A REPORT
TO THE
ARIZONA LEGISLATURE

Financial Audit Division

Report on Internal Control and Compliance

Maricopa County Community College District

Year Ended June 30, 2014

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.

The Auditor General's reports are available at:

www.azauditor.gov

Printed copies of our reports may be requested by contacting us at:

Office of the Auditor General
2910 N. 44th Street, Suite 410 • Phoenix, AZ 85018 • (602) 553-0333

Maricopa County Community College District
Report on Internal Control and Compliance
Year Ended June 30, 2014

Table of Contents

Report Issued Separately

Comprehensive Annual Financial Report

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
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 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, 2014, which collectively comprise the District's basic financial statements, and have issued our report thereon dated December 16, 2014. Our report includes a reference to other auditors who 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. 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. However, the financial statements of the Maricopa County Community College District Foundation were not audited in accordance with *Government Auditing Standards,* and accordingly, this report does not include reporting on internal control over financial reporting or instances of noncompliance associated with the Maricopa County Community College District Foundation.

Internal Control over Financial Reporting

In planning and performing our audit of the financial statements, we considered the District'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 District's internal control. Accordingly, we do not express an opinion on the effectiveness of the District'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 were not identified. However, as described in the accompanying Schedule of Findings and Recommendations, we identified certain deficiencies in internal control 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 District'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 2014-01, 2014-02, 2014-03, 2014-04, 2014-05, and 2014-06 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 deficiency described in the accompanying Schedule of Findings and Recommendations as item 2014-07 to be a significant deficiency.

Compliance and Other Matters

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

Maricopa County Community College District's Response to Findings

Maricopa County Community College District's responses to the findings identified in our audit are presented on pages 9 through 13. The District'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 District'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 District's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Jay Zsorey, CPA
Financial Audit Director

December 16, 2014

Maricopa County Community College District
Schedule of Findings and Recommendations
Year Ended June 30, 2014

Financial Statement Findings

2014-01

The District needs to improve procedures for approving adjunct faculty employment contracts

Criteria: The District should maintain a record of supervisory approvals of all employment contracts for adjunct faculty employees to help ensure that the District pays only for authorized and valid employment contracts.

Condition and context: The District needs to improve its procedures for paying its adjunct faculty employees. Payments to district employees were generally approved, recorded, and paid through the District's payroll system, except for adjunct faculty. Adjunct faculty are contracted part-time employees set up in the District's student information system (SIS) and then paid through the payroll system. Eighteen of 78 employees tested were adjunct faculty employees for whom the District did not have evidence that the employment contract was approved. The 18 adjunct faculty employees comprised a total of 35 SIS-initiated contracts paid without evidence of supervisory approval that the contracts were valid, and that payments were made from the correct district accounts for the proper amounts.

Effect: The District risks paying for unauthorized or invalid employment contracts, which could potentially result in inappropriate district charges. The District paid over $57.6 million to adjunct faculty employees during the fiscal year. Auditors were able to perform additional tests that confirmed that the 35 contracts for the 18 adjunct faculty employees tested were valid and correctly charged.

Cause: The District did not have adequate procedures for approving adjunct faculty employees' SIS-initiated contracts, as required by the District's policies.

Recommendation: To help ensure that the District pays only for authorized and valid employment contracts, the District should ensure that its established policies requiring the supervisory review and approval of employment contracts are consistently followed for adjunct faculty employees. Specifically, the District should improve its procedures for ensuring that approvals be performed, documented, and maintained for all employment contracts, including those initiated in SIS. Approvals may be maintained either in hard copy form or electronically.

This finding is similar to a prior-year finding.

2014-02

The District needs to improve procedures for approving employees' time sheets

Criteria: A district supervisor should review and approve employees' time sheets to help ensure that the District pays employees only for authorized hours worked.

