A REPORT
TO THE
ARIZONA LEGISLATURE

Financial Audit Division

Report on Internal Control and Compliance

Maricopa County Community College District

Year Ended June 30, 2008

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

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 Community College District
Report on Internal Control and Compliance
Year Ended June 30, 2008

Table of Contents

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 Governing Board of
Maricopa County Community College District

We have audited the financial statements of the business-type activities and discretely presented component unit of Maricopa County Community College District as of and for the year ended June 30, 2008, which collectively comprise the District's basic financial statements, and have issued our report thereon dated December 15, 2008. Our report was modified to include a reference to our reliance on other auditors and as to consistency because of the implementation of Governmental Accounting Standards Board Statement Nos. 45, 48, and 50. 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 Maricopa County Community College District Foundation, the discretely presented component unit, as described in our report on the District's financial statements. The financial statements of the Maricopa County Community College District Foundation were not audited by the other auditors in accordance with *Government Auditing Standards*. 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 report of the other auditors.

Internal Control over Financial Reporting

In planning and performing our audit, we considered the District'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 District's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the District'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.

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 District'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 District's basic financial statements that is more than inconsequential will not be prevented or detected by the District's internal control. We consider items 08-01 through 08-03 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 basic financial statements will not be prevented or detected by the District'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 item 08-01 to be material weakness.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the District'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 disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

Maricopa County Community College District's responses to the findings identified in our audit have been included herein. We did not audit the District'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 Governing Board, 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 15, 2008

Maricopa County Community College District
Schedule of Findings and Recommendations
Year Ended June 30, 2008

Maricopa County Community College District Findings

08-01
The District should strengthen computer access controls

System access controls restrict not only physical access to the District's computer information systems, but also logical access to those systems. System access controls help ensure that only authorized users have access to the District's computer systems and sensitive data. These controls are critical in preventing and detecting unauthorized use, damage, loss, or modification of programs and equipment, and the misuse of sensitive information. Therefore, the District should ensure that the access granted to users of its computer information systems is appropriate and limit physical access to IT equipment and stored data. However, the District's controls were not always sufficient for preventing and detecting unauthorized access. Specifically, the District did not retain documentation of user authorizations to its student information, general ledger, or payroll systems. As a result, the District could not provide documentation demonstrating who requested and approved the users access to these systems. Further, the District did not have guidelines when granting access to its computer systems to help ensure user access was appropriately restricted to only the access they needed to perform their jobs. In addition, the District did not monitor the campus security administrators and superusers for its Student Information System (SIS). These users had unlimited access privileges and could perform any and all operations on the SIS. Also, for the SIS, the District monitors activity and changes to the system on audit log reports. These audit log reports did not include key changes to database fields that would help monitor the system for unauthorized changes and all four database administrators had access to modify the audit logs. Finally, physical access to the District's main data center was not always restricted to authorized personnel and access was not adequately monitored.

The District should strengthen its policies and procedures over system access to help prevent or detect unauthorized use, damage, loss, or modification of programs and equipment and misuse of sensitive information. Only authorized users should have logical or physical access to the District's computer systems, and access should be limited to essential employees only. While the District currently has certain controls in place over electronic and physical access, implementing the following procedures will help strengthen controls:

- Retain system access authorizations.
- Identify roles and responsibilities on the SIS system that would be considered incompatible to help prevent these roles from being assigned incorrectly to any one employee.
- Limit the number of superusers.
- Monitor the system activities of each superuser and campus security administrator.
- Ensure audit log reports contain key fields. In addition, the database administrators should follow best business practices and have read-only access to the audit log reports.
- Access to the data center should be reviewed and approved prior to an employee's receiving access. Further, the District should frequently review the list of those authorized access to the data center and remove or modify access rights as necessary.

08-02

The District should test its disaster recovery plans for its computer information systems

The District's computerized information systems process, record, and store information that is vital to its daily operations. Therefore, it is critical that the District have an up-to-date disaster recovery plan in place to provide continued operations and to ensure electronic files are not lost because of a major computer hardware or software failure or other interruption. However, the District did not have a current and tested disaster recovery plan for its Student Information System (SIS). In addition, the District's disaster recovery plans for its IT Computer Center and payroll system have not been updated or tested since 2003. Additionally, the District's SIS backup server is physically stored at the same location as the main computer server. Further, the District has purchased but not set up an alternate computer facility that can be used to process daily transactions for its critical information systems in case of a major equipment or system failure. As a result, the District risks losing valuable data during a disruption or disaster.

