system development life cycle methodology, including change control management policies.

3.2 Ensure future projects are supported by a formal project budget to ensure costs are accounted for and compared to budgeted amounts.

3.3 Develop a long-range plan. In addition, the OSCA should prepare a thorough and reliable financial projection to support future budgets and funding needs. The plan should be updated as necessary based on unexpected occurrences and actual costs.

Auditee's Response

3.1 OSCA utilizes both Agile and Waterfall methodologies for application development. The MCA has a robust change control process which is documented and approved.

3.2 As noted, the CRMS is defined by OSCA as an ongoing process, whereas project costs are tracked at the project level (e.g. Pay by Web or eFiling) and court automation expenses are coded and capitalized.

3.3 Since the auditors' visit, the MCA has developed a detailed strategic plan which will provide a road map for future court automation including the CRMS. This plan contemplates the availability of fiscal and staff resources and tracks development from policy review through application maintenance and termination.

Auditor's Comment

3.1 The system development life cycle should include the overall process of developing, implementing, and retiring information systems, not just application development and change control.

4. Contingency Planning

OSCA management has not fully established a business continuity plan or a disaster recovery plan to ensure the availability of technology resources.

4.1 Business continuity plan

OSCA management has documented and informally adopted a business continuity plan; however, the plan has not been formally approved by management, updated, or tested, increasing the risk the plan may not be adequate to support the timely recovery of business functions after the occurrence of a disaster or other significant incident.

OSCA adopted an emergency plan reference guide, which was approved, and considered as part of the agency's business continuity plan. However, the guide does not discuss some necessary policies or procedures related to business continuity planning, such as continuity planning philosophy or strategy. The draft business continuity plan was originally created in 2011; however, formal documentation of senior management approval was not maintained and the plan has not been updated since that time.

Continuity planning provides an efficient approach for agencies to develop policies and procedures for the timely recovery and restoration of critical processes and services vital to citizens, according to accepted standards. Continuity planning also provides a structured approach for developing cost-effective solutions that accurately reflect business requirements and integrate continuity planning principles into all aspects of information technology operations.

Without an up-to-date or tested business continuity plan, management has limited assurance the organization's business functions can be sustained during or promptly resumed after a disruptive incident.

4.2 Disaster recovery plan

OSCA management has not fully established a disaster recovery plan to ensure the availability of technology resources.

OSCA management has developed certain contingency plans and implemented basic controls for recovery planning. However, the disaster recovery plan has not been fully established or formally tested to ascertain the effectiveness of recovery procedures. The disaster recovery plan was last updated in May 2014. The plan does not include information that would be necessary should a disaster occur, such as locations of backup data or replacement equipment, responsibilities of key personnel, and procedures to re-establish communications. In addition, since the plan has not been fully developed, a formal test to ensure critical systems can be fully restored has not been performed. OSCA officials said some recovery procedures have been implemented but acknowledged the plan is not comprehensive and has not been fully updated to reflect changes in the operating environment.

Losing the capability to process and retrieve information can significantly affect an agency's ability to accomplish its mission, according to the GAO. If recovery plans are inadequate, interruptions can result in lost or incorrectly processed data and expensive recovery efforts. Given the implications of mission critical systems not being available for use, it is essential an agency maintains a tested plan to recover critical operations should interruptions occur. According to accepted standards, a disaster recovery plan is a written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities. Recovery plans and procedures are essential steps in ensuring that agencies are adequately prepared to cope with the loss of operational capabilities due to a service disruption such as an act of nature, fire, accident, or sabotage. According to accepted standards, recovery plans should cover all key functions, including assessing an agency's information technology and identifying resources, minimizing potential damage and interruption, developing and documenting the plan, training personnel in their contingency roles and responsibilities and providing refresher training, and testing them and making necessary adjustments.

Without an operational disaster recovery plan, management does not have assurance technology resources could be restored in the event of a significant disruption to normal system operations and management has limited assurance data and systems could be recovered and made available to meet requirements in the event of failure at the primary processing location.

Recommendations

The OSCA:

4.1 Complete the process of documenting, approving, and testing the business continuity plan.

4.2 Establish, maintain, and test a comprehensive disaster recovery plan that reflects the current processing environment.

Auditee's Response

4.1 OSCA agrees that having a fully developed and formally approved plan is best practice and will take this recommendation under advisement.