Condition and context: The District's policies require a supervisory review and approval of employees' time sheets. However, to ensure that employees are paid in a timely manner, the District's payroll system automatically approves time sheets not approved by a supervisor in order to process payroll. The District did not have other controls to help ensure that supervisors reviewed and approved time sheets after the system's automatic approval. Specifically, for 7 of 78 employees tested, 41 percent of those employees' time sheets were not approved by a supervisor.

Effect: The District risks paying for unauthorized hours worked, which could potentially result in inappropriate District charges. The District paid over $43 million to hourly employees during the fiscal year. Auditors were not able to extend auditing procedures sufficiently to determine the total number of timesheets that may not have been approved.

Cause: The District's procedures for processing employees' time sheets did not ensure that time sheets were reviewed and approved by a supervisor, as required by the District's policies.

Recommendation: To help ensure that it pays employees only for authorized and approved hours worked, the District should improve its existing procedures for reviewing and approving employees' time sheets.

2014-03

The District needs to continue improving information technology oversight and risk management

Criteria: A strong governance structure over information technology (IT) involves the oversight of separately managed locations and uniform policies that are consistently applied. In addition, a strong governance structure and a continual risk management process that is documented and guides IT increases the likelihood that systems will operate as intended to protect the integrity of financial and sensitive information, and allow a reasonable response to and remediation of known and potential threats to information security.

Condition and context: The District needs to strengthen its oversight and risk management processes over IT and improve oversight of its 11 colleges and two skill centers, most of which have their own IT department and personnel. Auditors performed auditing procedures at the district office and two of the District's colleges and found that the District needs to expand its written policies and procedures so it can effectively oversee the consistent application of appropriate IT practices in securing financial and sensitive information on a district-wide basis. In addition, the District should perform IT risk management processes on a continual basis, and these processes should include colleges and skill centers, and address appropriate aspects of IT, including security. Certain information has been omitted from this finding because it is considered confidential as it pertains to IT security.

Effect: Without better oversight and continual risk management processes over IT, there is an increased likelihood that systems may not operate as intended to protect the integrity of financial and sensitive information.

Cause: The District needs to have sufficiently clear lines of authority for managing IT operations and needs to expand its written policies and procedures applicable to all of the colleges and skill centers. The District has contracted with consultants to assist in developing policies and to conduct information security assessments, including some risk management processes. Also, in July 2014, the District hired a chief information security officer, whose duties include helping improve the District's oversight of security at the colleges and skill centers and assisting with information security remediation efforts.

Recommendation: To help increase the likelihood that systems operate as intended to protect the integrity of financial and sensitive information, the District should continue to strengthen oversight and risk management processes over IT. To help achieve this, the District should clarify lines of authority at the district office and expand its written policies and procedures outlining appropriate practices applicable to all of the colleges and skill centers. Additionally, to enhance its ability to appropriately respond to and remediate known and potential threats to information security, the District's risk management processes should cover additional aspects of IT, including security; be performed on a continual basis; and include all of the colleges and skill centers. Furthermore, the District should train employees on its policies and procedures, and monitor employees' compliance with these policies and procedures.

2014-04

The District needs to continue improving IT security

Criteria: To effectively maintain and secure financial and sensitive information used in operations, guidance should be provided to employees through written policies and procedures that are based on acceptable IT industry practices, as appropriate. In addition, a formal security awareness program and proactive IT security controls and practices help to prevent, detect, and respond to instances of unauthorized access or use, damage, loss, or manipulation of IT systems and data, including financial and sensitive data, used in operations.

Condition and context: The District needs to continue developing and enhancing its policies and procedures for maintaining and securing financial and sensitive information. These policies and procedures should be carried out though written guidance and the implementation of security training, controls, and practices. Certain information has been omitted from this finding because it is considered confidential as it pertains to IT security.

Effect: Implementing additional security measures may not eliminate all risk. However, without implementing additional security measures, there is an increased likelihood of unauthorized access or use, damage, loss, or manipulation of IT systems and data that could potentially occur without being prevented or detected.

Cause: The District needs additional policies and procedures over IT security. In July 2014, the District hired a chief information security officer, whose duties include helping improve the District's oversight of security at the colleges and skill centers and assisting with information security remediation efforts.

