CITY OF DALLAS

Dallas City Council

Mayor
Michael S. Rawlings

Mayor Pro Tem
Monica R. Alonzo

Deputy Mayor Pro Tem
Erik Wilson

Council Members
Carolyn King Arnold
Rickey D. Callahan
Mark Clayton
Jennifer S. Gates
Sandy Greyson
Scott Griggs
Philip T. Kingston
Lee M. Kleinman
B. Adam McGough
Adam Medrano
Casey Thomas, II
Tiffinni A. Young

Office of the City Auditor

Audit Report

AUDIT OF ACCESS CONTROLS FOR THE COURTS' INFORMATION SYSTEMS

(Report No. A16-004)

December 4, 2015

City Auditor

Craig D. Kinton

Table of Contents

Executive Summary

The Department of Communication and Information Services (CIS) did not provide persuasive evidence to demonstrate that the $2.8 million contract to implement the Incode Municipal Court Case Management and the Content Management System (Incode System) was monitored effectively. As a result, the City of Dallas (City) cannot adequately assess whether the Incode System was implemented in accordance with City specifications.

In addition, the Department of Court and Detention Services (CTS):

- Did not clearly establish standard user profiles prior to Incode System implementation
- Continues to modify the standard user profiles and access privileges
- Does not adequately monitor user access and "Process and Transaction" activity logs (activity logs)

Background Summary

The Department of Court and Detention Services (CTS) implemented the Incode Court Case Management and the Content System (Incode System) in October 2013 to automate the court workflow process, such as issuing warrants and processing fines and fees. The CTS implemented the Incode System with assistance from the Department of Communication and Information Services (CIS). The Department of Judiciary (CTJ) and the City Attorney's Office (ATT) are also users of the Incode System.

For Fiscal Year (FY) 2014, the Municipal Court Services' adopted operating and revenue budgets were $10,033,215 and $13,779,457, respectively. The Municipal Court Services' performance measures included hearing 99.5 percent of traffic and ordinance cases within 45 days of request, accepting 50 percent of the payments without requiring an office visit, and achieving a seven minute average wait time at the cashier's window.

Source: City of Dallas Adopted Annual Budget; CIS and CTS

Due to the customization of the standard user profiles and access privileges within the Incode System, there is an increased risk of inadequate segregation of duties. When segregation of duties is not maintained or monitored periodically, users may take advantage of potential gaps in security. Also, invalid transactions may not be identified and corrected timely.

The CIS Project Management Office (PMO) could not provide persuasive evidence of the contract monitoring activities specified in the $2.8 million contract between the City and Tyler Technologies. The contract specifies that the CIS-PMO would monitor the overall status of the project, including risk and change management[1] activities to provide the City assurance that Tyler Technologies:

- Verified the Incode System was in full compliance with the application specifications defined in the Statement of Work (SOW) and/or business process requirements using City data

[1] Change management describes a process for controlling the life cycle of all changes that are beneficial, with minimal disruption to Information Technology (IT) services. Adequate documentation is a necessary subset of the change management process.

- Established the baseline for the business processes (business process analysis). A business process analysis is a disciplined approach where the department identifies and documents all the required manual and automated activities that would impact the Incode System's implementation.

- Included appropriate security management activities that define who has the ability to execute a transaction. Security management activities support segregation of duties by preventing one individual from having access that is not necessary for the performance of their job duties. In particular, segregation of duties should address the risk of management override, error, misuse or fraud.

We recommend the Director of CIS establishes, conducts, and retains evidence of monitoring activities to show that Tyler Technologies is complying with the remaining implementation activities in the contract.

We recommend the Director of CTS: (1) establishes standard user profiles. If business process changes result in the need to modify existing user profiles, management should evaluate these modifications for inadequate segregation of duties; (2) develops a mapping and/or reference document to assist in the consistent review of users' access; and, (3) periodically reviews the activity logs to monitor for known and other potential security risks.

The original audit objective was to evaluate the adequacy of the new CTS information systems': (1) access controls; and, (2) internal controls over cash management/collection processes for fines and fees which may include cash bond forfeitures and reinstatement on Class C misdemeanors. The audit objective was later divided into two audits. The focus of this audit was limited to contract monitoring and access controls. The scope of the audit was from October 2012 to August 2015; however, certain other matters, procedures, and transactions outside that period were reviewed to understand and verify information during the audit period.

