A REPORT
TO THE
ARIZONA LEGISLATURE

Financial Audit Division

Report on Internal Control and Compliance

Maricopa County

Year Ended June 30, 2009

Debra K. Davenport
Auditor General

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 of school districts, state agencies, and the programs they administer.

Copies of the Auditor General's reports are free.
You may request them by contacting us at:

Office of the Auditor General

2910 N. 44th Street, Suite 410 • Phoenix, AZ 85018 • (602) 553-0333

Additionally, many of our reports can be found in electronic format at:

www.azauditor.gov

Maricopa County
Report on Internal Control and Compliance
Year Ended June 30, 2009

Table of Contents — Page

Report Issued Separately

Comprehensive Annual Financial Report

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

WILLIAM THOMSON
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 the financial statements of the governmental activities, aggregate discretely presented component units, each major fund, and aggregate remaining fund information of Maricopa County as of and for the year ended June 30, 2009, which collectively comprise the County's basic financial statements, and have issued our report thereon dated December 22, 2009. Our report was modified to include a reference to our reliance on other auditors. We conducted our audit 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. Other auditors audited the financial statements of the Stadium District, Risk Management, Employee Benefits Trust, and the Housing Authority of Maricopa County, 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, we considered the County's internal control over financial reporting as a basis for designing our auditing procedures 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 over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the County's internal control over financial reporting.

Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and would not necessarily identify all deficiencies in internal control over financial reporting that might be significant deficiencies or material weaknesses. However, as discussed below, we identified certain deficiencies in internal control over financial reporting that we consider to be significant deficiencies.

2910 NORTH 44th STREET • SUITE 410 • PHOENIX, ARIZONA 85018 • (602) 553-0333 • FAX (602) 553-0051

A control deficiency 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 misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the County's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the County's basic financial statements that is more than inconsequential will not be prevented or detected by the County's internal control. We consider items 09-01 through 09-06 described in the accompanying Schedule of Findings and Recommendations to be significant deficiencies in internal control over financial reporting.

A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the County's internal control.

Our consideration of internal control over financial reporting was for the limited purpose described in the first paragraph of this section and would not necessarily identify all deficiencies in internal control that might be significant deficiencies and, accordingly, would not necessarily disclose all significant deficiencies that are also considered to be material weaknesses. However, of the significant deficiencies described above, we consider items 09-01, 09-03, and 09-05 to be material weaknesses.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the County's basic financial statements are free of 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's responses to the findings identified in our audit are included herein. We did not audit the County's responses and, accordingly, we express no opinion on them.

This report is intended solely for the information and use of the members of the Arizona State Legislature, the Board of Supervisors, management, federal awarding agencies, and pass-through entities and is not intended to be and should not be used by anyone other than these specified parties. However, this report is a matter of public record, and its distribution is not limited.

Jay Zsorey, CPA
Financial Audit Director

December 22, 2009

09-01
The County should improve transportation infrastructure reporting

Criteria: The County should accurately account for and value its transportation infrastructure capital assets in the government-wide financial statements as required by Governmental Accounting Standards Board (GASB) Statement No. 34, *Basic Financial Statements—and Management's Discussion and Analysis—for State and Local Governments*.

Condition and context: Approximately $918.6 million, 20 percent of the County's total assets, consist of transportation infrastructure capital assets. During test work on the County's transportation infrastructure capital assets, auditors noted the following errors:

- The County incorrectly capitalized $10 million in costs related to other governments' construction projects.
- The County incorrectly capitalized $5 million in costs to preserve the useful lives of existing assets.
- The County removed $16 million of assets that it still owned at June 30, 2009, and incorrectly included approximately $0.5 million of assets that it no longer owned.
- The County did not remove assets that were annexed by cities and towns from its transportation infrastructure assets listing at the proper amounts. As a result, it understated the deletion values for 21 land parcels by $1.5 million and understated the deletion value for 2 roadways by nearly $7 million.
- The County overstated infrastructure and construction in progress assets by $38 million and understated land by $42.6 million because of prior period misstatements resulting from assets that were incorrectly deleted, assets that should have been deleted but were not, assets that were incorrectly capitalized, and assets that were not recorded.

