



A REPORT  
TO THE  
ARIZONA LEGISLATURE

Financial Audit Division

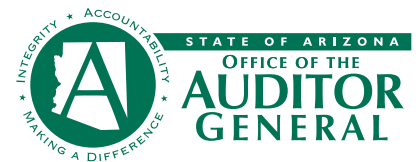
---

Report on Internal Control and Compliance

# Maricopa County Community College District

Year Ended June 30, 2015

---



---

**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](http://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, 2015

Table of Contents	Page
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 <i>Government Auditing Standards</i>	1
Schedule of Findings and Recommendations	3
District Response	9
Report Issued Separately	
Comprehensive Annual Financial Report	



DEBRA K. DAVENPORT, CPA  
AUDITOR GENERAL

STATE OF ARIZONA  
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 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, 2015, and the related notes to the financial statements, which collectively comprise the District's basic financial statements, and have issued our report thereon dated December 23, 2015. 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 reportable 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 first paragraph of this section 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 2015-01, 2015-02, 2015-03, 2015-04, and 2015-05 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 2015-06 and 2015-07 to be significant deficiencies.

### **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 23, 2015

Maricopa County Community College District  
Schedule of Findings and Recommendations  
Year Ended June 30, 2015

Financial Statement Findings

**2015-01**

---

---

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

---

---

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's policies and procedures did not ensure that adjunct faculty employees' employment contracts were approved. 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) before payment is processed on the payroll system. Specifically, 21 of 60 employees tested were adjunct faculty employees and for 18 of those 21 employees, the District did not have sufficient evidence that the employment contract was approved. The 21 adjunct faculty employees comprised a total of 35 SIS-initiated contracts and 30 of those 35 SIS-initiated contracts processed without sufficient evidence of supervisory approval indicating 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 \$56.7 million to adjunct faculty employees during the fiscal year. Auditors were able to perform additional tests that confirmed that the 30 contracts without sufficient evidential support for the 18 adjunct faculty employees tested were valid and correctly charged.

Cause: The District did not follow its policies and procedures for adjunct faculty employees whose employment contracts are initiated in SIS.

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

This is similar to prior-year finding 2014-01.

**2015-02**

---

---

**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.

Maricopa County Community College District  
Schedule of Findings and Recommendations  
Year Ended June 30, 2015

Condition and context: The District's policies require a supervisory review and approval of employees' time sheets. However, to help 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 for payroll to be processed. The District did not have other controls in place to require supervisors to review and approve time sheets after they had been automatically approved.

Effect: The District risks paying for unauthorized hours worked, which could potentially result in inappropriate district charges. The District paid over \$36 million to hourly employees during the fiscal year. Auditors were unable to extend auditing procedures sufficiently to determine the total number of time sheets 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.

This is similar to prior-year finding 2014-02.

**2015-03**

---

**The District should continue improving information technology oversight and risk management**

---

Criteria: A strong governance 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 helps guide IT policies increases the likelihood that systems will operate as intended to protect the integrity of information, and allow a reasonable response to and remediation of known and potential threats to information security.

Condition and context: During the year, the District strengthened oversight of its colleges and skill centers by clarifying authority and expanding its written policies and procedures over IT resources. The District should continue to oversee the colleges and skills centers for consistent application of appropriate IT practices in securing financial and sensitive information on a district-wide basis. In addition, the District enhanced its policies for assessing IT security risk during the year. The District should continue these efforts and perform IT risk management processes on a continual basis that include all 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 resources, there is an increased likelihood that systems may not operate as intended to protect the integrity of financial and sensitive information.

Maricopa County Community College District  
Schedule of Findings and Recommendations  
Year Ended June 30, 2015

Cause: Previously, the District needed to have sufficiently clear lines of authority for managing IT operations at its 11 colleges and two skill centers, most of which have their own IT department and personnel. The District strengthened this oversight. The District adopted written policies and procedures during the year and is continuing to assess and revise those policies and procedures.

Recommendation: To help increase the likelihood that systems operate as intended to protect the integrity of information, the District should continue to strengthen oversight and risk management processes over IT resources. The District should continue to oversee the colleges and skill centers for consistent application of its policies and procedures. To enhance its ability to appropriately respond to and remediate known and potential threats to information security, the District should continue to implement policies and procedures for assessing IT security risk as part of its overall risk management processes and ensure that risk assessments are performed on a continual basis and include all of the colleges and skill centers. Furthermore, the District should continue to train employees on its policies and procedures, and monitor employees' compliance with its policies and procedures.