Recommendation: To enhance its ability to secure financial and sensitive information, the District should continue developing its written IT security policies and procedures in line with acceptable IT practices as appropriate. Guidance to carry out these policies and procedures should be documented, communicated, and available to employees responsible for implementation. In addition, the District should implement a formalized training program for employees to help facilitate their understanding and application of the policies and procedures including security awareness.

2014-05

The District needs to continue improving IT access controls

Criteria: Effective internal control policies and procedures over access to IT are needed to help prevent and detect unauthorized access or use, damage, loss, or manipulation of IT systems and data, including financial and sensitive information.

Condition and context: The District needs to continue developing its policies and procedures for assigning, maintaining, monitoring, and removing logical access to IT systems. In addition, auditors performed limited tests and noted areas needing improvement that the District should include in its policies and procedures. Finally, the District had certain physical access controls in place for its data center, but needs to continually evaluate and update these policies and procedures to increase the likelihood that they remain effective. Certain information has been omitted from this finding because it is considered confidential as it pertains to IT security.

Effect: Implementing additional security measures may not eliminate all risk. However, without implementing additional security measures, there is an increased likelihood of unauthorized access or use, damage, loss, or manipulation of IT systems and data could potentially occur without being prevented or detected.

Cause: The District needs additional policies and procedures over IT access and increased oversight of the colleges to increase the likelihood that policies and procedures are effectively implemented. In July 2014, the District hired a chief information security officer, whose duties include helping improve the District's oversight of security at the colleges and skill centers and assisting with information security remediation efforts.

Recommendation: To help prevent and detect unauthorized access or use, damage, loss, or manipulation of IT systems and data, the District should continue developing its policies and procedures over IT access. Furthermore, the District should train employees on its policies and procedures, and monitor employees' compliance with these policies and procedures.

This finding is similar to a prior-year finding.

2014-06

The District needs to continue improving IT change management processes

Criteria: Policies and procedures for IT change management should be documented and consistently applied when making changes to IT systems and data to help decrease the likelihood of unauthorized, inappropriate, and unintended changes.

Condition and context: The District's policies and procedures for making changes to its IT systems and data should be updated to match existing practices and provide clear guidance to facilitate consistent application. In addition, the District's change management processes need to improve the manner in which the District addresses testing, reviewing, and implementing changes; adequately separating certain responsibilities; and detecting whether unauthorized, inappropriate, or unintended changes occurred. Certain information has been omitted from this finding because it is considered confidential as it pertains to IT security.

Effect: Implementing additional security measures may not eliminate all risk. However, without implementing additional security measures, there is an increased likelihood that unauthorized, inappropriate, or unintended changes to IT systems and data could potentially occur without being prevented or detected.

Cause: The District needs more comprehensive change management policies and procedures.

Recommendation: To help prevent and detect unauthorized, inappropriate, and unintended changes to IT systems, the District should continue enhancing its existing written policies and procedures for change management. In addition, the District should improve its change management processes. Furthermore, the District should train employees on its policies and procedures, and monitor employees' compliance with these policies and procedures.

2014-07

The District needs to continue improving data backup and recovery policies and procedures

Criteria: It is important to have a comprehensive contingency plan in place to provide for the continuity of operations and to increase the likelihood that vital IT systems and data can be recovered in the event of a disaster, system or equipment failure, or other system interruption.

Condition and context: The District had some backup and recovery processes in place, but needs to continue improving its written policies and procedures to increase the likelihood that it can efficiently recover IT systems and data vital to its operations in the event this is needed. Certain information has been omitted from this finding because it is considered confidential as it pertains to IT security.

Effect: Implementing additional data recovery and security measures may not eliminate all risk. The District could potentially have difficulty or be unsuccessful in recovering IT systems and data necessary to conduct daily operations in the event of a disaster, system or equipment failure, or other system interruption.

Cause: The District needed more comprehensive data recovery policies and procedures.