Management's response to this report is included as Appendix III.

Audit Results

Overall Conclusion

The Department of Communication and Information Services (CIS) did not provide persuasive evidence to demonstrate that CIS effectively monitored the $2.8 million contract to implement the Incode Municipal Court Case Management and the Content Management System (Incode System). As a result, the City of Dallas (City) cannot adequately assess whether the Incode System was implemented in accordance with the City specifications. In addition, the Department of Court and Detention Services (CTS):

- Did not clearly establish standard user profiles prior to Incode System implementation
- Continues to modify the standard user profiles and access privileges
- Does not adequately monitor user access and "Process and Transaction" activity logs (activity logs).

Due to the customization of the standard user profiles and access privileges within the Incode System, there is an increased risk of inadequate segregation of duties. When segregation of duties is not maintained or monitored periodically, users may take advantage of potential gaps in security. Also, invalid transactions may not be identified and corrected timely.

Persuasive Evidence Was Not Provided To Demonstrate the $2.8 Million Incode System Contract Was Monitored Effectively

The CIS did not provide persuasive evidence to show that CIS effectively monitored the $2.8 million contract to implement the Incode System. As a result, the City cannot adequately assess whether the Incode System was implemented in accordance with the City's specifications.

In the contract between the City and Tyler Technologies, the Statement of Work (SOW), specifies the CIS Project Management Office (PMO) would monitor the overall status of the project, including risk and change management[2] activities. The CIS-PMO could not provide persuasive evidence of the contract monitoring activities and the required deliverables, such as:

- Application questionnaires and a project planning survey that established the baseline for the business processes and related automated controls for court case management, cash collections, citations, and warrants processing. Automated control activities are activated through the application and tend to be more reliable than manual controls. Identifying business process control activities helps ensure the Incode System automated controls continue to operate properly.

[2] Change management describes a process for controlling the life cycle of all changes that are beneficial, with minimal disruption to Information Technology (IT) services. Adequate documentation is a necessary subset of the change management process.

- A base configuration plan that includes security, general ledger accounts, fee and offense codes, and the court calendar. Security specifically considers the segregation of duties to reduce the possibility that a single person could introduce errors or commit fraud which may not be detected in the normal course of business.

- Functional testing plans which verify the application functionality is in full compliance with the specifications and business process requirements using City data.

- Project management plan that would govern the successful implementation of the application. Tyler Technologies did establish roles and responsibilities with the City in the form of a Responsibility Assignment Matrix (RACI) matrix. The RACI matrix, however, was defined from the perspective of Tyler Technologies and may not have included all the necessary elements to benefit the City.

RACI Definition

RACI Matrix: A RACI matrix, also known as Responsibility Assignment Matrix (RAM), describes the participation by various roles in completing tasks or deliverables for a business process. The most common usage of responsibility matrices is in project management. In a RACI matrix, there are four levels: Responsible, Accountable, Consulted, and Informed. Sometimes the RACI matrix is modified with an additional role, such as Support.

Source: Information Technology Infrastructure Library website.

- Post implementation efforts to verify compliance with the City's security standards and policies. The City has established certain security standards through the CIS Enterprise Security Standards and the Administrative Directives (AD) for network access, use of data, and the role of the vendor in providing on-going services. Whether these standards were incorporated successfully into the security elements of the Incode System was not identifiable.

Currently, Tyler Technologies is still in the process of implementing additional SOW components that will continue to impact the functionality of the Incode System. According to AD 4-5 *Contracting Compliance*: "*Each City Department has the primary responsibility for monitoring the performance of vendors providing goods or services solely to that department."*

Recommendation I

We recommend the Director of CIS establishes, conducts, and retains evidence of monitoring activities to show that Tyler Technologies is complying with the remaining implementation activities in the contract.

Please see Appendix III for management's response to the recommendation.

Standard User Profiles and Access Privileges Were Not Clearly Established Prior to Implementation and Continue To Be Modified

Standard user profiles and access privileges were not clearly established prior to Incode System implementation. In addition, the standard user profiles and access privileges (e.g., cashier role) are still being modified by CTS. Due to the customization of the standard user profiles and access privileges within the Incode System, there is an increased risk of inadequate segregation of duties. When segregation of duties is not maintained or monitored periodically, users may take advantage of potential gaps in security.