Effect: Transportation infrastructure capital asset beginning balances were understated by $4.6 million, and auditors proposed approximately $40 million in audit adjustments to correct the financial statements. The County adjusted its financial statements for all significant errors and restated the July 1, 2008, balances for errors affecting prior years. This finding is a material weakness in internal control over financial reporting.

Cause: The County did not have complete written policies and procedures in place to accurately account for and value its transportation infrastructure capital assets.

Recommendation: The County should implement policies and procedures to accurately account for and value its transportation infrastructure capital assets. These policies and procedures should include the following:

- Establish guidelines to determine when to capitalize costs associated with projects managed in conjunction with other governments;
- Require that preservation costs be recorded as expenses in the year incurred;
- Remove the historical value of infrastructure assets from its accounting records in the fiscal year in which the annexation ordinance is received from a city or town; and
- Maintain an assets listing for land parcels and roadways that agrees to the financial statements and update the listing annually for improvements.

A similar finding was noted in the previous year.

09-02
The County should accurately report its infrastructure required supplementary information

Criteria: Since the County uses the modified approach for infrastructure assets, it should present certain infrastructure data as required supplementary information (RSI) to demonstrate that it is maintaining and preserving assets at a condition level established and disclosed by the County. This supplementary information is required by GASB Statement No. 34, *Basic Financial Statements—and Management's Discussion and Analysis—for State and Local Governments*.

Condition and context: Auditors performed limited procedures on the modified approach for infrastructure assets RSI and noted that the County did not include any of the estimated and actual preservation costs recorded in its Transportation Capital Projects Fund for the past 5 fiscal years.

Effect: The County understated its estimated annual maintenance and preservation costs for roadways by $1,176,000 to $9,315,000 and bridges by $273,000 to $2,590,000. Also, the County understated its actual annual maintenance and preservation costs for roadways by $1,105,559 to $4,476,090 and bridges by $41,057 to $904,814. The County adjusted its disclosure to correct the errors. This finding is a significant deficiency in internal control over financial reporting.

Cause: The County did not have written policies and procedures in place to clearly define what was to be included in RSI, and therefore, it failed to include the preservation costs recorded in the Transportation Capital Projects Fund.

Recommendation: The County should implement policies and procedures which provide instructions for calculating the estimated and actual costs that should be included in the RSI disclosure.

09-03
The County should develop, implement, and test a disaster recovery plan

Criteria: The County's policy states that each department should establish a disaster recovery plan to ensure that: (1) its information resources are protected, backed up, and recoverable and (2) the integrity, availability, and reliability of all electronic assets are not compromised or affected. In addition, a recommended practice of the Government Finance Officers Association concerning technology disaster recovery planning recommends that every government should evaluate its written disaster recovery policies and procedures annually and update and test them at least once every 3 years.

Condition and context: The County did not have written and tested disaster recovery plans for its network, document imaging system, human resources and payroll system, and the Treasurer's financial systems. Further, the Treasurer's financial systems lacked an uninterruptible power source.

Effect: The disruption of services, caused by disaster or other disturbances, could result in significant harm or inconvenience to the County and its citizens. In addition, inadequate disaster recovery controls subject the County to risks that can result in inaccurate or incomplete financial or management information, expensive recovery efforts, and financial losses. This finding is a material weakness in internal control over financial reporting.

Cause: A formal disaster recovery plan had not been developed in the past because of a lack of resources.

Recommendation: The County should develop a disaster recovery plan for its significant information technology systems. At a minimum, the County's plan for computer disaster recovery should include the following:

- A risk analysis identifying and prioritizing critical applications to determine which applications should be recovered first.
- A listing of current employees assigned to disaster teams, including telephone numbers.
- Employee assignments and responsibilities.
- A designated alternative computer facility or arrangements with vendors to support hardware and software requirements.
- Details of off-site storage locations and availability of information stored at these locations.
- A list of procedures for processing critical transactions, including forms or other documents to use.
- Restoration procedures for backup media such as tapes and servers.
- Documentation of overall testing strategies, testing frequencies, and disaster plan test results.