Recommendation: The District should continue to improve its backup and recovery policies and procedures and processes to increase the likelihood that IT systems and data necessary to conduct daily operations in the event of a disaster, system or equipment failure, or other system interruption, can be recovered and restored. Furthermore, the District should train employees on its policies and procedures, and monitor employees' compliance with these policies and procedures.

This finding is similar to a prior-year finding.

DISTRICT RESPONSE

MARICOPA COMMUNITY COLLEGES®

2411 W. 14th Street, Tempe, Arizona 85281 - 6942 • T 480.731.8000 • F 480.731.8506 • www.maricopa.edu

March 31, 2015

Debbie Davenport
Auditor General
2910 N. 44th St., Ste. 410
Phoenix, AZ 85018

Dear Ms. Davenport:

We have prepared the accompanying Corrective Action Plan as required by the standards applicable to financial audits contained in *Government Auditing Standards*. Specifically, for each financial reporting finding we are providing you with the names of the contact persons responsible for corrective action, the corrective action planned, and the anticipated completion date that is included in the Report on Internal Control and Compliance.

Sincerely,

Kimberly Brainard Granio, CPA, M.Ed.
Associate Vice Chancellor, Business Services & Controller

Maricopa County Community College District
Corrective Action Plan
Year Ended June 30, 2014

Financial Statement Findings

2014-01

The District needs better controls over adjunct faculty employment contracts
Names of contact persons: Kim Granio and Sam Dosumu
Anticipated completion date: Spring 2015

The District agrees with the finding and recommendation. Neither of the District's current enterprise systems (Human Resource Management System-HRMS and Student Information System-SIS) are currently able to require electronic approvals of adjunct faculty assignments initiated in SIS. Standardized alternative procedures have been implemented at each college to require the initiator of adjunct faculty assignments to manually review and approve such assignments each semester and approvals will be maintained either in hard copy form or electronically.

2014-02

The District needs better controls over approving employees' time sheets
Names of contact persons: Kim Granio
Anticipated completion date: Fall 2015

The District agrees with the finding and recommendation. The District's Human Resource Management System (HRMS) is not currently configured to require supervisory approvals of time sheets in order to pay employees for hours recorded. The District is in the process of updating and reconfiguring HRMS and changing the configuration to require supervisory approvals to pay time recorded is one of many changes in development. Although the current system doesn't require the supervisory approvals in order to pay hours recorded, there are many budget checks of expenses throughout the fiscal year and any material deviations from budgeted wages or large variances from prior year's actual expenses would be noted and investigated. In addition, all grant-funded time sheets that are not approved by a supervisor are manually certified by the project director.

2014-03

The District needs to continue improving information technology oversight and risk management
Names of contact persons: Edward Kelty and Miguel Hernandez
Anticipated completion date: There is no completion date for continued improvement of information technology oversight and risk management. Information security risks, and the means for containing these risks, evolve continuously, so the District must adapt as change takes place. Continued improvement is planned for 2015, and the District will refine these plans as warranted.

The District agrees with the finding that it needs to continue improving its information technology (IT) oversight and risk management. The District will continue to strengthen oversight and risk management processes over information technology. During the calendar year, the District hired both a Chief

Information Security Officer and a Chief Privacy Officer to lead district-wide information security and privacy efforts and clarify lines of authority from the District Office to the colleges and skill centers. In February of 2015, the District hired a Director of IT Security, and it plans to add two additional Directors of IT Security to the Information Security Office.

Additionally, the Information Technology Leadership Council ("ITLC"), which is comprised of senior IT leaders from the District and colleges, continues to meet on a bi-monthly basis to advise, provide input, and develop recommendations regarding information technology infrastructure, services, standards, and systems to the district-wide Information and Instructional Technology Governance Council. The purpose of this collaborative effort between the District Office and colleges is to improve information technology and security district-wide. In March 2015, the ITLC created the Information Security Council, a subcommittee which has been formed to strengthen communication and awareness of cybersecurity initiatives district-wide.

