Maricopa County

Report on Internal Control and on Compliance

Year Ended June 30, 2017

A Report to the Arizona Legislature

Debra K. Davenport
Auditor General

ARIZONA
Auditor General
Making a Positive Difference

ARIZONA
AuditorGeneral
Making a Positive Difference

The Auditor General is appointed by the Joint Legislative Audit Committee, a bipartisan committee composed of five senators and five representatives. Her mission is to provide independent and impartial information and specific recommendations to improve the operations of state and local government entities. To this end, she provides financial audits and accounting services to the State and political subdivisions, investigates possible misuse of public monies, and conducts performance audits and special reviews of school districts, state agencies, and the programs they administer.

The Joint Legislative Audit Committee

Representative **Anthony Kern**, Chair
Representative **John Allen**
Representative **Rusty Bowers**
Representative **Rebecca Rios**
Representative **Athena Salman**
Representative **J.D. Mesnard** (ex officio)

Senator **Bob Worsley**, Vice Chair
Senator **Sean Bowie**
Senator **Judy Burges**
Senator **Lupe Contreras**
Senator **John Kavanagh**
Senator **Steve Yarbrough** (ex officio)

Audit Staff

Jay Zsorey, Director
Taryn Stangle, Manager and Contact Person

Contact Information

Arizona Office of the Auditor General
2910 N. 44th St.
Ste. 410
Phoenix, AZ 85018

(602) 553-0333

www.azauditor.gov

TABLE OF CONTENTS

STATE OF ARIZONA

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

OFFICE OF THE
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

Independent auditors' report on internal control over financial reporting and on compliance and other matters based on an audit of basic financial statements performed in accordance with *Government Auditing Standards*

Members of the Arizona State Legislature

The Board of Supervisors of
Maricopa County, Arizona

We have audited, in accordance with U.S. generally accepted auditing standards and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, the financial statements of the governmental activities, business-type activities, discretely presented component unit, each major fund, and aggregate remaining fund information of Maricopa County as of and for the year ended June 30, 2017, and the related notes to the financial statements, which collectively comprise the County's basic financial statements, and have issued our report thereon dated December 21, 2017. Our report includes a reference to other auditors who audited the financial statements of the Stadium District, Risk Management, Employee Benefits Trust, Housing Authority, and Industrial Development Authority, as described in our report on the County's financial statements. This report includes our consideration of the results of the other auditors' testing of internal control over financial reporting and compliance and other matters that are reported on separately by those other auditors. However, this report, insofar as it relates to the results of the other auditors, is based solely on the reports of the other auditors.

Internal control over financial reporting

In planning and performing our audit of the financial statements, we considered the County's internal control over financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the basic financial statements, but not for the purpose of expressing an opinion on the effectiveness of the County's internal control. Accordingly, we do not express an opinion on the effectiveness of the County's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies, and therefore, material weaknesses or significant deficiencies may exist that have not been identified. However, as described in the accompanying schedule of findings and recommendations, we and the other auditors identified certain deficiencies in internal control over financial reporting that we consider to be material weaknesses and significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the County's basic financial statements will not be prevented, or detected and corrected, on a timely basis. We consider the deficiencies described in the accompanying schedule of findings and recommendations as items 2017-01, 2017-02, 2017-03, 2017-06, and 2017-07 to be material weaknesses.

A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We consider the deficiencies described in the accompanying schedule of findings and recommendations as items 2017-04 and 2017-05 to be significant deficiencies.

Compliance and other matters

As part of obtaining reasonable assurance about whether the County's basic financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests and those of the other auditors disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

Maricopa County response to findings

Maricopa County's responses to the findings identified in our audit are presented in its corrective action plan at the end of this report. The County's responses were not subjected to the auditing procedures applied in the audit of the basic financial statements, and accordingly, we express no opinion on them.

Purpose of this report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the County's internal control or on compliance. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the County's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Jay Zsorey, CPA
Financial Audit Director

December 21, 2017

SCHEDULE OF FINDINGS AND RECOMMENDATIONS

Financial statement findings

2017-01

The County should improve security over its information technology resources and improve its risk-assessment process

Criteria—The selection and implementation of security controls and the risk-assessment process over the County's information technology (IT) resources, which include its systems, network, infrastructure, and data, are important because they reduce the risks that arise from the loss of confidentiality, integrity, or availability of information that could adversely impact the County's operations or assets. Therefore, the County should implement internal control policies and procedures for an effective IT security process that includes practices to help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT resources. In addition, the County's risk-assessment process should identify, classify, and inventory sensitive information.