Further, the County should install an uninterruptible power source for its Treasurer's financial systems.

A similar finding was noted in the previous year.

09-04
The County should strengthen logical access controls for its computer systems

Criteria: Logical access controls ensure that only authorized users have access to the County's computer systems and are necessary to protect computer systems and data from unauthorized use, damage, loss, modification, or disclosure. To comply with industry standards, employees should have access to only those applications necessary for their job responsibilities. When circumstances exist that require an employee to have heightened access privileges, a supervisor should review the employee's system activity.

Condition and context: The County did not have proper and complete control procedures in place to ensure the system users were granted access rights to only those functions necessary to perform their job responsibilities. This resulted in a user having greater access rights than necessary without supervisory review of the user's activity within the system. Auditors identified the following instances of incompatible access or heightened privileges:

- Two employees with general ledger access had the ability to create and approve payment vouchers.
- Two employees with general ledger access had the ability to create and approve both vendors and payment vouchers.
- Twelve individuals from an outside vendor, utilized during a system conversion, maintained full privileges on the general ledger system even though this heightened access no longer appeared necessary.
- The activity of two employees in the Treasurer's financial systems with heightened user privileges was not regularly reviewed.

Effect: Users may have access to unauthorized information and the ability to perform unauthorized functions, including creating and approving vendors, purchase requisitions, receiving documents, and payment vouchers. Excessive access rights may allow users to perpetrate and conceal errors and irregularities, resulting in fraud and the possible misstatement of financial information. This finding is a significant deficiency in internal control over financial reporting.

Cause: The County did not have complete written control policies and procedures in place to ensure users were granted appropriate access rights or that the activities of approved employees with heightened access privileges were reviewed. In addition, the finance security administrator relied on the departments to check for incompatible responsibilities; however, departments were not aware of this responsibility.

Recommendation: The County should have control procedures in place to ensure users are granted access rights to only those functions necessary to perform their job responsibilities. Specifically, department administrators should review and approve individualized access rights for each employee and ensure that access is granted to employees for only those functions required to perform their job responsibilities. If department administrators find system access that is incompatible with an employee's responsibilities, they should revoke that access. Further, for users with heightened access privileges, activity should be listed in a report and an independent reviewer should review the report for unusual activity. In addition, a review of system access rights should be performed regularly to ensure heightened access rights assigned are still necessary. If they are not necessary, those rights should be removed.

09-05
The County needs to implement controls over physical access to its computer data centers

Criteria: Physical access controls ensure that only authorized users have physical access to the County's computer systems and are critical in protecting computer systems and data from unauthorized use, damage, loss, or modification. To comply with industry standards, procedures should be established that grant, limit, and revoke access according to business needs, and all access should be justified, authorized, reported, and monitored.

Condition and context: The County did not have control procedures in place to ensure that only specific users were granted physical access rights to the County's data centers which house the County's computer systems, and that access was properly monitored. Specifically, the Treasurer's data center access is by key entry; however, of the 24 keys issued to employees, one employee had a key, but there was no documentation showing that that employee was approved. In addition, four keys on the listing were missing, and two employees who had access to the Treasurer's data center did not appear to need access. In addition, for 10 of 20 individuals selected for test work at the Office of Enterprise Technology data center that houses the human resource and payroll system, document imaging system, and the network computers, the County was unable to provide documentation to verify that the individuals had legitimate purposes for having access to the data center.

Effect: By obtaining access to data centers and equipment, an individual could obtain access to terminals or telecommunications equipment that provide input into the computer, obtain access to confidential or sensitive information, substitute unauthorized data or programs, or inflict malicious damage on computer equipment and software. This finding is a material weakness in internal control over financial reporting.

Cause: Policies and procedures were lacking because of an oversight. In addition, responsibility over physical access had changed recently, and procedures for obtaining and monitoring access were not consistent.