To help ensure continuity of District operations in the event of major equipment or system failure or other interruption, the District's disaster recovery plan should be updated and tested annually for each of its critical systems. In addition, the District should ensure the plans include the following information:

- A current listing of employees assigned to disaster teams, including telephone numbers.
- Employee assignments and responsibilities.
- A risk analysis identifying critical applications.
- 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.
- Details of hardware and software requirements needed to run critical systems and the applicable vendors where hardware and software can be obtained.
- Restoration procedures for backup media (i.e., tapes and servers).
- An outline of overall testing strategies, establishing testing frequencies, and documentation of testing the disaster recovery plan.

In addition, the District should communicate and distribute copies of the disaster recovery plans to the necessary employees and ensure that they are aware of and are properly trained in their recovery responsibilities. Further, the District should periodically test the backup tapes and backup server, and the backup server should be located in a different physical location from the system servers so that it is available for operation in the event of a disaster.

A similar recommendation was previously provided to the District in our *Report on Internal Controls over Financial Reporting* dated December 17, 2007.

08-03

The District should improve controls over computer program changes

To help ensure that computer information systems function properly and to provide safeguards for confidential or sensitive information, it is critical that the District have written policies and procedures to provide the basic framework to ensure that changes to information system programs have been properly authorized, developed, tested, reviewed, and approved before being placed into operation. However, the District did not have adequate policies and procedures to control program changes to its Student Information System (SIS). Specifically, the District's policies did not include approval guidelines for program changes. Further, the District did not have a reliable program-change request-tracking system, that identified each request, and tracked the status of each request and the dates changes were made to the system. Additionally, the Development Manager and the programmer had unlimited access to make program changes. Finally, the District did not reconcile all changes moved into the production to those changes approved and authorized.

The District should have written policies and procedures documenting the SIS change management process. These procedures should include who has the ability to authorize, develop, test, and approve changes in the system, including emergency changes. In addition, the District should develop a tracking system to help monitor each request and change to the SIS. Further, the District should ensure that there is an adequate segregation of duties over the change management process so that no one individual can process and approve a critical change to the SIS. Finally, the District should reconcile all changes to the system to verify the changes were adequately tested, approved, and authorized.

MARICOPA COMMUNITY COLLEGES

www.maricopa.edu

DR. RUFUS GLASPER
CHANCELLOR

2411 W. 14th St.
Tempe, Arizona
85281-6942

Telephone
480.731.8000

Fax
480.731.8506

February 6, 2009

Ms. Debbie Davenport
Auditor General
2910 N. 44th Street, Suite 410
Phoenix, AZ 85018

Dear Ms. Davenport:

The accompanying corrective action plan has been prepared as required by Government Auditing Standards. Specifically, we are providing you with the names of the contact people responsible for the corrective action, the corrective action planned, and the anticipated completion date for the audit finding included in the Schedule of Findings and Recommendations for the fiscal year ended June 30, 2008.

Sincerely,

Kimberly Brainard Granio, CPA
Director, Financial Services and Controller

MARICOPA COUNTY COMMUNITY COLLEGE DISTRICT
Corrective Action Plan
Year Ended June 30, 2008

Financial Audit Findings

08-01
Contact person: Earl Monsour
Anticipated completion date: June 2009

Corrective Action Planned:
The District agrees with the finding and the recommendations. Procedures, policies and documentation will be developed to enhance logical and physical access controls.

08-02
Contact person: Earl Monsour
Anticipated completion date: June 2009 (however, the remote facility is not expected to be available for use until December 2009)

Corrective Action Planned:
The District agrees with the finding and the recommendations. Disaster recovery plans for critical systems will be updated. A testing schedule will be established to include recovery from backup tapes to ensure business continuity. A second data center is in the process of being established for the primary purpose of disaster recovery and operational backup capabilities. When this center is brought online in late 2009, failover systems will be located in a separate location.

08-03
Contact person: Earl Monsour
Anticipated completion date: June 2009

Corrective Action Planned:
The District agrees with the finding and the recommendations. A formal change management system, to include policy, procedures and tracking processes, will be developed.