Condition and context—The County did not have sufficient written IT security policies and procedures over its IT resources. In addition, the County's administrators did not identify and classify sensitive information as part of its risk-assessment process. Further, the County uses a service organization to house its data center but did not request and review the service organization's audit report until requested by auditors.

Effect—There is an increased risk that the County may not prevent or detect the loss of confidentiality, integrity, or availability of systems and data. Further, there is an increased risk that the County's administration and IT management may not effectively identify, analyze, and respond to risks that may impact its IT resources.

Cause—The County did not have adequate policies and procedures over IT security and its risk-assessment process and did not evaluate its policies and procedures against current IT standards and best practices. In addition, the County did not have policies and procedures in place to ensure that outside service organizations' independent audit reports were obtained and reviewed.

Recommendations—To help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT resources, the County needs to review its IT security policies and procedures against current IT standards and best practices, update them where needed, and implement them county-wide, as appropriate. Also, to help ensure the County has effective policies and procedures to identify, analyze, and respond to risks that may impact its IT resources, the County needs to improve its county-wide IT risk-assessment process. Further, the County should train staff on these policies and procedures. The information below provides guidance and best practices to help the County achieve these objectives.

- **Perform proactive logging and log monitoring**—Key user and system activity should be logged, particularly for users with administrative access privileges and remote access, along with other activities that could result in potential security incidents, such as unauthorized or inappropriate access. An entity should determine what events to log, configure the system to generate the logs, and decide how often to monitor these logs for indicators of potential attacks or misuse of IT resources. Finally, activity logs should be maintained where users with administrative access privileges cannot alter them.
- **Implement an incident response plan—**An incident response plan should be tested and implemented for an entity's IT resources, and staff responsible for the plan should be trained. The incident response plan should be distributed to incident response personnel and updated as necessary. Security incidents should be reported to incident response personnel so they can be tracked and documented. Policies and procedures should also follow regulatory and statutory requirements, provide a mechanism for assisting users in handling and reporting security incidents, and making disclosures to affected individuals and appropriate authorities if an incident occurs.
- **Provide training on IT security risks—**A plan should be developed to provide continuous training on IT security risks, including a security awareness training program for all employees that provides a basic understanding of information security, user actions to maintain security, and how to recognize and report potential indicators of security threats, including threats employees generate. Security awareness training should be provided to new employees and on an ongoing basis.
- **Perform IT vulnerability scans—**A formal process should be developed for vulnerability scans that includes performing vulnerability scans of IT resources on a periodic basis and utilizing tools and techniques to automate parts of the process by using standards for software flaws and improper configuration, formatting procedures to test for the presence of vulnerabilities, measuring the impact of identified vulnerabilities, and approving privileged access while scanning systems containing highly sensitive data. In addition, vulnerability scan reports and results should be analyzed and legitimate vulnerabilities remediated as appropriate, and information obtained from the vulnerability-scanning process should be shared with other departments of the entity to help eliminate similar vulnerabilities.
- **Apply patches—**Patches to IT resources should be evaluated, tested, and applied in a timely manner once the vendor makes them available.
- **Protect sensitive or restricted data—**Restrict access to media containing data the entity, federal regulation, or state statute identifies as sensitive or restricted. Such media should be appropriately marked indicating the distribution limitations and handling criteria for data included on the media. In addition, media should be physically controlled and secured until it can be destroyed or sanitized using sanitization mechanisms with the strength and integrity consistent with the data's security classification.
- **Develop and document a process for awarding and monitoring IT vendor contracts—**A process should be developed and documented to ensure the consideration of IT risks, costs, benefits, and technical specifications prior to awarding IT vendor contracts. In addition, contracts should include specifications addressing the management, reliability, governance, and security of the entity's IT resources. Finally, an IT vendor's performance should be monitored to ensure conformance with vendor contracts, including obtaining and reviewing the vendor's audit reports.
- **Identify, classify, inventory, and protect sensitive information—**Security measures should be developed to identify, classify, and inventory sensitive information and protect it, such as implementing controls to prevent unauthorized access to that information. Policies and procedures should include the security categories into which information should be classified, as well as any state statutes and federal regulations that could apply, and require disclosure to affected parties if sensitive information covered by state statutes or federal regulations is compromised.