Recommendation: The County should establish and implement formal policies and procedures for obtaining and monitoring access to the data centers that include preparing a formal request for access, documenting the reason for access, having access approved by system owners, and adhering to physical access controls by a security-responsible person. The formal request should be retained by the County for as long as the user has access to the data center. In addition, management should periodically review the access list and access should be revoked for those users who no longer need entrance to the data center.

09-06
The County should follow its policy for change management for the Treasurer's financial systems

Criteria: All changes, including emergency maintenance and patches, relating to computer systems or applications within the production environment should be formally controlled. Changes should be logged, tested, reviewed, and authorized prior to implementation and reviewed against planned outcomes following implementation according to county policy.

Condition and context: The County could not document that change controls were in place for all changes made to its Treasurer's financial systems programs. The Treasurer's Office used a commercial software program to track program changes; however, it did not use this software program for all changes. In addition, the Treasurer's systems allowed changes to be made through direct updates to the underlying database, and the report that tracked these kinds of changes can be turned off.

Effect: Inadequate program change management could lead to unauthorized changes; incorrect changes, or ineffective changes. This finding is a significant deficiency in internal control over financial reporting.

Cause: The County did not follow its change control policies because of a lack of resources.

Recommendation: The County should implement its change control procedures for all types of program changes to its Treasurer's financial systems and retain adequate supporting documentation for them.

A similar finding was noted in the previous year.

Maricopa County
Department of Finance

Shelby L. Scharbach
CPA, CGFM
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 11, 2010

Ms. Debbie Davenport
Auditor General
2910 North 44th Street, Suite 410
Phoenix, Arizona 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 names of the contact persons responsible for the corrective action, the corrective action planned, and the anticipated completion date for each finding included in the Report on Internal Control and Compliance.

Sincerely,

Shelby L. Scharbach
Chief Financial Officer

Maricopa County
Corrective Action Plan
Year Ended June 30, 2009

09-01
The County should improve transportation infrastructure reporting
Contact person: Mark Modin, Finance Manager, Maricopa County Department of Transportation, (602) 506-8644
Anticipated completion date: July 2010

Concur. The County recognizes the significance of accurately accounting for its infrastructure assets and is in the process of implementing County-wide infrastructure policies and procedures that will provide departments with guidance in reporting, accounting for, and valuing their infrastructure assets. In addition, the Department of Transportation will develop their own written policies and procedures to accurately value transportation infrastructure assets and will review the audit recommendations and implement controls for joint projects with other governments, preservation costs, and annexations. Each year the Department of Transportation will use an infrastructure project plan to list each action item and its due date to manage the reporting process. Further, the County will continue to seek opportunities to improve its policies and procedures over infrastructure assets.

09-02
The County should accurately report its required supplementary information
Contact person: Mark Modin, Finance Manager, Maricopa County Department of Transportation, (602) 506-8644
Anticipated completion date: July 2010

Concur. The Department of Transportation will develop written policies and procedures over Required Supplementary Information (RSI) reporting and will provide instructions for calculating the estimated and actual costs that should be included in the disclosure. Preservation costs will be identified in both the operations and capital projects funds and included for RSI reporting. In addition, capital projects will be reconciled to preservation and capital costs schedules. The County will continue to evaluate opportunities to improve controls over RSI reporting.

09-03
The County should develop, implement, and test a disaster recovery plan
Contact person: Stacey Haggart, Deputy CIO, Office of Enterprise Technology, (602) 506-7130
Anticipated completion date: November 2010

Concur.

Human Resources (HR) Application: All enterprise HR/payroll/benefit processing is currently being migrated to a fully-hosted solution. The fully-hosted solution includes disaster recovery as a contracted service.

Financial System Application: The scheduled 2009 disaster recovery test for the financial system application was postponed until May 7, 2010, due to its migration from the former vendor data center hosting platform to the new vendor application hosting solution, which was conducted in May 2009. The solution includes disaster recovery as a contracted service.

Treasurer's System uninterrupted power source (UPS): The Treasurer's system upgrade is in progress and according to the recent agreement the servers will migrate to the Office of Enterprise Technology (OET) data center which has ample UPS power backup. OET has formed a disaster recovery team for other enterprise applications supported by the department; the disaster recovery plan will be documented and implemented per industry standards.