4.2 Disaster recovery capabilities are a part of ongoing operational activities and are currently in place. Many disaster recovery procedures are executed on a regular basis (e.g., a sample of production JIS databases are restored monthly to ensure the validity of the backups, weekly the Judicial Data Center 1 utilizes the alternate power supply from a generator). Concurrent testing of all disaster recovery capabilities will be presented to the MCA for consideration.

5. Monitoring Reports

Opportunities exist to increase the efficiency and effectiveness of the monitoring performed of activity processed in the CRMS at the local courts. These opportunities to assist the courts could be accomplished through additional monitoring reports or other tools. Examples of the reports not currently available to courts include, but are not limited to, the following:

- A report to identify cases disposed with no fees or costs assessed. Without this report, cases could be inappropriately disposed without fees or costs assessed.
- A report to identify cases exempt from debt collections or cases with an unreasonable payment plan effective date or end date. Supreme Court Operating Rule (COR) 21.07 requires all courts using the JIS to participate in the tax offset and debt collection programs and requires the court to create payment plans in the JIS for all amounts not paid in full at case disposition. Without these reports, a case could be exempted from debt collections or a payment plan could be set for an unreasonable timeframe (such as 20 years from case disposition) without detection by management.
- A report to identify cases where the time payment fee was not assessed. COR 21.13 requires all divisions of the circuit courts, except municipal divisions, to assess a $25 time payment fee on all cases not paid in full within 30 days of disposition. Currently, court clerks are required to manually assess the time payment fee. OSCA officials said work is being performed to modify the JIS functionality to automatically assess the time payment fee.
- Additional report(s) or other tool(s) to assist the courts in reconciling eFiling transactions. The manner in which eFiling receipts are processed result in reconciling differences between the CRMS and the bank. As a result, some courts have established manual processes to track these differences.
- A report to identify garnishments not disbursed within 10 days of receipt. Supreme Court Rule 90.11 states garnishments collected shall be disbursed to the garnishor by the court clerk, less costs, within 10 days unless the garnishee has requested an allowance under Supreme Court Rule 90.12(a). An OSCA official said the open items report currently available could be used to assist in identifying receipts not disbursed timely. However, this report only shows the last receipt date for a case, so manual reviews of each case with receipts not disbursed are necessary to identify the receipts included on the open items report that exceed the 10 days.

Without adequate monitoring reports being available to assist courts, there is an increased risk of court staff not being able to effectively and efficiently identify discrepancies, potential loss of revenue, or noncompliance with court regulations.

Recommendation

The OSCA, in conjunction with the MCA Committee, review potential reports to assist in increasing the effectiveness and efficiency of court staff monitoring procedures and implement these reports or tools as necessary.

Auditee's Response

Since the auditors' visit, additional reporting tools have been deployed, including a report that identifies cases disposed with no fees or costs assessed and a report that assists clerks in identifying pending transactions in the clerk queue. Currently under development are a report to identify cases without a time payment fee and a report to identify cases without a payment plan.

Office of State Courts Administrator
System of Case and Record Management of the Judiciary
Division of Responsibility

OSCA officials provided a detailed breakdown of the main responsibilities set by the Missouri Court Automation Committee for OSCA and the local courts for the security, operation and maintenance of the case and record management system (CRMS) of the judiciary. OSCA is responsible for supporting the administration of the local courts and the local courts are responsible for the daily operations of court case management. Both OSCA and the local courts have responsibilities to ensure adequate controls are in place and operating effectively to maintain the integrity of court case data. This division of responsibility is described below.

The following tasks are the responsibility of staff at OSCA:

- Provide centralized security and database administration
- Grant system access once approved by the local courts
- Approve system access for OSCA staff
- Provide training, training materials, and procedure manuals for recommended use of the system (such as the Judicial Information System (JIS))
- Staff a help desk to provide assistance to the local courts
- Perform backup functions for servers and databases located at the OSCA and certain local courts
- Develop, test, and implement new systems
- Maintain the system, including testing and installing added functionality to existing systems
- Manage networking capabilities
- Maintain necessary hardware not provided by the local courts (i.e. computer servers)
- Liaison activities and contract management with court automation program vendors

The following tasks are the responsibility of the local court officials as they relate to the CRMS, with primary focus on the JIS:

- Approve system access for local court staff
- Perform case processing and management
- Receive, deposit and disburse monies
- Perform fiscal management, including daily accounting for cases and end-of-month accounting for the court
- Ensure compliance with procedures for recommended use of the CRMS
- Segregation of duties or a review of operations when segregation is not possible
- Physical security of court case information and computer equipment
- Maintain adequate work stations (i.e. personal computers)