The County's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

2017-02

The County should improve access controls over its information technology resources

Criteria—Logical and physical access controls help to protect a County's information technology (IT) resources, which include its systems, network, infrastructure, and data, from unauthorized or inappropriate access or use, manipulation, damage, or loss. Logical access controls also help to ensure that authenticated users access only what they are authorized to. Therefore, the County should have effective internal control policies and procedures to control access to its IT resources.

Condition and context—The County did not have adequate policies and procedures or consistently implement its policies and procedures to help prevent or detect unauthorized or inappropriate access to its IT resources. In addition, auditors noted that for 15 of 247 accounts tested, the access was either not properly reviewed and approved by a county employee, documentation was not maintained of the access granted, or the user accounts were active when no longer needed.

Effect—There is an increased risk that the County may not prevent or detect unauthorized or inappropriate access or use, manipulation, damage, or loss of its IT resources, including sensitive and confidential information.

Cause—The County did not have adequate policies and procedures or consistently implement its policies and procedures over logical and physical access controls.

Recommendations—To help prevent and detect unauthorized access or use, manipulation, damage, or loss to its IT resources, the County needs to improve and implement existing logical and physical access policies and procedures over its IT resources. IT policies and procedures should be reviewed against current IT standards and best practices, updated where needed, and implemented entity-wide, as appropriate. Further, staff should be trained on IT policies and procedures. The information below provides guidance and best practices to help the County achieve this objective.

- **Review account access to ensure appropriateness—**Documentation of access granted to each employee, contractor, and other nonentity accounts should be maintained. Access granted to IT resources should be reviewed and approved by a responsible employee to help ensure access granted is needed and compatible with job responsibilities and employee roles and responsibilities are appropriately separated. In addition, a periodic, comprehensive review should be performed of all existing employee, contractor, and other nonentity accounts to help ensure that network and system access granted remains necessary and appropriate and is compatible with job responsibilities.
- **Remove terminated employees' access to its IT resources—**Employees' network and system access should immediately be removed upon their terminations.
- **Review all shared and generic accounts—**Shared and generic network access accounts should be reviewed and eliminated or minimized when possible.
- **Manage shared and generic accounts—**Shared and generic accounts should be used only when appropriate and in accordance with an established policy authorizing the use of shared and generic accounts. In addition, account credentials should be reissued on shared accounts when a group member leaves.
- **Review and monitor key activity of users—**Key activities of users and those with elevated access should be reviewed for propriety.
- **Improve network and system password policies—**System password policies should be improved and ensure they address all accounts.

- **Manage remote access**—Security controls should be utilized for all remote access. These controls should include appropriate configuration of security settings such as configuration/connections requirements and the use of encryption to protect the confidentiality and integrity of remote sessions.
- **Review data center access**—A periodic review of physical access granted to the data center should be performed to ensure that it continues to be needed. In addition, this review should include a reconciliation of the County's listing of physical access badges assigned to its employees to employees with access to the data center.

The County's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

This finding is similar to prior year finding 2016-02.

2017-03

The County should improve its configuration management processes over its information technology resources

Criteria—A well-defined configuration management process, including a change management process, is needed to ensure that the County's information technology (IT) resources, which include its systems, network, infrastructure, and data are configured securely and that changes to these IT resources do not adversely affect security or operations. IT resources are typically constantly changing in response to new, enhanced, corrected, or updated hardware and software capabilities and new security threats. The County should have effective written configuration management internal control policies and procedures to track and document changes made to its IT resources.

Condition and context—The County has written policies and procedures for managing changes to most of its IT resources; however, they lacked critical elements and the County did not consistently implement its configuration management policies and procedures. As a result, for 26 of 40 changes to IT resources tested, there was a lack of supporting documentation demonstrating the change was authorized, reviewed, tested, and approved by an employee other than the employee making the change. Also, the County did not have policies and procedures to ensure all IT resources were configured securely.

Effect—There is an increased risk that the County's IT resources may not be configured appropriately and securely and that changes to those resources could be unauthorized or inappropriate, or could have unintended results without proper documentation, authorization, review, testing, and approval prior to being applied.