This is related to prior-year finding 2014-03.

## **2015-04**

---

### **The District should continue improving IT security**

---

Criteria: To effectively maintain and secure 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 used in operations.

Condition and context: During the year, the District adopted written policies and procedures on various areas of IT security and is continuing to assess those policies and procedures. The District should continue enhancing its policies and procedures for maintaining and securing financial and sensitive information through 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 adopted written policies and procedures during the year and is continuing to assess and revise those policies and procedures.



Maricopa County Community College District  
Schedule of Findings and Recommendations  
Year Ended June 30, 2015

Recommendation: To enhance its ability to secure information, the District should continue implementing IT security controls and practices outlined in its policies and procedures. Further, the District should ensure that employees responsible for implementing security controls and practices are properly trained to help facilitate their understanding and application of the policies and procedures so that the policies and procedures are consistently applied at the colleges and skill centers.

This is related to prior-year finding 2014-04.

**2015-05**

---

**The District should 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.

Condition and context: During the year, the District adopted written policies and procedures for assigning, maintaining, and removing physical and logical access to IT systems and data. The District is continuing to assess those policies and procedures and should continue enhancing its policies and procedures through 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 adopted written policies and procedures during the audit year and is continuing to assess and revise those policies and procedures.

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

This is related to prior-year finding 2014-05.

**2015-06**

---

**The District should 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.

Maricopa County Community College District  
Schedule of Findings and Recommendations  
Year Ended June 30, 2015

Condition and context: During the year, the District adopted written policies and procedures for making changes to IT systems and data, and improved its change management processes for testing, reviewing, and implementing changes and is continuing to assess those policies and procedures. The District should continue improving its processes, separate certain responsibilities, and enhance controls for 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 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 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 continue to train employees on its policies and procedures, and monitor employees' compliance with its policies and procedures.

This is related to prior-year finding 2014-06.

## **2015-07**

---

### **The District should 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 systems and data can be recovered in the event of a disaster, system or equipment failure, or other system interruption.

Condition and context: During the year, the District adopted written policies and procedures for backing up and recovering its systems and data and is continuing to assess those policies and procedures. The District should continue enhancing its policies and procedures through training, controls, and practices. Also, the District should continue monitoring the colleges and skill centers for consistent application of its policies for their disaster recovery plan efforts. 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 system and data necessary to conduct daily operations in the event of a disaster, system or equipment failure, or other system interruption.

Cause: The District adopted written policies and procedures during the year and is continuing to assess and revise those policies and procedures.

Maricopa County Community College District  
Schedule of Findings and Recommendations  
Year Ended June 30, 2015

Recommendation: To increase the likelihood that the District can efficiently recover IT systems and data vital to its operations in the event that it is needed, the District should continue to enhance its backup and data recovery policies and procedures and processes. Furthermore, the District should train employees on its policies and procedures, and monitor the colleges and skill centers for consistent application of its policies for their disaster recovery plan efforts.

This is related to prior-year finding 2014-07.





---

2411 W. 14th Street, Tempe, Arizona 85281 - 6942 • T 480.731.8000 • F 480.731.8506 • [www.maricopa.edu](http://www.maricopa.edu)

March 31, 2016

Debbie Davenport  
Auditor General  
2910 N. 44<sup>th</sup> 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, 2015**

Financial Statement Findings

**2015-01**

---

*The District needs to improve procedures for approving 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 Capital Management System-HCM and Student Information System-SIS) is currently able to require electronic approvals of adjunct faculty assignments initiated in SIS. Standardized alternative procedures were implemented at each college in Spring 2015 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.

**2015-02**

---

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

*Names of contact persons: Kim Granio and Barbara Basel*

Anticipated completion date: Fall 2015

---

The District agrees with the finding and recommendation. The District's Human Capital Management System (HCM) is not currently configured to require supervisory approvals of time sheets in order to pay employees for hours recorded and the District is reluctant to penalize hourly employees for lack of supervisory compliance. Therefore, throughout Fall 2015 and Spring 2016, the District has made a significant effort to train and notify supervisors and managers when recorded hours have not been approved and to escalate these notifications when non-compliance continues. The next step in the process is to determine what corrective action may be taken when repeated non-compliance is evidenced. Additionally, we will continue to seek out compensating controls so as to have adequate procedures while continuing to pay employees for hours recorded. Although this area still needs improvement, 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. Furthermore, all grant-funded time sheets that are not approved by a supervisor are manually certified by the project director.