Control Activities for Security Management

Unique User Identification: Management designs control activities to limit user access to information technology through authorization control activities such as providing a *unique user identification* or token to authorized users. These control activities may restrict authorized users to the applications or functions commensurate with their assigned responsibilities, supporting an appropriate *segregation of duties*. Management designs other controls to promptly update access rights when employees change job functions or leave the entity.

Segregation of Duties: Segregation of duties helps prevent fraud, waste, and abuse in the internal control system. Management considers the need to separate control activities related to authority, custody, and accounting of operations to achieve segregation of duties. In particular, segregation duties can address the risk of management override. Management override circumvents existing control activities and increases fraud risk.

Source: Standards for Internal Control in the Federal Government, Principle 11, Paragraph 11.14, Pages 54 and Principle 10, Paragraph 10.13, Page 51

The number of user access reviews completed after implementation shows that security risks were pervasive. Specifically, the user access reviews included the following:

- November 2013 – Reviewed security profiles for the Department of Judiciary (CTJ) employees and updated the granted users access in the Incode System to match actual roles and responsibilities

- April 2014 – Reviewed security profiles for CTS employees and updated granted users access in the Incode System to match user profiles

- June 2014 – Reviewed all the Incode System users and determined that some users had more than the necessary privileges and removed their administrative rights

- August 2014 – Reviewed all the Incode System users and determined that some users had void capabilities that were inappropriate for their job responsibilities

- December 2014 – Reviewed all the Incode System users for additional user access privileges modification. This review was completed with the assistance of Tyler Technologies

According to CTS management, user profiles and access privileges continue to be modified due to anticipated and unanticipated business process changes. For example, when customer volume decreased for CTS, cashiers had additional time to absorb other activities in the cash collection process. In order to provide additional access, more user

access privileges were granted than normally assigned to cashiers. These cashier user access privilege changes, however, were not consistent from one cashier to another.

According to the Federal Information System Controls Audit Manual (FISCAM), management should consider the organizational structure and roles when determining appropriate user profiles for a business process and develop standard user access profiles that could withstand new additions and changes in the business processes. Management should also divide or segregate duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. In particular, segregation of duties should address the risk of management override. If segregation of duties is not practical, management should design alternative control activities to address the risk of fraud, waste or abuse in operations.

Recommendation II

We recommend the Director of CTS establishes standard user profiles. If business process changes result in the need to modify existing user profiles, management should evaluate these modifications for inadequate segregation of duties.

Please see Appendix III for management's response to the recommendation.

Monitoring Of Users' Access and Activity Logs Is Not Fully Implemented

The CTS does not adequately monitor the Incode System's users' access or activity logs. As a result, there is an increased risk that segregation of duties may not be maintained and that invalid transactions may not be identified and corrected timely. Specifically:

Incode System's User Access Reviews

Control Activity for Reviews

Reviews by management at the functional or activity level compare actual performance to planned or expected results throughout the organization and analyze significant differences.

Source: Standards for Internal Control in the Federal Government, Principle 11, Page 53.

The Incode System's annual user access reviews are not performed consistently. Instead of using a mapping or reference document, user access reviews are completed based on the CTS managers' knowledge of the business process and the users in the department. Also, the Incode System user access reports are not user friendly and are often missing one or two of the three items necessary for appropriate user access review, such as security codes.

The combination of an individual reviewer's knowledge and the difficulty in understanding user access reports make it challenging to maintain consistency when performing user access reviews. The current mechanisms employed by CTS make it more difficult for the CTS managers to perform user access reviews consistently over time.

Incode System's Activity Logs

The Incode System's activity logs are not set to track known security risks. For example, due to an Incode System limitation CTS supervisors are given application administrator level access to perform void transactions which creates a security risk; however, these transactions are not identified in the activity logs. In addition, CTS Incode System administrators are not reviewing the activity logs to identify other potential security risks.

According to the CTS Incode User Access Auditing, the CIS Standard Operating Procedures: *Managing User Administration Tyler Incode Central CCMS System User Administration,* and AD 2-24, *Computer Security,* access should be granted upon proper approval and authorization, terminations should be removed completely, and monitoring should be completed consistently to capture all access issues. At the account or transaction levels, management may periodically compare users to their recorded accountability to help reduce the risk of errors, fraud, abuse or unauthorized alteration.