Cause—The County lacked sufficient policies and procedures over configuration management and detailed instructions for employees to follow and did not evaluate its policies and procedures against current IT standards and best practices.

Recommendations—To help prevent and detect unauthorized, inappropriate, and unintended changes to its IT resources, the County needs to review its configuration management policies and procedures against current IT standards and best practices, update them where needed, and implement them county-wide, as appropriate. The information below provides guidance and best practices to help the County achieve this objective.

- **Follow change management processes—**For changes to IT resources, the County should follow its change management process for each type of change, including emergency changes and other changes that might not follow the normal change management process. Further, all changes should follow the applicable change management process and should be appropriately documented.
- **Review proposed changes—**Proposed changes to IT resources should be reviewed for appropriateness and justification, including consideration of the change's security impact, in accordance with the established policies and procedures.
- **Document changes—**Changes made to IT resources should be logged and documented, and a record should be retained of all change details, including a description of the change, the departments and systems impacted, the individual responsible for making the change, test procedures performed and the test results, security impact analysis results, change approvals at each appropriate phase of the change management process, and a post-change review.
- **Rollback changes—**Rollback procedures should be established that include documentation necessary to back out changes that negatively impact IT resources.
- **Test—**Changes should be tested prior to implementation, including performing a security impact analysis of the change.
- **Separate responsibilities for the change management process—**Responsibilities for developing and implementing changes to IT resources should be separated from the responsibilities of authorizing, reviewing, testing, and approving changes for implementation or, if impractical, performing a post-implementation review of the change to confirm the change followed the change management process and was implemented as approved.
- **Configure IT resources appropriately and securely, and maintain configuration settings—**Configure IT resources appropriately and securely, which includes limiting the functionality to ensure only essential services are performed, and maintain configuration settings for all systems.
- **Manage software installed on employee computer workstations—**For software installed on employee computer workstations, policies and procedures should be developed to address what software is appropriate and the process for requesting, approving, installing, monitoring, and removing software on employee computer workstations.

The County's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

2017-04

The County should improve its contingency planning procedures for its information technology resources

Criteria—It is critical that the County have contingency planning procedures in place to provide for the continuity of operations and to help ensure that vital information technology (IT) resources, which include its systems, network, infrastructure, and data, can be recovered in the event of a disaster, system or equipment failure, or other interruption. Contingency planning procedures include having a comprehensive, up-to-date contingency plan; taking steps to facilitate activation of the plan; and having system and data backup policies and procedures.

Condition and context—The County's contingency plan lacked certain key elements related to restoring operations in the event of a disaster or other system interruption of its IT resources and the County did not consistently implement its contingency plan. Also, although the County was performing system and data backups, it did not have adequate policies and procedures for performing the backups or testing them to ensure they were operational and could be used to restore its IT resources.

Effect—The County risks not being able to provide for the continuity of operations, recover vital IT systems and data, and conduct daily operations in the event of a disaster, system or equipment failure, or other interruption, which could cause inaccurate or incomplete system and data recovery.

Cause—The County did not have adequate policies and procedures over its contingency plan and backup processes, or procedures in place to ensure they were tested appropriately, and did not evaluate its policies and procedures against current IT standards and best practices.

Recommendations—To help ensure county operations continue in the event of a disaster, system or equipment failure, or other interruption, the County needs to further develop its contingency planning procedures. The County should review its contingency planning procedures against current IT standards and best practices, update them where needed, and implement them county-wide, as appropriate. The information below provides guidance and best practices to help the County achieve this objective.

