Clerk of Superior Court

February 2018

Internal Audit Report Authorized by the Maricopa County Board of Supervisors

Internal Audit Department

301 W Jefferson St
Suite 660
Phoenix, AZ 85003

maricopa.gov/internalaudit

602.506.1585

Mike McGee
County Auditor

Objectives

- Accounts payable, purchasing card, and travel controls are adequate to ensure expenditures are processed according to policy.
- Statutorily set fees are accurately recorded in the billing system and fee distributions are made according to statute.
- Information Technology (IT) controls governing system access and data center activities adequately restrict access to computer resources and support data center security and functions.
- IT project and change management controls provide reasonable assurance that IT projects and system changes are appropriately authorized and implemented.
- Data backup and contingency planning controls provide reasonable assurance that critical information processing could be restored in the event of a disaster.

Scope

This audit primarily focused on controls over the Clerk of the Superior Court (COSC) finance and IT functions. The audit covered July 2014 – September 2017. We interviewed key personnel, reviewed applicable policies and procedures, and examined financial and IT supporting documentation. Due to unforeseen circumstances, our review of statutorily set fees, fee distribution percentages, and the proper restriction of access to data in key software applications will be postponed to FY 2019.

Standards

This audit was approved by the Board of Supervisors and was conducted in conformance with International Standards for the Professional Practice of Internal Auditing. The specific areas reviewed were selected through a formal risk-assessment process.

Auditors

Stella Fusaro, Audit Manager, CIA, CGAP, CRMA, CFE
Susan Adams, Audit Supervisor, MBA, CISA, ITIL
Kenton Schaben, Senior Auditor, CFE
Megan McPherson, Senior Auditor, MEd

This report is intended primarily for the information and use of the County Board of Supervisors, County leadership, and other County stakeholders. However, this report is a public record and its distribution is not limited. We have reviewed this information with Clerk of Superior Court management. The Action Plan was approved by Michael Jeanes, Clerk of Superior Court, on February 1, 2018. If you have any questions about this report, please contact Mike McGee, County Auditor, at 602-506-1585.

Audit Results

Issue #1: Expenditures

Observation: We interviewed key personnel and reviewed a sample of expenditures to assess internal controls over accounts payable and purchasing cards. Overall, we determined that expenditures were authorized and properly recorded. However, there were some internal control weaknesses related to documentation for contract purchases and payments as described below.

We reviewed supporting documentation for a sample of expenditures and found three purchases, totaling $167,570, without completed competition impracticable documentation. Competition impracticable policy allows County agencies to request procurement specific to one potential vendor by eliminating the competitive bidding process. Procurement Code requires a documented explanation of the need, the unique circumstances making compliance with regular procurement code unfeasible, and appropriate authorization based on the procurement price. We found two of the three purchases were under $100,000 and were missing the required Chief Procurement Officer approval; one purchase, over $100,000, was missing the required Board of Supervisor approval. We noted that all three purchases were from vendors used by COSC in the past.

We identified 14 purchases where the invoice pricing could not be matched to contract pricing. We also found two purchases where the labor rates on the invoice could not be matched with the rates on the contract. There was one purchase for which the renewed contract and related pricing could not be located.

<table>
<tr><th colspan="2"><b>Conclusion #1A:</b> Overall, expenditures were authorized and properly recorded.</th></tr>
<tr><th>Recommendation</th><th>COSC Action Plan</th></tr>
<tr><td>None</td><td>N/A</td></tr>
</table>

<table>
<tr><td colspan="2"><b>Conclusion #1B:</b> Competition Impracticable documentation was not always completed as required.</td></tr>
<tr><td><b>Recommendation</b></td><td><b>COSC Action Plan</b></td></tr>
<tr><td><b>1B-1</b> Develop procedures to ensure competition impracticable forms are submitted and retained according to policy. COSC should consider entering into a multi-year Competition Impracticable Agreement for reoccurring purchases.</td><td><b>Concur</b> – completed
COSC began using the County ERP system (ADV. 3X, implemented 7/1/2016). This system requires completed CI forms and certain processing steps to produce payments for these type of expenditures.
COSC has updated internal steps to meet these requirements, which were clarified by the Office of Procurement Services (OPS) (7/22/2017). COSC has contacted OPS to further research the multi-year CI agreement option.</td></tr>
<tr><td colspan="2"><b>Conclusion #1C:</b> Contract payment documentation did not demonstrate that invoice pricing complied with current contract terms.</td></tr>
<tr><td><b>Recommendation</b></td><td><b>COSC Action Plan</b></td></tr>
<tr><td><b>1C-1</b> Develop procedures to ensure that invoice pricing is compared to contract information (pricing, quotes, discounts and contractor information, etc.). Supporting documentation should be maintained according to policy/retention requirements.</td><td><b>Concur</b> – in progress
COSC will update its internal process to include screenshots from vendor portals and itemized quotes to further verify invoice pricing with contract pricing.
<b>Target Date:</b> February 1, 2018</td></tr>
</table>

Issue #2: Information Technology – Policies and Procedures

Observation: We interviewed IT personnel and reviewed supporting documentation and determined that COSC has implemented partial and informal procedures relating to data center operations management, change management, and IT project management. Establishing written policies and procedures creates consistency in how tasks are performed, and ensures controls are implemented as designed. They also allow management to identify and address or reduce risks that could jeopardize the accuracy and/or availability of systems and data necessary for business operations.