Recommendation III

We recommend the Director of CTS:

- Develops a mapping and/or reference document to assist in the consistent review of users' access

- Periodically reviews the activity logs to monitor for known and other potential security risks

Please see Appendix XX for management's response to the recommendation.

Appendix I

Background, Objective, Scope and Methodology

Background

The Department of Court and Detention Services' (CTS) Municipal Court Services provides administrative and clerical support for the Dallas Municipal Court. The Dallas Municipal Court is divided into 15 Municipal Courts. The CTS is responsible for processing civil cases, citations and requests for court programs, providing courtroom support, collection of fines and fees, warrant enforcement, contract compliance, and financial services, responding to information requests, confirming warrants for the Dallas Police Department and 150 regional law enforcement agencies, and preparing court dockets.

For Fiscal Year (FY) 2014, the CTS' Municipal Court Services was authorized a total of 145 full-time equivalents, and the adopted operating and revenue budgets were $10,033,215 and $13,779,457, respectively. The performance measures included hearing 99.5 percent of traffic and ordinance cases within 45 days of request, accepting 50 percent of the payments without requiring an office visit, and achieving seven minute average wait time at the cashier's window.

For FY 2015, the CTS' Municipal Court Services was authorized a total of 102 full-time equivalents, and the adopted operating and revenue budgets were $8,525,026 and $12,213,568, respectively. The CTS' performance measures included hearing 95 percent of traffic and ordinance cases within 30 days of request, accepting 35 percent of the payments without requiring an office visit, and achieving five minute average wait time at the cashier's window.

The Incode Court Case Management and the Content Management System (Incode System) was implemented in October 2013 to automate the court workflow process that includes uploading the citation (e-citations and paper citations) information, scheduling court dates, maintaining the court dockets, scheduling officers, notifying judiciary, updating case status, issuing warrants, and processing fines and fees. The Incode System was implemented as an off-the-shelf product with the assistance of the vendor, Tyler Technologies. The contract between the City and Tyler Technologies specifies the Department of Communication and Information Services (CIS) Project Management Office (PMO) would monitor the overall status of the project including risk and change management activities.

Objective, Scope and Methodology

This audit was conducted under the authority of the City Charter, Chapter IX, Section 3 and in accordance with the FY 2014 Audit Plan approved by the City Council. This performance audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained

provides a reasonable basis for our findings and conclusions based on our audit objective.

The original audit objective was to evaluate the adequacy of the new CTS information systems': (1) access controls; and, (2) internal controls over cash management/collection processes for fines and fees which may include cash bond forfeitures and reinstatement on Class C misdemeanors. The audit objective was later divided into two audits. The focus of this audit was limited to contract monitoring and access controls. The scope of the audit was from October 2012 to August 2015; however, certain other matters, procedures, and transactions outside that period were reviewed to understand and verify information during the audit period.

To achieve the audit objective, we performed the following procedures:

- Reviewed and analyzed best practices, such as the National Institute for Standards and Technology, Federal Information System Controls Audit Manual, Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control – Integrated Framework, 2013, Administrative Directives, CIS and CTS policies and procedures

- Reviewed the contract for the Incode System

- Interviewed personnel from CIS and CTS

- Performed walkthroughs of security processes

- Reviewed and analyzed supporting documentation for new hires, terminations, and transfers

Appendix II

Major Contributors to This Report

Sam Willson, Auditor
Anoosha Sagi, CIA – Project Manager
Mamatha Sparks, CIA, CISA – Audit Manager
Carol Smith, CPA, CIA, CFE – First Assistant City Auditor
Theresa Hampden, CPA – Quality Control Manager

Appendix III

Management's Response

Memorandum

RECEIVED
DEC - 3 2015
City Auditor's Office

CITY OF DALLAS

DATE: November 20, 2015

TO: Craig D. Kinton, City Auditor

SUBJECT: Response to Audit Report:
Audit of Access Controls for the Courts' Information Systems

Our responses to the audit report recommendations are as follows:

Recommendation I

We recommend the Director of CIS establishes, conducts, and retains evidence of monitoring activities to show that Tyler Technologies is complying with the remaining implementation activities in the contract.