- **Update the contingency plan to ensure it includes all required elements to restore operations—**Contingency plans should be updated annually and encompass all county IT resources, and updates to the plan should be communicated to key personnel. The plan should include essential business functions and associated contingency requirements, including processes for eventual system recovery and reconstitution to return the IT resources to a fully operational state and ensure all transactions have been recovered. The contingency plan should be accessible to those who need to use it and protected from unauthorized disclosure or modification.
- **Move critical operations to a separate alternative site—**Policies and procedures should be developed and documented for migrating critical IT operations to a separate alternative site for essential business functions, including equipping the alternative site to resume essential business functions, if necessary.
- **Test the contingency plan—**A process should be developed and documented to perform regularly scheduled tests of the contingency plan and document the tests performed and results. This process should include updating and testing the contingency plan at least annually or as changes necessitate, and coordinating testing with other plans of the entity such as its continuity of operations, cyber incident response, and emergency response plans. Plan testing may include actual tests, simulations, or table top discussions and should be comprehensive enough to evaluate whether the plan can be successfully carried out. The test results should be used to update or change the plan.
- **Train staff responsible for implementing the contingency plan—**An ongoing training schedule should be developed for staff responsible for implementing the plan that is specific to each user's assigned role and responsibilities.
- **Backup systems and data—**Establish and document policies and procedures for storage and testing of backup media, including media containing sensitive information, to help ensure they could be recovered if needed. Policies and procedures should be updated and require system software and data backups to be protected.

The County's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

2017-05

The County should ensure all journal vouchers are reviewed and approved by someone other than the preparer

Criteria—In accordance with best practices and the County's policies and procedures, all journal vouchers should be reviewed and approved by someone other than the preparer. Proper segregation of duties helps ensure that financial activity is properly recorded in the accounting records and prevents fraudulent transactions from occurring.

Condition and context—The County's internal controls over journal vouchers were not adequate to ensure that transactions were properly reviewed and approved by a second employee. Specifically, for 8 of 239 transactions tested, county departments circumvented policies and procedures by requesting an employee to enter journal vouchers into the accounting system that were prepared and approved by the same employee. As a result, the transaction appeared to have been reviewed by two separate employees when it had not been. In addition, for one of the journal vouchers, the County could not locate supporting documentation for the transaction. No errors were noted to the financial statements.

Effect—Departmental journal vouchers were not always reviewed and approved by an employee other than the preparer.

Cause—County departments circumvented the County's policies and procedures because staff was limited in some departments.

Recommendations—To help ensure accuracy of the financial statements and validity of journal voucher transactions, the County should enforce its policies and procedures requiring all journal vouchers have a detailed review and approval by a second employee.

The County's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

2017-06

The County should ensure expenditures are recorded in the proper period

Criteria—The County should record expenditure transactions in the period the liability was incurred. Expenditures should be identifiable in the County's accounting system to ensure transactions are recorded in the proper accounting period in accordance with U.S. generally accepted accounting principles (GAAP).

Condition and context—The County's policies and procedures for coding expenditure transactions were not always followed to ensure that expenditures were recorded in the proper accounting period. Specifically, for 12 of 321 expenditure transactions tested, the County did not properly record the expenditure in the appropriate fiscal year. Auditors noted that 8 of the expenditure transactions should have been recorded in the prior fiscal year; whereas the other 4 transactions were incorrectly recorded in the subsequent fiscal year.

Effect—The County did not properly accrue year-end expenditures and liabilities in accordance with GAAP at June 30, 2016 and June 30, 2017, on the financial statements. The County made recommended audit adjustments to the financial statements to correct for these errors.

Cause—Several county departments did not always follow the finance department's policies and procedures for coding expenditure transactions in the proper fiscal year.

Recommendations—To help ensure accuracy of the County's financial statements, the County's departments should follow the finance department's policies and procedures and code expenditures correctly in the accounting system to ensure the expenditures are properly recorded in the correct fiscal year on the financial statements.

The County's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

Other auditor's findings:

The other auditors who audited the Housing Authority (Authority) reported the following material weakness:

2017-07

Balance Sheet Reconciliations

Criteria—Adequate internal controls require timely recording and reconciliation of general ledger activity to ensure accurate financial reporting and the safeguarding of funds.

Condition and context—Balance sheet accounts are not reconciled timely and/or on a periodic basis. Most significantly, bank reconciliations were not completed timely throughout the year. In addition, the bank reconciliation process includes significant recording activities.

Effect—Significant yearend reconciliations and adjustments were necessary to report accurate financial statements. Most significantly, bank reconciliations contained approximately $90,000 in unreconciled differences and interfund balances and inter-program transfers required $321,725 and $493,920 in audit adjustments to correct.

Cause—

- Employee turnover
- Chronically behind on financial processes/reconciliations
- Complexity of accounting enterprise software including creation of new cost centers
- Increased training and monitoring requirements due to the above causes.