**Maricopa County Community College District  
Corrective Action Plan  
Year Ended June 30, 2015**

**2015-03**

---

*The District should 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 2016, and the District will refine these plans as warranted.

---

The District agrees with the finding that it should continue improving its information technology oversight and risk management. To continue its efforts to strengthen IT security oversight and risk management processes, the following activities have occurred:

During the calendar year 2015, the District Information Security Office expanded from one Chief Information Security Officer (“CISO”) with no dedicated staff to an office of four (one CISO and three Directors of Information Security). Plans are in place to continue expanding the District Information Security Office to include five additional Directors of Information Security to assist with IT oversight at the colleges and skill centers.

The CISO continues to meet regularly with the Information Technology Leadership Council (“ITLC”), which is comprised of senior IT leaders from the District and colleges. The purpose of the ITLC is to continue improving information technology and security district-wide. In addition, the ITLC Information Security Council, which contains representation from each College, continues to meet to enhance communication and awareness of cybersecurity initiatives district-wide.

The District continues to enhance and improve IT Risk Management. In particular, a vulnerability assessment tool was purchased for all Colleges and the District Office to standardize the approach to vulnerability identification. During the audit year, District IT also purchased training for one staff member from each of the colleges. Training on the tool was completed by September 2015. Additional efforts are underway to provide additional training for each college so that both a primary and secondary staff member could be trained in the use of the tool.

The District provisionally adopted written policies and procedures in June 2015 and is working with a variety of constituent groups including the Information Security Office, ITLC, the Information Security Council, Privacy, Legal, Faculty, and employee groups in an effort to continually assess and enhance those policies and procedures. Finalized policies and procedures will be socialized district-wide using email announcements and articles in the District’s newsletter, The Maricopan. The District will continue to provide guidance to increase the likelihood that the policies and procedures are consistently applied at the colleges and skill centers.

**Maricopa County Community College District  
Corrective Action Plan  
Year Ended June 30, 2015**

**2015-04**

---

*The District should 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 2016, and the District will refine these plans as warranted.

---

The District agrees with the finding that it should continue improving its information technology security. The District provisionally adopted written policies and procedures in June 2015, and is working with a variety of constituent groups including the Information Security Office, ITLC, the Information Security Council, Privacy, Legal, Faculty, and employee groups in an effort to continually assess and enhance those policies and procedures. Finalized policies and procedures will be socialized district-wide using email announcements and articles in the District's newsletter, The Maricopan.

All employees are required to take and acknowledge training on the Information Security and Privacy Administrative Regulations. This mandatory training continues and efforts are underway to provide additional mandatory information security awareness training.

The following steps have been taken to further increase information security awareness district-wide:

1. The District Information Security Office provides all new employees with an introduction to Information Privacy and Security principles at each New Employee Orientation.
2. For two consecutive years, the District has participated in Cyber Security Awareness Month.
3. For two consecutive years, the District has participated in Data Privacy Day.

The District Information Security Office is in the very early stages of establishing a social media and social networking presence on Twitter and Google+.

**2015-05**

---

*The District should 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 2016, and the District will refine these plans as warranted.

---

The District agrees with the finding that it should continue improving its information technology access controls. The District will continue assessing and enhancing its policies and procedures over IT access controls, and will continue its efforts to provide training and monitor compliance of its policies and procedures.



**Maricopa County Community College District  
Corrective Action Plan  
Year Ended June 30, 2015**

**2015-06**

---

*The District should 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 2016, 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. The Change Advisory Board, which governs the change management program and processes, continues to consistently meet weekly to review and communicate changes to information technology systems. The program has been further enhanced to include core members from Human Resources, Business Services, and Student Affairs. The District will continue to enhance and improve its change management program and update its written guidance to reflect improved change management procedures as necessary.

**2015-07**

---

*The District should 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 backup and 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 2016, and the District will refine these plans as warranted.**

---

The District agrees that it should continue improving its data backup and recovery policies and procedures. During the year, the District Emergency Manager, Information Technology, and core members from Business Services, Academic Affairs, and Human Resources engaged with a consulting firm specializing in Business Continuity and Disaster Recovery to conduct a Business Impact Analysis. Information Technology will continue to work with the District Emergency Manager and the consulting firm to complete the Disaster Recovery initiative. The District will continue to enhance and improve its backup and data recovery policies and procedures.