During the audit year, Administrative Regulations were published on appropriate information security and privacy practices for the District Office, colleges, and skill centers. Beginning in March 2015, all employees are required to take and acknowledge training on the Information Security and Privacy Administrative Regulations. These policies will be reviewed and enhanced on a consistent basis, where necessary. Further, the District is in the process of developing and enhancing written guidance regarding information technology and security, which will be applicable to District Office and the colleges and skill centers.

2014-04

The District needs to continue improving IT security

Names of contact persons: Edward Kelty and Miguel Hernandez

Anticipated completion date: There is no completion date for continued improvement of information technology security. Information security risks, and the means for containing these risks, evolve continuously, so the District must adapt as change takes place. Continued improvement is planned for 2015, and the District will refine these plans as warranted.

The District agrees with the finding that it needs to continue improving its information technology security. During the audit year, Administrative Regulations were published to outline appropriate information security and privacy practices for the District Office, colleges, and skill centers. These policies were reviewed and enhanced in November 2014. Beginning in March 2015, all employees are required to take and acknowledge training on the Information Security and Privacy Administrative Regulations. The District also intends to provide privacy and security training to Maricopa's Information Security Incident Response Plan, management, and Board by June 2015. Further, the District is in the process of enhancing and formalizing written guidance regarding various components of information technology and security, which will be applicable to District Office and the colleges and skill centers. These policies will be reviewed and enhanced on a consistent basis, as necessary.

The District also is in the process of enhancing its formal security awareness program. In October of 2014, Maricopa participated in Cybersecurity Awareness Month as "Champions" of cybersecurity. This educational campaign, which included the dissemination of educational materials and training videos as

well as related cybersecurity events, targeted Maricopa's students, faculty, and staff to enhance cybersecurity awareness at the enterprise level.

2014-05

The District needs to continue improving IT access controls

Names of contact persons: Edward Kelty and Miguel Hernandez

Anticipated completion date: There is no completion date for continued improvement of information technology access controls. Information security risks, and the means for containing these risks, evolve continuously, so the District must adapt as change takes place. Continued improvement is planned for 2015, and the District will refine these plans as warranted.

The District agrees with the finding that it needs to continue improving its information technology access controls. During the audit year, Administrative Regulations were published to outline appropriate information security and privacy practices for the District Office, colleges, and skill centers. The District also is in the process of developing and enhancing written guidance regarding information technology and security, including physical and logical access controls, which will be applicable to District Office, colleges, and skill centers. These policies will be reviewed and enhanced on a consistent basis, where necessary, to further improve Maricopa's information security posture and information technology access controls.

2014-06

The District needs to continue improving IT change management processes

Names of contact persons: Edward Kelty and Miguel Hernandez

Anticipated completion date: There is no completion date for continued improvement of information technology change management processes. Information security risks, and the means for containing these risks, evolve continuously, so the District must adapt as change takes place. Continued improvement is planned for 2015, and the District will refine these plans as warranted.

The District agrees with the finding that it needs to continue improving its information technology change management processes. During the audit year, the District updated its change management program and processes governed by the Change Advisory Board which meets weekly to review and communicate changes to information technology systems. The District will continue to develop and enhance its change management program, and update its written guidance to reflect improved change management procedures.

Maricopa County Community College District
Corrective Action Plan
Year Ended June 30, 2014

2014-07

The District needs to continue improving data backup and recovery policies and procedures

Names of contact persons: Edward Kelty and Miguel Hernandez

Anticipated completion date: There is no completion date for continued improvement of data recovery policies and procedures. Information security risks, and the means for containing these risks, evolve continuously, so the District must adapt as change takes place. Continued improvement is planned for 2015, and the District will refine these plans as warranted.

The District agrees that it needs to continue improving its data recovery policies and procedures. The District will review and continue to improve its backup and data recovery policies and procedures.

Maricopa County Community College District
Report on Internal Control and Compliance
Year Ended June 30, 2014

State of Arizona
Office of the Auditor General