The OET disaster recovery team will investigate and address the recommendations in the 09-03 audit finding listed below:

- A risk analysis identifying and prioritizing critical applications to determine which applications should be recovered first.
- A listing of current employees assigned to disaster teams, including telephone numbers.
- Employee assignments and responsibilities.
- A designated alternative computer facility or arrangements with vendors to support hardware and software requirements.
- Details of off-site storage locations and availability of information stored at these locations.
- A list of procedures for processing critical transactions, including forms or other documents to use.
- Restoration procedures for backup media such as tapes and servers.
- Documentation of overall testing strategies, testing frequencies, and disaster plan test results.

09-04
The County should strengthen logical access controls to its computer systems.
Contact persons: Gina Denney, Financial Services Manager, Department of Finance, (602) 506-7297; Stacey Haggart, Deputy CIO, Maricopa County Office of Enterprise Technology, (602) 506-7130
Anticipated Completion Date: Financial System items #1 – 3 completed, #4 – September 2010; Treasurer's System - November 2010

Concur. The Department of Finance has been reviewing security profile changes made to the financial system for many years. The financial system generates an electronic communication with a log that defines all security profiles changes made during the week. Upon receipt, the Department of Finance Manager reviews the report and takes the appropriate action. These reports are imaged and available for review. The Department of Finance has taken the opportunity to enhance our policies and procedures by:

1) Including a "Reviewed By" section on the financial system Access Request Form which will be completed by the DOF Finance Manager or DOF Financial Supervisor. The

inclusion of this section ensures that a secondary review of the system access request is conducted. The associated Security Policy and Procedure Manual has been updated and is available on the Department of Finance Website.

2) Included the following statement of understanding on the financial system Access Form: By signing this application as the "Approving Authority," you are responsible for having reviewed all current user security profiles and confirming that the financial system USERID request and/or profile change has no internal control conflicts and is authorized."

3) Initiated a process to complete an annual review of all security profiles associated with the financial system to identify and correct any conflicts of interest and/or segregation of duties. The associated Security Policy and Procedure Manual has been updated and is available on the Department of Finance Website.

4) Maricopa County has been working with the hosting vendor to review the opportunities of implementing "logging." An analysis is currently being completed to review the types and number of tables to be logged, the potential impact on system performance and the costs associated with implementing logging.

In regards to the Treasurer's financial systems, the current legacy database does not have monitoring/auditing capabilities. With the planned move of the Treasurer's server and storage systems to the OET datacenter and hardware upgrades, acquiring a software package that provides logging capability is going to be analyzed. After the logging capability is implemented, the Treasurer's Office will collaborate with OET and business owners to identify users with heightened privileges, establish database logging and reporting of those users, and identify business application owners that will periodically review the database logging reports.

09-05
The County needs to implement controls over physical access to its computer data centers
Contact person: Stacey Haggart, Deputy CIO, Maricopa County Office of Enterprise Technology, (602) 506-7130
Anticipated Completion Date: May 2010

Concur. As part of the Treasurer's agreement, servers will move into the OET data center. OET is working on a procedure to incorporate datacenter badge access during Human Resources' employee processing for new hires, transfers, and terminations. Physical access will only be granted to those individuals that have been properly authorized by business owners and datacenter management. Badge access is defined by Zones which is handled by Protective Services. The process will include periodic access audits.

Maricopa County
Corrective Action Plan
Year Ended June 30, 2009

09-06
The County should follow its policy for Change Management for the Treasurer's financial systems
Contact person: Phil Van Kley, Maricopa County Treasurer's Office, (602) 506-4635
Anticipated Completion Date: August 2010

Concur. The Treasurer's Office agrees with the statements brought forth by the audit findings that the Treasurer's Office is in need of a revised change management policy. The Treasurer's Office recognizes the importance for change management and is working towards implementing the necessary procedures and protocols. Although many of the procedures will be implemented within the following weeks, the Treasurer's Office has determined that full implementation of all procedures and protocols will take approximately six months to complete. The Treasurer's Office plans to log, assess, and maintain authorization information in order to comply with County policies.