<table>
<tr><th colspan="2"><b>Conclusion #2A:</b> COSC has not fully developed policies and procedures for key IT functions.</th></tr>
<tr><th>Recommendation</th><th>COSC Action Plan</th></tr>
<tr><td><b>2A-1</b> Develop and implement policies and procedures to ensure implementation of controls over:
a. Data Center Operations
b. Change Management
c. IT Project Management</td><td><b>Concur</b> – in progress
COSC recently hired two new IT Managers that will be tasked with creating and formalizing policies and procedures as recommended in this report.
<b>Target Date:</b> Dec 31, 2018</td></tr>
</table>

Issue #3: User Access – Data Center Systems, Remote Access, and Passwords

Observation: We interviewed IT personnel and reviewed applicable documentation, and found that the COSC's Information Technology Group (ITG) has established policies addressing user access to key data center and business applications. In addition, COSC relies on the Administrative Office of the Court's (AOC) Minimum Security Standards for implementing appropriate user access controls. We reviewed COSC's password policy settings and found that the settings align with COSC policy and AOC recommended standards.

ITG has established controls over super-user level access to data center applications. We reviewed access lists for seven data center applications and found that 100% of the users with super-level access to the applications are appropriately restricted based on job responsibilities.

We also determined that COSC's remote access controls are adequate to ensure VPN access is restricted to current users. We found that 92 of 92 (100%) of the COSC VPN user accounts were for active, current users; no accounts belonged to terminated users.

<table>
<tr><th colspan="2"><b>Conclusion #3A:</b> COSC controls over remote access, passwords, and super-user level access to key data center applications are sufficient.</th></tr>
<tr><th>Recommendation</th><th>COSC Action Plan</th></tr>
<tr><td>None</td><td>N/A</td></tr>
</table>

Issue #4: Information Technology – Patching

Observation: Security patching refers to the process of installing software updates to fix or improve security holes within a computer program or data. We found that COSC has established automated procedures for patching and updating workstations. However, we found that a small number of servers had not been patched in a timely manner.

Conclusion #4A: System patching updates are not always performed timely.	
Recommendation	**COSC Action Plan**
4A-1 Ensure all systems are appropriately patched timely. As applicable, document specific reasons why systems may not be regularly updated.	**Concur** – completed COSC ITG has established controls that define when patching will be performed. ITG has documented the reasons why specific patching was not completed on-time during the audit. Moving forward all patching will be completed according to internal procedures, and there will be documentation explaining if there is a delay for a particular patching.

Issue #5: Information Technology – Change Management

Observation: Change management refers to the controlled identification and implementation of required computer system changes. We interviewed IT personnel and requested a list of application program changes for a recent six month period. COSC was not able to differentiate program changes from other help desk tickets because program changes had not been consistently entered into the tracking application. We also reviewed documentation provided as examples of change request authorization. None of the examples provided had an authorizing signature or date included on the form. Ineffective change management processes may result in possible equipment outages, damage, or failures.

Conclusion #5A: Program change requests cannot be distinguished from other help desk tickets.	
Recommendation	**COSC Action Plan**
5A-1 Establish procedures for entering and tracking program changes in the help desk ticket system. Ensure program changes are appropriately authorized.	**Concur** – in progress COSC recently hired an IT Manager that will directly oversee the Help Desk and its procedures. This manager will be implementing a new ticketing system for Help Desk; the system will ensure a formalized process to track Program Changes. Furthermore, the procedures will outline the approval process for program changes. **Target Date:** Dec 31, 2018

Issue #6: Data Backup and Contingency Planning

Observation: We interviewed key personnel and reviewed supporting documentation of COSC's contingency planning, data backup, recovery, and tape storage procedures.

COSC developed a disaster recovery plan to document its contingency planning. Based on our review of the disaster recovery plan, we determined that sufficient plans were in place to help ensure critical data could be restored during a disaster.

We reviewed the system configurations to determine that daily, weekly, and monthly backups were being performed as reported by management. There were some minor exceptions; however, those concerns were corrected by management during the audit. The monthly backup tapes are sent to an off-site storage facility. We reviewed facility reports and determined that tapes are kept off-site for one year.

COSC performs regular data recovery tests to ensure data can be properly recovered from backups. We reviewed data recovery test results for tests performed January – November 2017, and determined that the recoveries performed were successful.

Conclusion #6A: The disaster recovery plan provides reasonable assurance that critical information processing could be restored during a disaster.	
Recommendation	**COSC Action Plan**
None	N/A

<table>
<tr><td colspan="2"><b>Conclusion #6B:</b> Backup procedures are in place and were enhanced during the audit to help ensure all necessary data is appropriately backed up.</td></tr>
<tr><td><b>Recommendation</b></td><td><b>COSC Action Plan</b></td></tr>
<tr><td>None</td><td>N/A</td></tr>
<tr><td colspan="2"><b>Conclusion #6C:</b> Regular data recovery tests are performed and the results are documented.</td></tr>
<tr><td><b>Recommendation</b></td><td><b>COSC Action Plan</b></td></tr>
<tr><td>None</td><td>N/A</td></tr>
</table>