Recommendations—We recommend that financial activity be reconciled on a periodic basis to ensure accurate and timely financial reporting. Further, we recommend the Authority discontinue the process of reported and recording inter-program and other month-end reconciliation entries through the bank reconciliation function. The bank reconciliation process should not be used to track and record entries within the accounting system. Unreconciled items should be corrected with approved journal entries in a timely basis.

The County's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

COUNTY RESPONSE

Maricopa County

Office of Assistant County Manager and Department of Finance

Shelby L. Scharbach
CPA, CGFM
Assistant County Manager
and
Chief Financial Officer
301 West Jefferson St Suite
960
Phx, AZ 85003-2148
Phone: 602-506-3561
Fax: 602-506-4451
www.maricopa.gov

February 9, 2018

Debbie Davenport
Auditor General
2910 North 44th Street, Suite 410
Phoenix, AZ 85018

Dear Ms. Davenport:

The accompanying Corrective Action Plan has been prepared as required by Governmental Auditing Standards. Specifically, we are providing you with the name of the contact person responsible for the corrective action, the corrective action planned, and the anticipated completion date for the finding included in the Report on Internal Control and Compliance.

Sincerely,

Shelby L. Scharbach, CPA, CGFM
Assistant County Manager — Chief Financial Officer

Maricopa County
Corrective Action Plan
Year Ended June 30, 2017

Financial statement findings

2017-01
The County should improve security over its information technology resources and improve its risk-assessment process
Contact person(s): Kevin Westover, Business Integration Specialist, Office of Enterprise Technology, (602) 506-1667
Anticipated completion date: December 15, 2018

Concur. Maricopa County takes all IT audit findings seriously and will make efforts to resolve any deficiencies. The County will take actions to improve security over IT resources and improve its risk-assessment process.

2017-02
The County should improve access controls over its information technology resources
Contact person(s): Kevin Westover, Business Integration Specialist, Office of Enterprise Technology, (602) 506-1667
Anticipated completion date: March 30, 2018

Concur. Maricopa County takes all IT audit findings seriously and will make efforts to resolve any deficiencies. The County will improve access controls over its IT resources.

2017-03
The County should improve its configuration management processes over its information technology resources
Contact person(s): Kevin Westover, Business Integration Specialist, Office of Enterprise Technology, (602) 506-1667
Anticipated completion date: February 28, 2018

Concur. Maricopa County takes all IT audit findings seriously and will make efforts to resolve any deficiencies. The County will improve its configuration management process over IT resources.

2017-04
The County should improve its contingency planning procedures for its information technology resources
Contact person(s): Kevin Westover, Business Integration Specialist, Office of Enterprise Technology, (602) 506-1667
Anticipated completion date: June 29, 2018

Concur. Maricopa County takes all IT audit findings seriously and will make efforts to resolve any deficiencies. The County will improve contingency planning procedures for IT resources.

Maricopa County
Corrective Action Plan
Year Ended June 30, 2017

2017-05
The County should ensure all journal vouchers are reviewed and approved by someone other than the preparer
Contact person(s): John Lewis, Finance Director, Department of Finance, (602) 506-1376
Anticipated completion date: June 29, 2018

Concur. The Department of Finance sent out an email to all departments in August 2017 as a reminder of the importance of segregation of duties. In addition, the County is currently updating its policies and procedures over journal vouchers, which includes preparer and approver responsibilities.

2017-06
The County should ensure expenditures are recorded in the proper period.
Contact person(s): John Lewis, Finance Director, Department of Finance, (602) 506-1376
Anticipated completion date: June 29, 2018

Concur. The Department of Finance continues to work with departments to ensure that expenditures are properly recorded in the correct fiscal year. In addition, the Department of Finance performs additional procedures at year end to analyze and identify transactions that may be incorrectly recorded.

2017-07
Housing Authority of Maricopa County (HAMC): Balance Sheet Reconciliations
Contact person(s): Mario L. Aniles, HAMC Director of Finance and Portfolio Management, (602) 744-4517
Anticipated completion date: December 2017

Concur. HAMC will be updating the bank reconciliation process to include timely resolution for “unreconciled” or “need more research” items along with separate reconciliations for non-cash items. Additionally trainings and technical assistance has been obtained to accelerate and address the agency’s learning curve for new staff.

ARIZONA
Auditor General
Making a Positive Difference