Management Response / Corrective Action Plan

Agree ☒ Disagree ☐

The replacement of the City's in-house developed Court Case Management System was successfully completed on schedule and met the primary goal of bringing to the City a new and more efficient technology for processing the daily activities in our municipal court. Since the system came online two years ago on October 1, 2013, there have not been any significant issues with the system and it continues to serve the citizens of Dallas as originally envisioned.

CIS acknowledges that it did not provide a complete set of documents regarding the project implementation per the auditors requested timeframe. After visiting with the auditors about the information we did provide, CIS undertook an effort to collect from the external system integrator the entire volume of recorded information for the Court Case Management System project. After the report was drafted, CIS offered the information to the auditors; however, the agreed-upon timeframe for providing the information had passed so the information was not used by the auditors.

Over 200 documents and several thousands of pages of documentation were recorded and maintained for the implementation. These documents encompass Assistant City Manager-led project review meetings, application specifications, business requirements, project plans, functional test plans, regular project risk

assessment, segregation of duties delineation, security implementation, and many others. However, due to staffing changes after the project was successfully completed, the documentation was not organized into a single repository, readily available. Consequently, many documents supporting the implementation were not reviewed by the auditor. Those documents are now available and address and explain many of the individual findings that comprise this recommendation.

CIS is updating its project management methodology to account for and ensure project documentation is located in a single and logically organized repository.

CIS will establish, conduct, and retain evidence of monitoring activities to show that Tyler is complying with the remaining implementation activities in the contract.

Implementation Date
June 30, 2016

Responsible Manager
CIS, Senior Manager for Project Management Office

Sincerely,

William Finch, Director
Department of Communication and
Information Systems

Mark McDaniel
Assistant City Manager

C:

RECEIVED

DEC – 2 2015

City Auditor's Office

Memorandum

DATE: December 1, 2015

TO: Craig D. Kinton, City Auditor

SUBJECT: Response to Audit Report:
Audit of Access Controls for the Courts' Information Systems

Our responses to the audit report recommendations are as follows:

Recommendation II

We recommend the Director of CTS establishes standard user profiles. If business process changes result in the need to modify existing user profiles, management should evaluate these modifications for inadequate segregation of duties.

Management Response / Corrective Action Plan

Agree ☒ Disagree ☐

Court and Detention Services, Municipal Prosecution, and Judiciary established user profiles prior to the system go-live date. In the months after go-live, end user departments became more familiar with the system and refined "off the shelf" security access levels to curtail risk. A standard and documented process to set up, modify and delete user profiles has been in place since August 2014. All user profiles are assigned a standard template type, which accounts for job functions and segregation of duty considerations. Since the advent of this process, user profiles have been set up in a consistent manner. As a failsafe, annual profile reviews are conducted by executives in Court and Detention Services to ensure there are no lapses in this standardized process.

In an effort to ensure all user profiles established prior to August 2014 fit the current standard template types, Court and Detention Services will delete all current users and recreate their profiles. This will ensure that no user established prior to August 2014 holds access levels outside of the standard template type. Additionally, Court and Detention Services will create a documented process enumerating how internal control conflicts are considered when new user profile templates are implemented. Municipal Prosecution and Judiciary have agreed to follow a similar process.

Implementation Date

All profiles will be deleted and recreated with a standardized template by June 30, 2016. The creation of a documented process on how to evaluate internal control conflicts for new user template types will be implemented by June 30, 2016.

Responsible Manager

Assistant Director of CTS

Recommendation III

We recommend the Director of CTS:

- Develops a mapping and/or reference document to assist in the consistent review of the users' access

- Periodically reviews the activity logs to monitor for known and other potential security risks

Management Response / Corrective Action Plan

Agree ☒ Disagree ☐

Court and Detention Services will expand the level of detail provided in its current International Standard of Operations (ISO) process on how to conduct a security user access review. Within the expanded description, a previously unutilized method of identifying potential internal control violations will be conducted and documented.

Implementation Date

June 30, 2016

Responsible Manager

Assistant Director CTS

Sincerely,

Gloria López Carter, Director
Department of Court and Detention Services

Eric D. Campbell
Assistant City Manager